

Total Information Risk Management

Maximizing the Value of Data
and Information Assets

Alexander Borek

Ajith K. Parlikad

Jela Webb

Philip Woodall



ELSEVIER

AMSTERDAM ■ BOSTON ■ HEIDELBERG ■ LONDON
NEW YORK ■ OXFORD ■ PARIS ■ SAN DIEGO
SAN FRANCISCO ■ SINGAPORE ■ SYDNEY ■ TOKYO

Morgan Kaufmann is an imprint of Elsevier



Acquiring Editor: Andrea Dierna
Editorial Project Manager: Heather Scherer
Project Manager: Priya Kumaraguruparan
Designer: Maria Inês Cruz

Morgan Kaufmann is an imprint of Elsevier
225 Wyman Street, Waltham, MA, 02451, USA

Copyright © 2014 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility. To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Borek, Alexander.

Total information risk management : maximizing the value of data and information assets / Alexander Borek, Ajith Kumar Parlikad, Jela Webb, Philip Woodall. -- 1st edition.
pages cm

Includes bibliographical references and index.

1. Business information services. 2. Database management--Quality control. 3. Information technology--Security measures. 4. Data protection. 5. Intellectual capital. I. Title.

HF54.5.B67 2014

658.4'038011--dc23

2013027888

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-405547-6

Printed in the United States of America

14 15 16 17 10 9 8 7 6 5 4 3 2 1

For information on all MK publications visit our website at www.mkp.com



Working together
to grow libraries in
developing countries

www.elsevier.com • www.bookaid.org

Dedication

Alex: To my parents, Jadwiga and Jerzy - for all your love

Ajith: To Siddharth and Priya - my pillars of strength

Jela: To Richard - for your love and support

Phil: To Anna Mieczakowski - my amazing inspiration

In praise of *Total Information Risk Management: Maximizing the Value of Data and Information Assets*

“Alexander’s research and this book represents a significant contribution to the fields of Information Quality and Data Governance. Having worked in staff roles at the coal face applying IQ principles and DG practices to Regulatory risk I was pleased to see many of the methods and insights my old team stumbled on nearly a decade ago validated through rigorous research. A worthy addition to the practitioner’s book shelf!”

- Daragh O’Brien, Castlebridge Associates

“When writing about information and data quality, most authors have focused on assessment and improvement. Approaching information quality from the perspective of risk management is a great contribution to the field because it helps to broaden and deepen the conversation in a way that address information quality value and business impact in a quantifiable way. Both IT professionals and business managers will benefit from reading this book.”

- Professor John R. Talburt, Graduate Coordinator for the Information Quality Graduate Program, University of Arkansas at Little Rock

“Most organizations have an often-overlooked sweet spot, where risk management and information quality intersect and combine to significantly reduce risk and improve business performance. In this breakthrough book, Alexander Borek leads us there.”

- C. Lwanga Yonke, Information Quality Practitioner

Acknowledgments

We are very grateful to the Engineering and Physical Sciences Research Council (EPSRC) in United Kingdom, which funded this research.

Moreover, the book would not exist without the kind help of many different people that were part of our journey. In particular, we would like to warmly thank the following individuals:

Martin Oberhofer, Valeria Klassen, Ismael Caballero, John Ladley, Julian Schwarzenbach, Tom Redman, Lwanga Yonke, Andy Koronios, Jing Gao, Maurizio Tomasella, Raj Srinivasan, David Loshin, Andrea Dierna, Priya Kumaraguruparan, Heather Scherer, Markus Helfert, Pascal Wichmann, Zbigniew Gackowski, Mark Gosden, Allan MacMaster, Gerhard Satzger, Robert Kern, Hans-Joerg Fromm, Matthew West, Andreas Hart, David Becker, Dylan Jones, John Talburt, Alois Vogl, Bill Winkler, Gerhard Lackner, Danette McGilvray, Duncan McFarlane, Andy Neely, Daragh O Brian and all other academic and industrial collaborators that we missed out to mention here. Finally, we would like to remember Professor Zbigniew Gackowski from California State University in Stanislaus who sadly passed away on the 28th of May 2013. You were an inspiration to us. When work is not work then there is no need to retire.

Foreword by Thomas C. Redman

People in the data quality profession should feel rightly proud in having created a body of thinking, approaches, methods, and tools that work! When applied with reasonable diligence, departments and companies that first direct their data quality efforts on preventing errors at the source, focus on the most important needs of the most important customers, identify and eliminate the root causes of error, and build in controls to keep root causes from coming back nearly always succeed. They make huge improvements, sometimes an order of magnitude or more. And they reap enormous benefits!

At the same time, people in the data quality profession have to ask themselves the hard question: “So why doesn’t everyone pick up the data quality mantra?” I think about and discuss this question with others all the time. There are many reasons—some direct all their attention to clean-up and never get to the root causes, some don’t stick it out, and many treat data quality solely as an IT issue. Others haven’t been able to establish and communicate a powerful enough business case to advance the effort! I don’t have too much sympathy for those who don’t approach data quality correctly, who don’t have the wherewithal to stick with it, and who assign the effort to the wrong group.

I do, however, have considerable sympathy for those who have been unable to establish the business case. In the data quality profession we have to take a measure of responsibility here—we have not developed the comprehensive, powerful, compelling business cases, delivered them in convincing fashions, or built the base of support needed to consistently convince a critical mass of people that improving data quality is worth the trouble! Don’t misunderstand here—we have developed “good enough” business cases for the leading few, but not for the many. Nor have we laid out the methods that “less-than-expert” people can use to build their business cases and have a fair shot.

This is where this book comes in! It fills a big hole, providing several things. First, is a new way of thinking about the business cases for data quality, featuring “risk” as the key insight. At the company level, more people understand risk than the cost of poor data quality, so business cases based on risk have a better chance.

Second are the step-by-step instructions needed to actually complete a business case. Early in my career I gave too little weight to step by steps. After all, if you understand the principles, you can work out the steps. This may be true, but the simple fact is that most people learn by doing. Further, the discipline of step-by-step instructions means a more inclusive, more carefully thought-out business case. In following a disciplined sequence, people will almost always uncover opportunities or insights they didn’t have before. I recall one such instance, when a team I worked with was presenting a review for senior

management. The project had saved the company tens of millions. But one senior executive pointed out, "I appreciate the money. But even more, I have the trusted data I need to run this operation far, far sooner. I appreciate that even more."¹

Third, the book drives us to quantify our business cases, including both uncertainty and costs, in better ways than we do now.

Fourth, this book makes clear that building a comprehensive business case is hard work! I read somewhere that it is generally considered unwise to put in just enough energy to leap halfway across the stream. So thanks for this reminder guys. Do a good job on the business case or don't do it all!

Finally, though it doesn't say so explicitly, the book reminds us that it's not just what you say, it is where you say it. Indeed, companies in many industries already have a chief risk officer. They may become the natural constituency for the risks associated with bad data.

To conclude, the book could not be more timely, especially in light of all the excitement about Big Data. Count me as the most enthusiastic supporter. I see the potential as virtually unlimited. So too the risk! Consider the brilliant Big Data work throughout the mid-2000s to slice and dice mortgages into collateralized debt obligations, satisfying different investors' appetites for risk and reward. But data about the underlying mortgages was wrong, and so on, and so on, and so on, and near financial collapse. Risk in bad data indeed!

Yet, as I type this (June 5, 2013), a front-page headline in today's *Wall Street Journal* reads "One of Wall Street's Riskiest Bets Returns." Collateralized debt obligations are back. Let's get the data right this time. Or at least understand the implications.

Thomas C. Redman,
The Data Doc
Rumson, New Jersey USA
June 2013

¹ Personal communication from memory and may not be exact.

Foreword by John Ladley

There is no lack of thinkers and pundits who like to slice the world of business and organizations into their component parts. The early decades of the 21st century are going to be identified, in part, by organizations delving into understanding the various disciplines around data and information. This is a good thing to a point. After all, our world gets more complicated over time, not less. But the business world has a tendency to get to a point where the pundits are just talking *about* things, and not *doing* anything.

This is the case around the managing of information assets. The information component is fully acknowledged as being vital to our business and political world. This includes managing transactions, spreadsheets, emails, media, etc. For the first time in human history, mainstream media, marketing, and government are directly addressing using data and information to make society better, optimize companies, and answer unasked questions. All of these messages are technology rich, optimistic and rosy.

No one talks about the other side of the coin. Bad things can happen. Executives and marketers hate the perception of negative. Most of us who do information quality and governance work have been told to “spin” our findings because the boss hates bad news. But when you talk about the bad things, you start to manage risk. And managing risk is a good thing. So talking about that which is perceived as bad means opening another aspect to the value of information assets.

You can quantify risk and, therefore, the management of risk. And for organizations that want to manage information assets, managing risk is a fresh angle to selling a desperately needed set of activity to upper managers who do not want to take the time to learn about data value.

Until now, associating risk management with an information program seemed esoteric. The first time I presented risk as a means to the end that we call data governance, I was told I was way out of the comfort zone for information managers. That was true. I was also told I was being too esoteric and should stick to benefits around “better data and more accurate reports.” That was not true. It might be hard, but it needs to be done. I am glad someone was listening.

Alexander Borek approached me after a talk about business alignment and data governance I gave in San Diego a few years ago. Normally when someone comes up after a talk it's because he or she was too shy to ask a question, wants a business card, or wants something for free. Refreshingly, Alexander was none of these, although he did get my business card. He proceeded to tell me he loved my talk, was all over the concept of risk, and, in fact, was going to write a book about it.

I am glad he and his coauthors stuck with it. The book you are about to read connects the dots. Very few authors in the field of EIM have managed to connect real business issues to the management of information. This one does it. Information asset management is a required component of modern business. Managing risk that lies within your information is crucial to business and organization success.

Risk is the “anti-value.” Information risk can render your multimillion-dollar Big Data wonderfulness into a pile of expensive barely understood technology. The TIRM approach is a formal process for quantifying information risk and is just as critical as quantifying better cash flow or more customers.

Is TIRM esoteric? Hardly, as risk management is a staple element in our business world. Is TIRM new? Not really. Risk management is real business “stuff.” But four decades of data processing have created an ability to foul up an organization quicker than ever before. Risk management needs to be applied to data and information.

Information risk management just seems new and esoteric. That’s what happens when humans label something as a change. We all know change isn’t easy and a good explanation sure helps. TIRM does that.

John Ladley
IMCue Solutions
St. Louis, Missouri USA
June 2013

About the Authors

Dr. Alexander Borek is the inventor of Total Information Risk Management (TIRM) and the leading expert on how to apply risk management principles to data management. Dr. Borek is a frequent speaker at international information management conferences and author of many articles covering a range of topics, including EIM, data governance, data quality, crowd sourcing, business intelligence and IT business value. In his current role as senior strategy consultant at IBM's corporate headquarters, Dr. Borek applies data analytics to drive IBM's worldwide sales strategy and is part of a team responsible for the transformation of IBM to a data-driven business. Previously, he led a team at the University of Cambridge to develop the TIRM process and test it in a number of different industries. He holds a PhD in engineering from the University of Cambridge.

Dr. Ajith Kumar Parlikad is a senior lecturer in industrial systems at the University of Cambridge. Dr. Parlikad leads research activities on engineering asset management and maintenance. His particular focus is examining how asset information can be used to improve asset performance through effective decision making. Ajith is an editor of the *International Journal of Information Quality* and has published over 60 papers in reputed academic journals and conferences. He actively engages with industry through research and consulting projects. He is a member of The Institution of Engineering and Technology (IET) Technical Professional Network Committee on Asset Management and sits on the judging panel for the IET Innovation Awards in Asset Management.

Jela Webb is a senior lecturer at the University of Brighton; her specialism is information and knowledge management. Ms. Webb first became interested in this discipline in the 1990s while researching her MBA examining teamwork in organizations. She subsequently formed her own management consultancy offering strategic advisory services in this emerging field and has consulted with organizations in a variety of sectors both in the United Kingdom and abroad. She was one of the first people in Europe to be awarded an MSc in information and knowledge management (IKM), completing her studies in 2002. In addition to writing articles and reports on IKM and related topics for various publications, she is the author of *Strategic Information Management* published by Chandos Publishing (Oxford) Ltd. in 2008. She has presented at conferences and facilitated discussion forums on the implementation of IKM programs. She has also been involved in research programs focusing on skills development for the new economy.

Dr. Philip Woodall is a research scientist at the University of Cambridge specializing in information management. He has extensive experience working with international public and private organizations

from various sectors, including transport, utilities, defense, public sector, manufacturing, and aerospace, to improve their information management and information quality practices. He has published numerous academic articles in leading international journals and conferences, and is an editor of *The International Journal of Information Quality*. In 2011, he was elected as chairman of the IET Asset Management conference in London, after having worked on information quality with several asset management organizations. Dr. Woodall also advises the U.K. government and leading business organizations on data management issues within the University of Cambridge Centre for Science and Policy, and is a proud member of St. Edmund's College in Cambridge. Previously, he worked in the software industry and gained his PhD in computer science from Keele University.

Introduction

WHAT YOU WILL LEARN IN THIS CHAPTER:

- The purpose of this book
- Intended audiences
- Structure of this book
- How to use this book

We are living in exciting times. The notion of Big Data has become a much discussed topic in the business world. Almost every chief executive officer (CEO) who regularly reads business magazines has to ask: “Am I on the right track with data and information management and utilization in my company?” In most organizations there are several new technologies emerging on top of what is already a myriad of old technologies, and this brings with it specific challenges. Many organizations are desperately seeking to hire data scientists to help weave through the complexity now being seen, and the new discipline of data science is evolving at a fast pace.

Data becomes the focus of executives because it is the essential material to generate the information insights that a business needs to strive in today’s increasingly competitive environment. Information insights allow commercial businesses to allocate resources more profitably, satisfy their customers more effectively, reduce costs, save energy and materials, and offer better products and services that consumers really want and that are priced competitively. Public authorities, governments, and local communities can use analytics to minimize the financial burdens placed on taxpayers, reduce crime, optimize transportation, improve reliability and quality of utility and citizen services, and diminish environmental pollution. Nonprofit organizations are also able to take considerable advantage of information insights to increase the speed of support logistics in crisis regions, achieve a better allocation of resources to solve global challenges, and speed up medical progress in fighting diseases. It is not an overstatement to say that advanced data analytics will drive a smarter and hopefully better planet.

As much as data and information are becoming key assets for all organizations, however, its use does undoubtedly bring with it many potential risks from strategic, operational, financial, compliance, governance, environmental, and societal perspectives. Information governance is increasingly exercising the minds of many organizations, not least because of more stringent legal and regulatory requirements being imposed on both private and public sector entities. All organizations handle information. The governance of information is absolutely vital to the early identification of potential risk, the prevention of risk, and ensuring business continuity in the event of adverse risk. Accurate data records and

the maintenance of such records is critical not only for meeting compliance requirements but for the longer-term survival of the organization. Organizations that fail to manage information risk effectively leave themselves open to fines, sanctions, and other penalties, not to mention loss of reputation and potential failure of the business.

Poor information management is not an option. There are many ways in which information can be compromised, damaged, or destabilized, leading to a multiplicity of problems. These range from those that are merely an inconvenience to those that can cause significantly harm to the organization. Nevertheless, the management of information risks is often poorly achieved because organizations give it low priority and, indeed, low visibility. Many view information risk as intangible and do not know how best to manage it. Consequently, and due to the challenges it brings, it is not given all the time and attention that it rightly deserves. The fact is that in today's increasingly intensive information-driven economy, new risks derived from information with poor-quality levels can and do appear quickly.

Organizations should recognize information risk management as being of vital strategic importance and a key component of overall business strategy. Managing information risk is important for all organizations regardless of size or structure—people within organizations need to be encouraged to manage the associated risks and regard such management as part and parcel of their day-to-day operations. Without an appreciation of the role they play, employees may either undertake activities or conversely fail to undertake activities, which consequently leave the organization exposed to unnecessary risks. Many organizations struggle to understand how to measure and quantify the impact information quality has on performance.

Luckily, the well-established discipline of risk management offers a variety of recognized concepts and methods to control the impact of uncertain events. In the data and information management discipline, thus far, risk management has been used in the past either to manage risks connected to disclosure of information or that arise from the failure of IT systems, but not directly to manage the risks when data and information assets are of poor quality. Therefore, existing information risk management processes address only a very small subset of the range of risks that are caused by poor data and information management.

The core idea in this book is to provide managers with a practical guide on how to apply risk management methods and principles more directly to data and information management. The journey to effectively manage information risks will undoubtedly require some initial investment in time and resources. But we also believe that managing information risk is an imperative for all organizations that want to protect themselves from malfunctioning. And there is a very positive side of managing information risk too: in the long term, the rewards for those organizations that manage information risk effectively will be significant, ranging from higher profitability, happier customers, and improved operational efficiency, to better investment decisions, and eventually leading to a sustainable competitive advantage.

WHAT IS TOTAL INFORMATION RISK MANAGEMENT?

Managers have to address the new challenges posed by the rising importance of data and information being viewed as key assets. Data and information are such important assets for an organization that it

is vital to understand how they impact the business performance of an organization. Data and information have an impact in every part of the organization; not taking these business impacts seriously can lead to risks that damage the organization.

Total Information Risk Management (TIRM) is a collection of concepts, methods, and techniques that we have developed to address these new challenges. The TIRM process has been advanced after conducting ground-breaking research at the University of Cambridge, funded by the British Engineering and Physical Sciences Research Council (EPSRC). Our research was undertaken in collaboration with many other international universities and many different organizations in a number of industrial sectors.

TIRM draws upon the extensive body of knowledge in the well-established discipline of risk management, as well as the newer discipline of data and information management. It provides organizations with the tools necessary to understand, measure, and control the business impact of data and information assets, effectively and efficiently.

PURPOSE OF THIS BOOK

In our view, current approaches to data and information management do not create a clear enough link between data and its actual business value. Many of the existing data management books deal with the technicalities of data management but only a few discuss in detail how data and information should be governed. This emphasis is well described in the following recommended texts: Danette McGilvray's "Executing Data Quality Projects", David Loshin's "The Practitioner's Guide to Data Quality Improvement", Thomas C. Redman's "Data-Driven: Profiting From Your Most Important Business Asset" and John Ladley's books "Data Governance" and "Making Enterprise Information Management (EIM) Work for Business".

One of the most integral questions about the management of data and information currently remains unanswered: it is very hard to provide real evidence as to where data and information really impact the business, and it is even more difficult to say to what extent an organization might be affected. This book offers an innovative approach to TIRM, which achieves a clear link between data, information, and the business. We demonstrate how best to achieve this by integrating risk management methods and techniques with the discipline of data and information management.

INTENDED AUDIENCES

The target audience for this book is people who want to learn how to make closer linkages between data and information and business value—that is, people who want to ensure that poor data and information do not threaten the well-being of their organization. The readership is targeted at both students and professionals in data management, business intelligence, and in the management of information systems and IT. This book will also be of interest to general managers and risk management practitioners. The book is written in a language that does not require readers to have any specific technical knowledge. Additionally, if readers are interested in how best to integrate the concepts in this book into a new or existing software system, Chapter 12 on software tools offers valuable guidance.

STRUCTURE OF THIS BOOK

This book is divided into four parts:

- In the first part of the book, we introduce general concepts in information and risk management to bring you up to speed with the concepts that TIRM is based upon.
- In the second part of the book, we explain the TIRM process in detail and how it can be implemented within an organization; we use a case study example to aid with understanding the process.
- In the third part of the book, we present advanced risk assessment techniques and software tools, and ways to establish organizational support and employee engagement, which can be used to support and enhance TIRM.
- The fourth part of the book offers a conclusion and outlook.

HOW TO USE THIS BOOK

The first part of the book discusses existing concepts in data and information management, data and information quality, and risk management. We recommend that you assimilate Chapter 3 because it explains the fundamentals that underpin the whole text. If you are new to data and information management and/or risk management, it is important to also read the remaining chapters in Part 1; they provide the basis for a general understanding of the rest of the text. If you are already familiar with some or all of the concepts, you can just read the parts that you are currently unfamiliar with and then move on to Part 2.

The second part of the book contains the new and most essential material: the TIRM process and how to apply it in an organization. This part should be read from beginning to end. When you later apply the TIRM process in your organization, this part of the book can be used as a facilitator's guide and you can refer to each step of the process, on an individual basis, as and when required.

The third part of the book on risk assessment techniques and software tools, and organizational support and employee engagements for TIRM, can be read either from beginning to end or you can select topic areas that are most relevant for you during the implementation of TIRM in your organization.

Chapter 1: Data and Information Assets

This chapter introduces key concepts about data and information assets and includes a discussion about the characteristics of data and information assets. This chapter also considers key concepts of data and information quality and explores the impact of having low-quality data and information assets.

Chapter 2: Enterprise Information Management

This chapter introduces the concept of enterprise information management (EIM) and discusses the key challenges and pressures for EIM today.

Chapter 3: How Data and Information Create Risk

This purpose of this chapter is to explain how data and information create risk in an organization. It starts with a short introduction to the anatomy of information risks, explores ways in which to mitigate risks, discusses how risk does not always have to have negative connotations, and moves on to explain why quantifying risk is worth the effort, before concluding with an explanation as to how risk management can help improve EIM.

Chapter 4: Introduction to Enterprise Risk Management

This chapter explores the well-established discipline of risk management, explaining what is risk, the processes associated with risk management, how to determine your organization's risk appetite, and how risk can be assessed and treated. It concludes with a description of the role of a key player in TIRM: the chief risk officer.

Chapter 5: Overview of TIRM Process and Model

This chapter gives an overview of the various stages of the TIRM process and discusses general aspects that need to be considered when applying the TIRM process. We also give an overview of the TIRM model, which is needed for stage B of the TIRM process.

Chapter 6: TIRM Process Stage A: Establish the Context

This chapter is the first of three that explain the three stages of the TIRM process. Here, you are shown how to set the motivation, goals, initial scope, responsibilities, and context of the TIRM process. Key areas, including how to establish the external environment, how to analyze the organization, and how to identify business objectives, measurement units, and risk criteria, are explained in this chapter. It also explains how to gain a thorough understanding of the information environment in which your particular business operates.

Chapter 7: TIRM Process Stage B: Information Risk Assessment

This chapter provides a step-by-step guide for implementing the information risk assessment stage of the TIRM process. The chapter demonstrates how to quantify the business impact of poor data and information quality, as well as illustrates how to identify information risks, analyze and quantify information risks, and evaluate and rank information risks.

Chapter 8: TIRM Process Stage C: Information Risk Treatment

This chapter provides a step-by-step guide for implementing the information risk treatment stage of the TIRM process. It covers the identification of causes of information risks, finding appropriate information risk treatments, calculating the costs and benefits, selecting and implementing information risk treatments, and verifying their effectiveness after implementation.

Chapter 9: Integrating the TIRM Process Within the Organization

This chapter gives a comprehensive illustration of how to integrate the TIRM process within an organization. It clarifies the roles and responsibilities that lead to successful integration and offers guiding principles for successful implementation.

Chapter 10: TIRM Process Application Example

Using a case study based on the authors' experience of implementing TIRM in an energy utility, this chapter shows the practical application of the TIRM process. It also demonstrates the significant benefits that can accrue from improving the quality of data and information holdings.

Chapter 11: Risk Assessment Techniques for TIRM

This chapter examines the popular techniques used for risk management and goes on to explore how they may be used in the context of information risk management. Some of these may be familiar and some less so.

Chapter 12: Software Tools: Automated Methods for TIRM

This chapter considers how automated software solutions can support the TIRM and examines how some of the TIRM process stages can be automated. It continues with a discussion about what information management tools and technologies are currently available for detecting and mitigating information risks.

Chapter 13: Establishing Organizational Support and Employee Engagement for TIRM

This chapter discusses strategies and concepts to overcome organizational resistance and increase employees' support for TIRM. It draws on models published in the literature to show how employee "buy-in" might best be achieved.

Chapter 14: Conclusions and Outlook

In the final chapter, we gather together our thoughts on the book and hope that you and your organization will gain benefit from the book as a whole.

WHAT IS THE VALUE OF READING THIS BOOK?

Most senior managers are interested in seeing the quantitative business value of an investment. Thus far, business value has been particularly hard to measure for data and information because they are usually considered as being too "intangible" to be quantified. This book removes the mystique that currently prevents organizations from managing information risks by introducing you to the discipline of TIRM. TIRM will help you to measure the benefits of improving the level of data quality and information insights in your organization and furthermore demonstrate how this provides real business value-driven recommendations.

In our research and consultancy with organizations in many different industrial sectors we found that there were many benefits attributable to the application of the TIRM process and we believe that your organization will similarly reap real business value from its implementation.

Building a Convincing Business Case for Any Type of Project, Program and Initiative that Aims to Improve the Quality of Data and Information Assets

The program, project or initiative can be anything from data management, data governance, data warehousing, data quality, business intelligence, business analytics, Big Data, social media analytics to more basic IT investments in infrastructure, services and software. It actually really does not matter what kind of project, program or initiative you want to run, you will need to convince the senior management in your organization of the business value of your planned undertaking. And for most of these projects the business value is that the business will be supplied with higher quality data and information assets, which improve business performance and reduce risk. We have good news for you: TIRM can help you to build a convincing business case for what you plan to do.

Focusing on Problems that Really Matter

Within organizations, TIRM can substantially leverage the success of information quality initiatives. Focusing on the information quality problems that cause the biggest issues and putting in place mitigation procedures to overcome these issues can reap significant rewards and provide organizations with high quality data and information assets.

Changing the Attitude of Your Employees Toward Information Quality

Information risk assessment illustrates to employees in their own task area the value of having a high level of information quality; this transmission of value can change the way employees think about information. As many information quality problems are attributable to people's behavior during data collection and processing, this can make a positive contribution to performance.

Fine-tuning Your Information Systems

Understanding how information is combined and used in an organization in a given context and knowing the information risks helps organizations fine-tune their information systems for optimum performance in the given context of the organization.

Investing in IT Only When it is Truly Valuable

Many effective solutions to mitigate information risks are nontechnical; they are, in fact, organizational. To avoid unnecessarily "throwing" an expensive IT solution at problems that can be better solved with less expensive methods, TIRM will help you identify the true root causes of the business problems and find the optimal solutions taking a holistic, interdisciplinary perspective. The number of wasted IT projects could be reduced in the long run as information systems are continuously optimized to deliver best value.

Protect Your Organization from Exposures

Data and information are such vital assets that they can do major harm to your organization if not managed correctly. TIRM can help you to protect your organization from regulatory fines, mis-investments, damages to your brand and other major risks that can arise from poor data and information assets.

A Relatively Inexpensive but Very Effective Way to Manage Information

TIRM does not require a huge investment in additional resources. In fact, it can be integrated into daily business routines in such a way that it is hardly noticeable. The benefits mentioned earlier can provide long-term, sustainable competitive advantage for organizations.

SUMMARY

In this book, we will show you how to set up an effective TIRM program in your organization, which can be a valuable source of sustainable competitive advantage. We will help you address the new challenges presented by the rising importance of recognizing and managing data and information as key organizational assets. We will show you how to maximize the value of data and information assets.

Data and Information Assets

“I would like to assert that data will be the basis of competitive advantage for any organization that you run.”

—Ginni Rometty, CEO of IBM

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How data and information have become the most important assets of the 21st century
- How to define data and information assets and what their unique characteristics are
- Key concepts of data and information quality
- The business impact of having low-quality data and information assets

WHERE NAPOLEON MEETS MICHAEL PORTER: DATA AND INFORMATION ARE ASSETS

Napoleon Bonaparte, the great French emperor, conquered nearly the whole of Europe in the early 19th century before he was finally defeated at Waterloo. According to some sources, one of his famous sayings was “war is 90% information.”

In the Second World War, the allies could decrypt the secret codes generated by the ENIGMA machine that the Nazi regime used for communicating. This enabled the allies to end Nazi Germany’s submarine dominance in the world’s oceans.

More recently, in the mid-1980s, Michael Porter, one of the great management thinkers of our generation, observed, together with Victor Millar, that “the information revolution is sweeping through our economy,” thus making information the foremost competitive differentiator.

In a way, in the time between Napoleon and Porter, not much seems to have changed in this regard: information was and is one of the most important factors for competitive advantage. Data and information can help to win wars—both real ones and those we fight in business and our everyday life. And even if you are not competing against another organization, your biggest obstacles might be the constraint of time and resources, thereby limiting the means with which to

follow your noble goals. It is no understatement to say that information can make the difference in the fight against poverty, environmental pollution, climate change, and diseases like cancer, malaria, and HIV.

It really does not matter what type of business you are in—information will be key to your success. Your organization could be in the private, public, or nonprofit sector. It may be local, national, or global. It may be a sole trader, a partnership, a company, or a charity. It may be large or small. The permutations are varied, but what is homogenous is the reliance upon information.

Analyzing large volumes of data can provide us with such valuable insights that it can be a true game changer. And because data and information are so valuable and powerful, we call them *assets*. This chapter explores what is behind the concept of data and information assets. We start with some recent history, look at data and information themselves, including how they are manufactured, their quality, and how they influence the success of organizations.

HOW DATA AND INFORMATION HAVE BECOME THE MOST IMPORTANT ASSETS OF THE 21ST CENTURY

When you think of the most significant innovation drivers in the 20th century, one of them is surely information technology (IT). IT has fundamentally changed how organizations do business and has revolutionized both product offerings and processes. Think, for example, of the level of automation in manufacturing today, where computer-controlled robot arms have replaced human work, or the digitalization of services, which has led to the emergence of companies like Amazon, Facebook, and Google. In recent years, we have seen IT assets increasingly turn into a commodity (similar to, for example, electricity and water), to such a degree that they are in many cases relatively insignificant in terms of competitive advantage. However, IT has provided the foundation for the rise of another type of resource, which has become central from a strategic point of view: information.

There are two major trends that brought us to the Information Age, and made information a central resource in the 21st century. The first is the massive abundance of information due to the rise of the capabilities and the decreasing costs of IT over the last few decades. Today, information can be automatically captured with technologies like sensors and radio-frequency identification (RFID), efficiently processed using large computer systems, and accessed at any time and place via the Internet. The retailer Wal-Mart, alone, processes one million customer transactions every hour—that is, 2.5 petabytes (*The Economist*, 2010)—that can be used, for instance, to analyze customer behaviors in ways that have not been possible before.

Of course, this is not exclusive to Wal-Mart. Large IT vendors such as IBM, having recognized the potential that organizations can leverage from all this data, have strategically aligned themselves for a future of Big Data (see, for instance, <http://www-01.ibm.com/software/data/bigdata/>). The degree of automation that is possible when it comes to managing large quantities of data and information is constantly advancing. Today, we are living in the middle of what has been defined as the Information Age. Nearly every aspect of private and corporate life can and often is captured,

processed, and exchanged digitally using personal computers, mobile devices, cameras, microphones, and other types of sensors, radio-frequency identification, Internet, e-commerce applications, social networking, emails, enterprise applications, and corporate and public databases. Potentially, every piece of information, wherever it may reside, could be accessed from any place within seconds. It can be automatically analyzed and combined to provide higher-level insights. Big Data is a resource that we not only have to protect, but also utilize in a way that is most beneficial for society.

The second major trend is the globalization of all economies, which puts organizations under constantly increasing pressure to adapt, innovate, and speed up their processes to keep up with their competitors. Information, using the enormous capabilities of today's IT, can help companies to make better-informed timely decisions and innovate the business. In a world where almost everything can be outsourced to a cheaper supplier, information (and knowledge) are often the only remaining effective differentiators when no other traditional market barriers exist.

So, "Is data the new oil?" (see [Figure 1.1](#)), a question posed by Perry Rotella in an article for *Forbes.com*, a leading business magazine ([Rotella, 2012](#)), referring to a comparison first expressed by Clive Humby at the ANA Senior Marketer's Summit 2006 at Kellogg School of Management, and to Michael Palmer's blog post in which he wrote: "Data is just like crude. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc., to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value" ([Palmer, 2006](#)). Jer Thorp responded in a blog article for *Harvard Business Review*, in which he points out a very valid distinction between data and oil: "Information is the ultimate renewable resource. Any kind of data reserve that exists has not been lying in wait beneath the surface; data are being created, in vast quantities, every day. Finding value from data is much more a process of cultivation than it is one of extraction or refinement" ([Thorp, 2012](#)). To be more precise, we will take a closer look at what data and information assets actually are and the characteristics they possess.

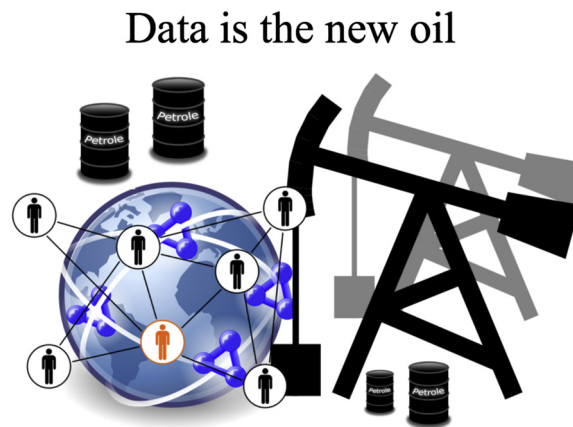


FIGURE 1.1

Is data the new oil?

WHAT ARE DATA AND INFORMATION ASSETS?

When data and information are important for the success of an organization, data and information become assets for the organization. Data and information assets can be in the form of structured, semi-structured, or unstructured data that is physically stored not only in computer systems, but also in paper records, drawings, photographs, etc. A data and information asset might even be something as simple as a regular phone call.



IMPORTANT

When data and information are important for the success of an organization, data and information become assets for the organization.



IMPORTANT

Data and information assets can be in the form of structured, semi-structured, or unstructured data; they can also be stored on mediums other than in a database, for example, on paper or even not stored at all (e.g., information given in a phone call).

Structured (electronic) data is data stored in tables in relationship or other types of databases. [Table 1.1](#) provides a summary description of different data types. Master data is probably one of the most valuable types of structured data; it contains more permanent information about important things such as customers (e.g., address data), suppliers (e.g., an evaluation of the suppliers), physical assets (e.g., pipelines, machines, facilities), products, and product parts (e.g., their materials and subparts).

A large volume of data is automatically collected in transactions about events that occur in the organization. Transactional data records the status of organizational transactions, such as product sales, and therefore this data type record can grow to become extremely large, and is highly volatile. Reference data is classification schemas and sets of values (e.g., country codes) that are referred to by other data types, which are important to make the usage of other data (e.g., master data or interoperable data). Metadata is data about data (e.g., field names, value types, field definitions, etc.). Much of the data today is historical data about transactions in the past that often need to be stored for compliance reasons, but that can also be used for data analysis.



IMPORTANT

Structured (electronic) data is data stored in tables in relationships or other types of databases (e.g., SQL database), while semi-structured data is stored in a less well-defined form (e.g., XML file). Unstructured data is the other extreme and has no predefined structure at all (e.g., JPEG picture file).

Table 1.1 Data Types

Data Type	Description
Master data	Master data is key business information about customers, suppliers, products, etc., and remains relatively static.
Transactional data	Transactional data describes events happening at a particular time and refers usually to one or more master or reference data elements. This data type is very volatile.
Historical data	Historical data is data about past transactions that often need to be retained for compliance purposes. Historical data may be saved in an obsolete format or in computer (legacy) systems, which can make them difficult to access and process in an organization. Historical data will also include master and transactional data.
Temporary data	When applications require additional memory in addition to the virtual memory available, temporary data is saved.
Reference data	Reference data is classification schemas and sets of values (e.g., country codes) provided by bodies external to the organization. It may also include internal classification schema and sets of values.
Business metadata	Business metadata is characterized by a lot of free text information describing business terms, key performance indicators (KPIs), etc. It can also contain business rules.
Technical metadata	This is structured data that describes objects such as tables, attributes, etc.; the database structure and technical rules are defined in this data type.
Operational metadata	Operational metadata describes operational characteristics happening in IT systems, such as the number of rows inserted by other software applications.

Semi-structured data can be, for example, XML or HTML files; this data type can predominantly be found on the Internet. Another example of semi-structured data is unstructured data, for instance, in the form of text processing, emails, and presentations saved on personal computers, mobile devices, and network storage systems, but also in hardcopy documents. Besides information from IT systems and documents, information also comes from communications among people who share their knowledge and observations, in both formal and informal ways. This information is not readily accessible because it is tacit, hidden in human brains. (The role of the discipline known as *knowledge management* seeks to make such tacit information more tangible—that is, explicit—or at least seeks to make knowledge-sharing mechanisms more effective.)

We do not make a distinction between data and information in this book. Of course, there is a difference between the two terms. But the problem is that it is very hard to draw a correct line between data and information. This is because there is no agreement on a clear definition of what information actually is, in the academic literature. A theoretical discussion of the most common definitions of data and information is presented in the following box.



ATTENTION

Data and information assets are not distinguished from each other in this book.



THEORETICAL EXCURSION: DATA VERSUS INFORMATION

There seems to be a general agreement that *data* can be defined as a symbol, sign, or raw fact (Mingers, 2006). Defining information is yet more difficult as Shannon, the thought-leader of information theory, points out: “The word ‘information’ has been given different meanings by various writers in the general field of information theory It is hardly to be expected that a single concept of information would satisfactorily account for the numerous possible applications of this general field” (Shannon, 1993).

Thus far, in the information systems (IS) discipline, there are two different definitions that dominate:

1. Information is “data that has been processed in some way to make it useful” (Mingers, 1996). This definition

of information implies that the concept of data is objective, which means “it has an existence and structure in itself, independent of an observer” and that information “can be objectively defined relatively to a particular task or decision” (Mingers, 1996).

2. “Information equals data plus meaning” (in a specific context) (Checkland and Scholes, 1990). This definition implies that information is subjective—dependent on the values, beliefs, and expectations of the observer—and as a consequence there can be different information created from the same piece of data.

A survey of 39 introductory IS texts indicates that the first definition seems to have wider acceptance (Lewis, 1993).

The unique characteristics of data and information assets

Data and information assets carry unique characteristics that make them different from traditional assets (Eaton and Bawden, 1991; Cleveland, 1985). Bear in mind though that there are exceptions to every rule. Still the observations give us some more insight about the characteristics of data and information assets.

One problem with data and information assets is that they are not easily quantifiable when compared to traditional goods. There are many approaches to valuing data and information assets (e.g., see Glazer, 1993); however, there are different opinions about which approaches are the best. Applying an approach often leads to inconsistent valuations when it is applied for a second or subsequent time. As a consequence, data and information assets are therefore not typically considered in financial accounting.



IMPORTANT

It is often difficult to measure the financial value of data and information assets consistently.

Data and information assets are usually transportable at ultra-high speed for a low cost. In an instant of a second, using a computer in London, one can access information from Wikipedia from a server that is based in San Francisco. Transporting a car from London to San Francisco will take much more effort, would cost more, and would take more time. In a way, this is a new development and has only been possible on a large scale since the advent of broadband Internet. The way our economies work today would not be imaginable without this development. Only the ultra-fast speed of communication allows an organization to become a globally integrated organization. Nobody is surprised anymore

when telephoning a call center that the caller on the other end of the line is based in a different country or different continent.



IMPORTANT

Data and information assets can be transported at ultra-high speed for a low cost.

Data and information assets often can be reused over and over again after initial consumption, without necessarily losing their value—with a few exceptions. When one uses a brick to build a house, one cannot use the same brick to build another house. The particular brick has already been used. Data and information assets behave very differently—they are sharable. They do not lose value when they get used per se. Let's take the example of a weather forecast. Just because somebody else has seen the weather forecast before you might have, it does not diminish its value to you. Nevertheless, there are situations in which one has an advantage when one's opponents do not have the same information. For instance, information that guides an investment might be worthless if everyone else has availability to the same information. Unlike physical goods, information usually has several life cycles, as it can be combined with other resources and there is no clear point of obsolescence. Data and information assets can still decay as they can get out of date and become less valuable.

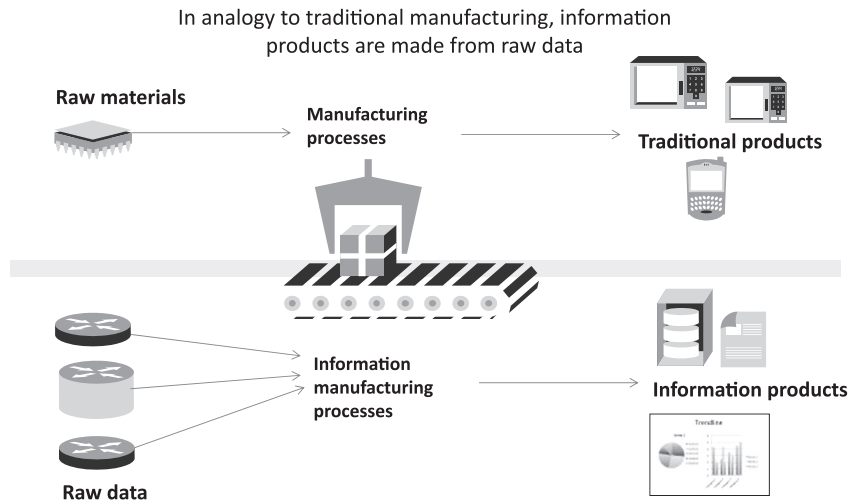


IMPORTANT

Data and information assets are reusable.

THE ANALOGY TO TRADITIONAL MANUFACTURING: HOW RAW DATA IS TRANSFORMED INTO INFORMATION PRODUCTS

The idea of an information manufacturing system was pioneered by Ballou, Wang, Pazer, and Tayi ([Ballou et al., 1998](#)). As in a traditional manufacturing system, in which manufacturing processes transform raw materials into products, an information manufacturing system transforms raw data (e.g., records in databases) into information products (e.g., a quarterly report) that are consumed by information users (e.g., shareholders). An illustration is shown in [Figure 1.2](#). The quality of the information product is dependent on both the quality of the raw data and the quality of the information manufacturing processes. Information manufacturing processes can be automated data processed by a computer, for example, age is calculated based on a consumer's birth date. It can also be manually processed by a human, such as, for instance, writing a report that scrutinizes the financial results of a company. Like physical economic goods, data and information assets can be a commodity, which are interchangeable with other commodities of the same type, or a good that is diversified ([Glazer, 1993](#)). Many concepts from traditional manufacturing, like quality management, can be transferred to information production using this analogy.

**FIGURE 1.2**

A comparison of traditional manufacturing to information manufacturing.



IMPORTANT

Similar to transformation processes in a traditional manufacturing system, information management processes can transform raw data into information products.

A number of practitioners and academics have advocated that data and information should be managed as a product similar to the ways in which physical products are managed. In particular, Wang and colleagues set four principles to succeed in treating information as a product instead of a by-product of a system (Wang et al., 1998). First, it is necessary to understand the needs of the customers, the information users. Second, information production has to be managed as a process with adequate quality controls, similar to those seen in traditional manufacturing. Third, information needs to be managed during its whole life cycle. And fourth, a new organizational role is required, the information product manager, who is responsible for the supplies of raw information, the production of information products, the safe storage and stewardship of data, and for the information consumers.

LIFE CYCLE OF DATA AND INFORMATION ASSETS

Considering data and information as a product, one can draw a parallel between the manufacture of a product and the manufacture of information. Like a product in its early life, information needs to be



IMPORTANT

The life-cycle stages of data and information assets can be summarized as:

- Capture/creation
- Organization
- Storage
- Processing
- Distribution
- Retrieval
- Usage
- Archiving
- Disposal

created, organized, and stored. To make use of information for analysis and decision making, it needs to be distributed to the relevant storage systems and retrieved from these storage systems. Processing may also occur before retrieval. Finally, at the end of the life of the information, it can be archived, if required, or deleted.

QUALITY OF DATA AND INFORMATION ASSETS

A new discipline emerged in the 1990s dealing explicitly with data and information quality management (e.g., see [Wang and Strong, 1996](#); [English, 1999](#)); it has its roots in the concepts of quality management, most prominently, quality control, quality assurance, and total quality management, being pioneered by the quality gurus W. E. [Deming \(1981\)](#), J. M. [Juran \(1988\)](#), and P. B. [Crosby \(1979\)](#). Quality management revolutionized the manufacturing industry in Japan and helped Japan's economy to its astonishing growth during the second part of the 20th century. Western manufacturing companies subsequently copied the quality management principles to catch up with the new competition emanating from Japan. The data and information quality discipline provides many valuable new concepts and techniques that can be used to manage the quality of data and information assets. Some of the most important concepts are discussed in the following sections.

What is data and information quality?

Not all data and information assets can provide data of the same amount of quality. In fact, most organizations suffer from information quality problems and are not able to support activities in the way they should. Data and information quality is defined as "the fitness for use of data and information" ([Wang and Strong, 1996](#)). This means that it is a user-centric concept and strongly depends on the context of usage. A data and information asset might be of high enough quality for one task, but the same data and information asset can be of low quality for a different task. For instance, a spelling error in the address might prevent a parcel being delivered to a customer and is therefore of poor quality for this task, while it can be good enough for the marketing department to perform a customer segmentation analysis.



IMPORTANT

Data and information quality is defined as the fitness for use of data and information. It is strongly dependent on the user and the context of usage. The terms *data quality* and *information quality* are usually used interchangeably.

In the data and information quality literature, the terms *data quality* and *information quality* are usually used synonymously and interchangeably, which as explained earlier, is also done in this book. It is noted though that “there is a tendency to use data quality to refer to technical issues and information quality to refer to nontechnical issues” ([Madnick et al., 2009](#)).

Different dimensions of data and information quality

Data and information quality are multidimensional concepts and go beyond accuracy, as illustrated in [Figure 1.3](#). In the following, we will give some examples of information quality dimensions and how they can be defined.



IMPORTANT

Data and information quality are multidimensional concepts.

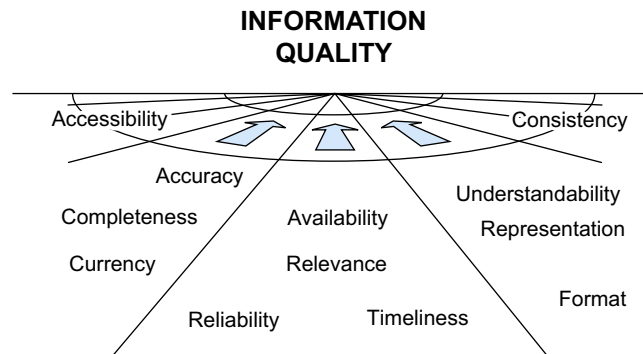


FIGURE 1.3

Data and information quality dimensions.



EXAMPLE DEFINITIONS OF DATA AND INFORMATION QUALITY DIMENSIONS

Accuracy: The extent to which data and information are correct, for instance, the values in a database correspond to the real-world values (e.g., the address data in the customer database does not correspond to the right address in the real world).

Completeness: Data and information have all the required parts of an entity's description (e.g., the attributes of a record are not null, or the zip code of a customer address is missing).

Consistency: Data and information have a consistent unit of measurement (e.g., some lengths of steel tubes are provided in centimeters and others in inches).

Timeliness: Extent to which data and information are sufficiently up to date for a task (e.g., the address used to be correct but the customer moved).

Interpretability: The extent to which data and information are sufficiently understandable for a task by the information user (e.g., the user manual is written in French and most users cannot understand it).

Conceptual frameworks for information quality give a systematic set of criteria for evaluation of information, help to analyze and solve information quality problems, and can be a basis for measurement and proactive management of information quality (Eppler and Wüting, 2000). Some examples of data and information quality frameworks are shown in the following box.



THEORETICAL EXCURSION: DATA AND INFORMATION QUALITY DIMENSIONS AND FRAMEWORKS

Many different frameworks have been proposed that provide different sets, categorizations, and definitions of information quality dimensions. Some examples are presented here.

In 1995, Goodhue investigated user evaluations of information systems and identified accuracy, reliability, currency, detail level, compatibility, meaning, and presentation as important information quality dimensions (Goodhue, 1995).

Maybe the most prominent example of an information quality framework was proposed by Wang and Strong in 1996, which defines four categories of information quality dimensions (Wang and Strong, 1996):

1. The *intrinsic information quality category* implies that information has quality in its own right and consists of the dimensions accuracy, precision, reliability, and freedom from bias.
2. The *contextual information quality category* highlights the requirement that information quality must be considered within the context of the task and includes the information quality dimensions importance, relevance, usefulness, informativeness, content, sufficiency, completeness, currency, and timeliness.

3. The *representational information quality category* concentrates on representational aspects with the dimensions understandability, readability, clarity, format, appearance, conciseness, uniqueness, and comparability.
4. The *accessibility information quality category* focuses on the ability of IT systems to store and access information and contains the dimensions usability, quantitateness, and convenience of access.

In 1996, Wand and Wang also developed an ontological approach to information quality, using the dimensions correctness, unambiguous, completeness, and meaningfulness. They claimed that dimensions could be assessed by comparing the values in a system to the true real-world values they represent (Wand and Wang, 1996).

Finally, Bovee and colleagues developed the AI1RI2 framework, which comprises the information quality dimensions accessibility, interpretability, relevance, and integrity (Bovee et al., 2003). They strongly criticized existing inconsistencies in Wang and Strong's 1996 framework.

Many more frameworks are proposed in the literature but there does not seem to be any agreement on a fixed set of dimensions (Batini et al., 2009). As there is no standard set of information quality dimensions, Lee and colleagues argued that it is essential for every organization to choose the most relevant information quality dimensions for their organization depending on the tasks that have to be performed (Lee et al., 2006).

Sources of poor data and information quality

A lot of the data and information are not in the right format, are inaccurate, incomplete, have a poor representation, are out of date, or suffer from other defects. The reasons for poor data and information quality are varied and diverse:

- Organizations have a large amount of legacy data that contains flaws.
- Many systems are not very well integrated and do not have the functionality that is actually required.
- Data is not maintained and kept up to date.
- Information collection is often seen as a side activity with not much relevance compared to other parts of the business processes in the organization.

The sources for poor data and information quality can be categorized into technological, organizational, and human factors (Figure 1.4).

Assessment of data and information quality

Data and information quality can be measured in two different ways. Subjective measurement is based on users' expectations. For instance, a survey of all users of an IT system might reveal that data in the IT system is often incorrect and not fit for use for the tasks that the information users perform. Objective measurement directly examines the data and information assets, for instance, by using data profiling algorithms (see Chapter 12). Information quality metrics are often calculated automatically;

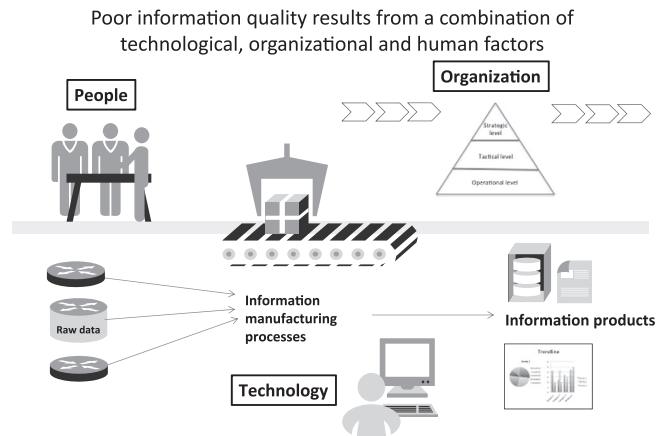


FIGURE 1.4

The sources of poor data and information quality.

information users have to provide rules that define what fitness for use means, giving due regard to both the considered task and the given metric.

Improvement of data and information quality

Improvement of data and information quality has to address the root causes of poor data and information quality. Therefore, this can cover a wide range of options, for instance, the redesign of data collection processes, the introduction of new IT systems, the enrichment of data with data from external sources, and the change of organizational culture and data responsibilities.



ACTION TIP

Data and information quality can be measured in two different ways: (1) subjectively, based on users' expectations, for example, by using a questionnaire, or (2) objectively, using defined information quality metrics.



ATTENTION

Data and information quality improvement has to address the root causes of the problems to be effective. There is a wide range of potential improvement activities, which are strongly dependent on the nature of the root causes.

HOW DATA AND INFORMATION ASSETS INFLUENCE ORGANIZATIONAL SUCCESS

One of the most important models in the information systems discipline is the Delone and McLean model for information system success ([Delone and McLean, 1992, 2003](#)), shown in [Figure 1.5](#). It

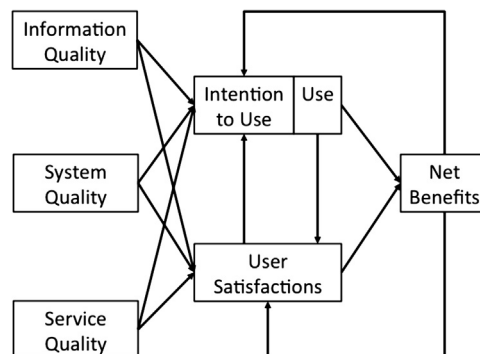


FIGURE 1.5

Updated Delone and McLean IS success model. (Source: [Delone and McLean, 2003](#).)

provides an insight into the key factors that explain why some organizations have better working information systems than other organizations. It is not all too surprising that information quality has been identified as being one of the few key determinants of business success of information systems.

A few years ago, we conducted research in conjunction with Dr. Markus Helfert, Lecturer at Dublin City University, and Dr. Mouzhi Ge, Adjunct Assistant Professor at Universitaet der Bundeswehr Munich, to understand, more explicitly, the role of information in the IS/IT business value chain (Borek et al., 2012). The model links IS/IT business value and information quality literature and shows how different elements of the value chain are interlinked from an information perspective. The developed model, which is illustrated in Figure 1.6, explains the IS/IT business value chain as follows. Information is manufactured and managed with the help of IS/IT capabilities that use a variety of IS/IT assets and complementary organizational assets. The quality of the resulting information products determines if IS/IT utilization can meet its purpose. It influences the business processes, the decision making, and ultimately the organizational performance. When information is manufactured and managed poorly,

Macro Environment (e.g. competition, market)

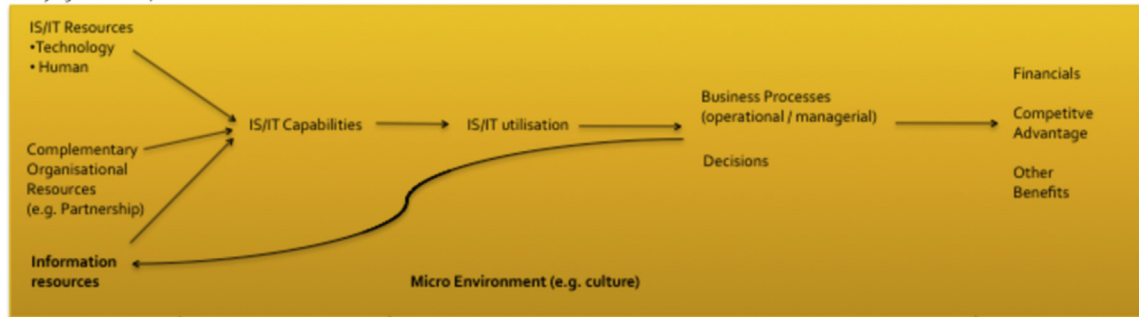
Information Perspective



What to explain



Underlying Relationship



Measure / Indicators



Related Concepts

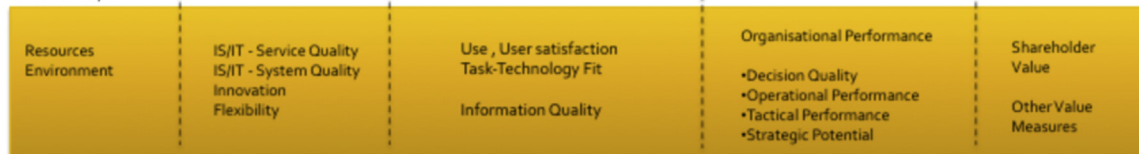


FIGURE 1.6

An information-oriented framework for relating IT assets and business value. (Source: Borek et al., 2012.)

it leads to poor information quality, which then further creates information risk, which can be both financial and nonfinancial.

Note that the relationship between information quality and the potential for information risk is not deterministic. This means that even though information is of poor quality, the effect on the business of using that poor-quality information will not necessarily be the same each time. Therefore, there is inherent uncertainty in the relationship between poor-quality data and information assets, and the impact they have on business outcomes.

How data and information quality influence decision making

Many studies provide evidence of the clear link between the level of data and information quality and organizational success. For instance, Slone finds empirical evidence for all four categories of the information quality dimensions of Wang and Strong's information quality framework—information soundness, dependability, usefulness, and usability—to have a significant effect on organizational outcomes (which he divides into strategic and transactional benefits) (Slone, 2006). Even more studies have shown the tremendous effect that data and information quality has on decision making (see the following box).



THEORETICAL EXCURSION: THE IMPACT OF DATA AND INFORMATION QUALITY ON DECISION MAKING

Findings in the literature provide evidence that information quality has a strong influence upon decision quality. Some of the works are described in more detail in the following commentary.

O'Reilly III discovered in a study with decision makers how perceived quality and accessibility influence the use of different information sources (e.g., written documents, internal group members, external sources) in tasks of varying complexity and uncertainty (O'Reilly III, 1982). He found that accessibility is the main driver for the use of an information source. Moreover, perceived information quality is also a critical factor for use of an information source; this is more important than the type of task or information source and personal attributes of the decision maker.

Keller and Staelin investigated the effects of quality and quantity of information on decision effectiveness of consumers in a three-phase job-choice experiment using second-year MBA students (Keller and Staelin, 1987). They conducted an experiment with four different levels of information quantity and four different levels of information quality. Their results indicate that increasing information quantity impairs decision effectiveness and, in contrast, increasing information quality improves decision effectiveness.

Ahituv and colleagues analyzed the effects of time pressure and information completeness on decision making in an experiment with military commanders with different levels of experience (mid-level field versus top strategic commanders) using a simulation of the Israeli Air Force (IAF) (Ahituv et al., 1998). The results show that complete information improves performance, yet less advanced commanders (as opposed to top strategic ones) did not improve their performance when presented with complete information under time pressure. Moreover, time pressure normally, but not always, had a negative effect on performance. Finally, higher-qualified subjects (top commanders) usually made fewer changes in previous decisions than less senior field commanders.

Chengalur-Smith and colleagues made an exploratory analysis of the impact of data quality information on decision making (Chengalur-Smith et al., 1999). They found that the subjects often ignored the information about data quality in their decision making and rather used it in the simple scenario when an interval scale was given compared to no data quality information, and seemed to not use it in the complex scenario, probably due to an information overload.

Raghunathan explored the relationship between information quality, decision-maker quality, and decision

Continued



THEORETICAL EXCURSION: THE IMPACT OF DATA AND INFORMATION QUALITY ON DECISION MAKING—cont'd

quality using a theoretic and simulation approach (Raghunathan, 1999). He concluded that information quality can have a positive effect on decision quality when a decision maker has knowledge about the relationship among problem variables, otherwise the effect can also be negative.

Fisher and colleagues investigated the effect of providing metadata about the quality of information used during decision making (Fisher et al., 2003). Their results indicate that the usefulness of metadata about information quality is positively correlated with the amount of experience of the decision maker.

Jung and colleagues conducted a study to explore the impact of representational data quality (which comprises the information quality dimensions interpretability, easy to understand, concise, and consistent representation) on decision effectiveness in a laboratory experiment with two tasks that have different levels of complexity (Jung et al., 2005). The results strongly support the hypothesis that a higher representational data

quality improves the decision-making performance regarding problem-solving accuracy and time.

Ge and Helfert presented a framework to measure the relationship between information quality and decision quality. They simulated the influence of two information quality dimensions—completeness and accuracy—in a simple yes or no decision scenario, in which they measured decision quality as the ratio of the number of right decisions in relation to the number of total decisions. Their results suggest that poor information quality can mislead decision makers and can be even worse than no information at all (Ge and Helfert, 2006). Based on this work, Ge and Helfert found statistically significant results that show the improvement of information quality in the intrinsic category (e.g., accuracy) and in the contextual category (e.g., completeness) enhance decision quality (Ge and Helfert, 2008).

Altogether, there is strong evidence that data sets with poor information quality can substantially affect the outcomes of decision making.

Organizational costs and impacts of data and information quality

Some groundwork in laying out how poor data and information quality impacts the business has been established by three pioneers in information quality: Larry English, Tom Redman, and David Loshin.

Larry English identified three types of costs—process failure costs, information scrap and rework costs, and lost and missed opportunity costs—as the major costs that are caused by poor information quality (English, 1999). Process failure costs are those that occur when a process does not perform properly; this encompasses irrecoverable costs (e.g., costs of mailing a catalog twice to the same person), liability and exposure costs, and recovery costs of unhappy customers. Information scrap (marking as an error) and rework (cleansing) costs occur when information is defective and can include a number of costs such as redundant data.

Tom Redman identified a list of impacts of information quality on the organization at three different organizational levels: operational, tactical, and strategic (see Table 1.2; Redman, 1998). Some of the impacts are tangible (e.g., reduced customer satisfaction, increased cost, ineffective decision making, reduced ability to make and execute strategy), whereas others are intangible (e.g., lower employee morale, organizational mistrust, difficulties in aligning the enterprise, issues of ownership/politics).

A list of impacts is also given by David Loshin (2010) in Table 1.3. There are four major categories of impact identified: financial impact, confidence and satisfaction, productivity, and risk and compliance. Each of the categories has a number of subcategories, which are shown in the table, and many

Table 1.2 Classification of Information Quality Business Impacts

Operational Impacts	Tactical Impacts	Strategic Impacts
Lowered customer satisfaction	Poorer decision making; poorer decisions that take longer to make	More difficult to set strategy
Increased cost: 8–12% of revenue in the few, carefully studied cases; for service organizations, 40–60% of expenses	More difficult to implement data warehouses	More difficult to execute strategy
Lowered employee satisfaction	More difficult to reengineer Increased organizational mistrust	Contribute to issues of data ownership Compromise ability to align organizations Divert management attention

Source: [Redman, 1998](#).

Table 1.3 Classification of Information Quality Business Impacts

Category	Subcategories
Financial	■ Direct operating expenses ■ General overhead ■ Staff overhead ■ Fees and charges ■ Cost of goods sold ■ Revenue ■ Cash flow ■ Depreciation ■ Capitalization ■ Leakage
Confidence and satisfaction	■ Forecasting ■ Reporting ■ Customer satisfaction ■ Employee satisfaction
Productivity	■ Workloads ■ Throughput ■ Output quality ■ Supply chain
Risk and compliance	■ Regulatory ■ Industry ■ Safety ■ Market ■ Financial ■ System ■ Credit/underwriting ■ Legal

Source: [Loshin, 2010](#).

examples for each subcategory are given in the book. It is emphasized that this list is not inclusive and strategies are provided for organizations to iteratively refine the impact list to better fit their application domain and industry.

WHY WE NEED BETTER METHODS TO UNDERSTAND AND MEASURE THE IMPACT OF DATA AND INFORMATION QUALITY

Many practitioners complain that they struggle to understand and measure the impact of poor data and information quality. They, therefore, have trouble building believable business cases for investments in data and information asset quality. When data and information assets are of poor quality, it is likely that something will go wrong, but it does not have an impact every time; the impact occurs only with a certain likelihood. This makes it even more complicated to measure the impact. Tom Redman emphasized in his keynote speech at the International Conference on Information Quality in November 2011 that assessing the business impact of information quality is still one of the big unsolved research problems for the data and information quality discipline. The assessment of the business impact of poor data and information quality is currently only a side element to data and information quality methodologies (many do not assess it at all). As we are living in a world of restrained assets, we believe that this puts the wrong emphasis on the dominant data and information quality improvement approaches. The methodology in this book is an attempt to shift information quality management into being more value driven and better aligned with business goals and strategy. We are convinced that understanding where data and information assets create the biggest pain points or where they can provide the biggest opportunities is a cornerstone to a more value-driven enterprise information management program in your organization.

REFERENCES

- Ahituv, N., Igbaria, M., & Sella, A. (1998). The Effects of Time Pressure and Completeness of Information on Decision Making. *Journal of Management Information Systems*, 15(2), 153–172.
- Ballou, D., Wang, R., Pazer, H., & Kumar, G. (1998). Modeling Information Manufacturing Systems to Determine Information Product Quality. *Management Science*, 44(4), 462–484.
- Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009). Methodologies for Data Quality Assessment and Improvement. *ACM Computing Surveys (CSUR)*, 41(3).
- Borek, A., Helfert, M., Ge, M., & Parlikad, A. K. (2012). IS/IT Resources and Business Value: Operationalization of an Information-Oriented Framework. Enterprise Information Systems 13th International Conference, ICEIS 2011, Beijing, China, June 8–11, 2011, Revised Selected Papers. Vol. 102. Lecture Notes in Business Information Processing. Berlin: Springer.
- Bovee, M., Srivastava, R. P., & Mak, B. (2003). A Conceptual Framework and Belief-function Approach to Assessing Overall Information Quality. *International Journal of Intelligent Systems*, 18(1), 51–74.
- Checkland, P., & Scholes, J. (1990). *Soft Systems Methodology in Action*. New York: John Wiley and Sons.
- Chengalur-Smith, I. N., Ballou, D. P., & Pazer, H. L. (1999). The Impact of Data Quality Information on Decision Making: An Exploratory Analysis. *IEEE Transactions on Knowledge and Data Engineering*, 11(6), 853–864.
- Cleveland, H. (1985). The Twilight of Hierarchy: Speculations on the Global Information Society. *Public Administration Review*, 45(1), 185–195.
- Crosby, P. B. (1979). *Quality Is Free*. New York: McGraw-Hill.
- Deming, W. E. (1981). *Management of Statistical Techniques for Quality and Productivity*. New York: New York University, Graduate School of Business.

- Delone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research*, 3(1), 60–95.
- Delone, W. H., & McLean, E. R. The Delone and McLean Model of Information Systems Success: A Ten-year Update. *Journal of Management Information Systems* 19(4), 9–30.
- Eaton, J. J., & Bauden, D. (1991). What Kind of Resource Is Information. *International Journal of Information Management*, 11(2), 156–165.
- Economist. *Data, Data Everywhere—A Special Report on Managing Information*. available at, <http://www.economist.com/node/15557443>. 2010.
- Eppler, M. J., & Wittig, D. (2000). Conceptualizing Information Quality: A Review of Information Quality Frameworks from the Last Ten Years. *Proceedings of 5th International Conference on Information Quality (ICIQ 2000)*. MIT, Cambridge, MA, USA. October 20–22 2000.
- English, L. P. (1999). *Improving Data Warehouse and Business Information Quality: Methods for Reducing Costs and Increasing Profits*. New York: John Wiley and Sons.
- Fisher, C. W., Chengalur-Smith, I. S., & Ballou, D. P. (2003). The Impact of Experience and Time on the Use of Data Quality Information in Decision Making. *Information Systems Research*, 14(2), 170–188.
- Ge, M., & Helfert, M. (2006). A Framework to Assess Decision Quality Using Information Quality Dimensions. *Proceedings of the 11th International Conference on Information Quality—ICIQ*, 6, 10–12.
- Ge, M., & Helfert, M. (2008). Effects of Information Quality on Inventory Management. *International Journal of Information Quality*, 2(2), 177–191.
- Glazer, R. (1993). Measuring the Value of Information: The Information-intensive Organization. *IBM Systems Journal*, 32(1), 99–110.
- Goodhue, D. L. (1995). Understanding User Evaluations of Information Systems. *Management Science*, 41(12), 1827–1844.
- Jung, W., Olfman, L., Ryan, T., & T Park, Y. (2005). An Experimental Study of the Effects of Representational Data Quality on Decision Performance. *AMCIS 2005 Proceedings*, 298.
- Juran, J. M. (1988). *Quality Control Handbook* (4th ed.). New York: McGraw-Hill.
- Keller, K. L., & Staelin, R. (1987). Effects of Quality and Quantity of Information on Decision Effectiveness. *The Journal of Consumer Research*, 14(2), 200–213.
- Lee, Y. W., Pipino, L. L., Funk, J. D., & Wang, R. Y. (2006). *Journey to Data Quality*. Cambridge, MA: MIT Press.
- Lewis, P. J. (1993). Linking Soft Systems Methodology with Data-focused Information Systems Development. *Information Systems Journal*, 3(3), 169–186.
- Loshin, D. (2010). *The Practitioner's Guide to Data Quality Improvement*. San Francisco: Morgan Kaufmann.
- Madnick, S. E., Wang, R. Y., Lee, Y. W., & Zhu, H. (2009). Overview and Framework for Data and Information Quality Research. *Journal of Data and Information Quality (JDIQ)*, 1(1), 1–22.
- Mingers, J. (2006). *Realizing Systems Thinking: Knowledge and Action in Management Science*. Berlin: Springer.
- Mingers, J. (1996). An Evaluation of Theories of Information with Regard to the Semantic and Pragmatic Aspects of Information Systems. *Systemic Practice and Action Research*, 9(3), 187–209.
- O'Reilly, C. A., III (1982). Variations in Decision Makers' Use of Information Sources: The Impact of Quality and Accessibility of Information. *Academy of Management Journal*, 25(4), 756–771.
- Palmer, M. (2006). "Data Is the New Oil," available at, http://ana.blogs.com/maestros/2006/11/data_is_the_new.html.
- Raghunathan, S. (1999). Impact of Information Quality and Decision-maker Quality on Decision Quality: A Theoretical Model and Simulation Analysis. *Decision Support Systems*, 26(4), 275–286.
- Redman, T. C. (1998). The Impact of Poor Data Quality on the Typical Enterprise. *Communications of the ACM*, 41(2), 79–82.
- Rotella, P. (2012). *Is Data the New Oil?* available at, <http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/>.
- Shannon, C. E. (1993). The Lattice Theory of Information. In N. J. A. Sloane & A. D. Wyner (Eds.), *Claude Elwood Shannon: Collected Papers* (pp. 180). New York: IEEE Press, Institute of Electrical and Electronics Engineers.

- Slone, J. P. (2006). *Information Quality Strategy: An Empirical Investigation of the Relationship Between Information Quality Improvements and Organizational Outcomes*. Doctoral Thesis, Minneapolis: Capella University.
- Thorp, J. (2012). *Big Data Is Not the New Oil*. available at, http://blogs.hbr.org/cs/2012/11/data_humans_and_the_new_oil.html.
- Wand, Y., & Wang, R. Y. (1996). Anchoring Data Quality Dimensions in Ontological Foundations. *Communications of the ACM*, 39(11), 95.
- Wang, R. Y., Lee, Y. W., Pipino, L. L., & Strong, D. M. (1998). Manage Your Information as a Product. *Sloan Management Review*, 39, 95–105.
- Wang, R. Y., & Strong, D. M. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*, 12(4), 33.

Enterprise Information Management

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to set up EIM governance
- Things to be considered when creating a strategy for EIM
- What the different components of EIM are that should be considered
- How Big Data and other challenges create new pressures for EIM

WHAT IS ENTERPRISE INFORMATION MANAGEMENT?

Enterprise information management (EIM) is the organizational-wide management of information in a coordinated framework of disciplines. Information management is the management of the processes and systems that create, acquire, organize, store, distribute, and use information with the goal of helping people and organizations access, process, and use information efficiently and effectively (Detlor, 2010). David Marco, a leading data management practitioner, defines EIM as “systematic processes and governance procedures for applications, processes, data, and technology at a holistic enterprise perspective” (Marco, 2012). The orchestration of the multitude of disciplines requires a unified governance approach and strategy, which are illustrated in Figure 2.1.

After describing EIM governance and EIM strategy, subsections A to J describe some of the components of EIM; this is not meant to be an exhaustive list, but rather highlights the diversity of different aspects that need to be considered as part of EIM.



IMPORTANT

EIM is the organizational-wide management of the processes and systems that create, acquire, organize, store, distribute, and use information with the goal of helping people and organizations access, process, and use information efficiently and effectively.

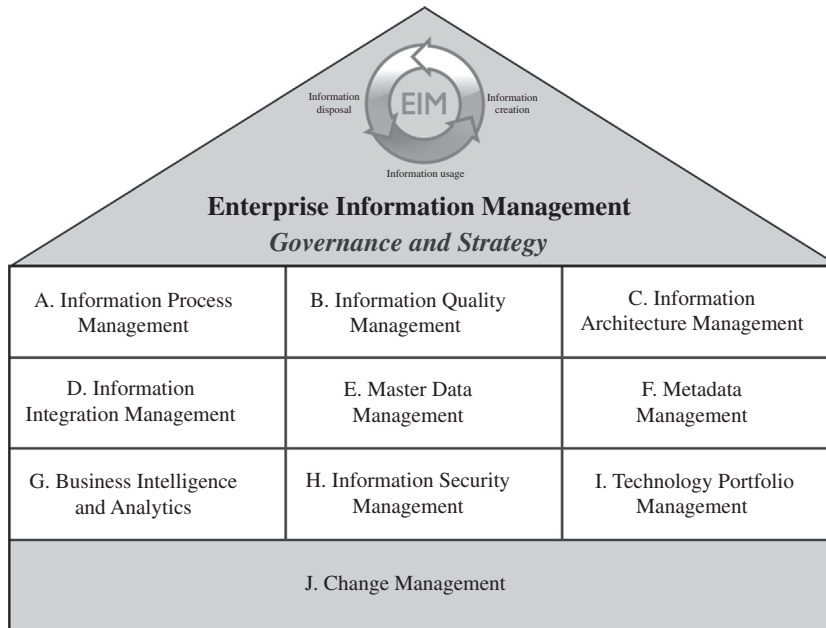


FIGURE 2.1
Key components for EIM.



ATTENTION

EIM is an interdisciplinary framework. This means that many parts of EIM overlap with other organizational functions. EIM efforts usually have to be coordinated across the different individual business functions.

EIM governance

EIM governance includes all the issues that arise from the need to manage, protect, control, and report information. The benefits accruing from good enterprise-wide information governance include:

- Being confident that the foundation upon which activities are undertaken is based on information that is accurate, up to date, and complete.
- Having the right information, in the right place, at the right time, available to the right people in the right format, which in turn facilitates faster decision making and execution of the right actions.
- Employees have the best information available to them making them more effective in discharging their responsibilities.
- Establishing and maintaining a reputation for reliability and openness in transactions with all stakeholders.
- The organization does not leave itself exposed to claims of information malpractice.
- Being confident that the organization has met its obligations in terms of compliance needs and can confidently withstand any challenges made in this regard.

Good EIM governance can and does lead to enhanced stakeholder experience. It can also help with innovation and expansion policy. Benefits will vary from organization to organization and you may identify other areas where your particular organization can benefit from having good information governance. Information governance does not seek to stifle operations; on the contrary, it seeks to enhance them.

John Ladley defines the following critical success factors for information governance ([Ladley, 2012](#)):

- Is mandatory for the successful implementation of any project or initiative that uses information.
- Has to explicitly show business value.
- Requires the management of organizational culture change.
- Is an enterprise effort.

One of the most important parts of EIM governance is to create the information policy for an organization. An information policy will provide a set of guidelines within which work processes are performed. It will ensure that all employees know the parameters and boundaries for, among other things, the effective management of information risk. Once the information policy has been developed, then the EIM strategy will articulate how the policy is to be put in effect. This will include internal control procedures for information risk management.



IMPORTANT

Information policy is an overarching statement setting out *why* information management is mission critical to the organization and how it sits within a wider organizational expression of objectives.

Once developed within the organization, the information policy needs to gain not only acceptance but commitment as well. Employee commitment is vital, because without it, the information policy will not gain traction and it will not take its rightful place in organizational activity. This could lead to significant risk. The engagement of employees should be achieved by involving them in discussions about the impact on individual roles and by clarifying what is expected of them to fulfill the policy.

When the information policy has been agreed on, the next step is to develop the EIM strategy that will enable implementation of the policy. This means turning the policies into objectives, targets, milestones, and specific actions, and this is where information governance starts. Strategy implementation may be challenging, and it should not be underestimated. Communication is key but should not be too directional—employees always respond to new ways of working if they feel they have been able to contribute to the debate and their voice has been heard. Build consensus by presenting employees with opportunities and conditions for change. That said, bear in mind that the



ACTION TIP

The information policy should be clear, concise, and realistic, and provide employees with a framework upon which they can build and develop skills that enable them (and consequently also the business) to compete effectively in a rapidly changing environment.

debate needs to be balanced with fulfilling business objectives. The level of empowerment/debate should be appropriate to both an organization and an employee's role.

Neither the EIM governance policy nor the EIM strategy should be left unchecked for more than six months. As highlighted previously, the information economy is subject to rapid change. Any business should scan the horizon on a regular basis to find new ways to remain alive to the impact of changes that may have occurred in its current sphere of operations. Information policy and strategy should be flexible enough to respond to any significant changes whether they are internal or external, or indeed a combination of both.

EIM strategy

EIM strategy is the approach that an organization takes to orchestrate its technology, organization, and people to build and sustain the organization's information management capability. It basically sets the goals and approach for EIM governance. EIM should be derived from and closely aligned to the corporate business strategy and business objectives.



IMPORTANT

EIM strategy is the approach that an organization takes to orchestrate its technology, organization, and people to build and sustain the organization's information management capability.

Sometimes information strategy can influence business strategy as it might have the potential to transform the business to increase competitive advantage. EIM strategy consists of three parts:

1. Technology strategy, which is the approach to manage the IT infrastructure.
2. Systems, which are the information systems and surrounding business processes.
3. Content, which is the information contained in the systems.

The ultimate goal is the creation of an information-enabled enterprise that is driven by information in all its core activities, which can lead to a sustainable competitive advantage in the market. EIM strategy goes far beyond technological issues, incorporating aspects such as strategic management, globalization, change management, and human/cultural issues ([Galliers and Leidner, 2009](#)). EIM strategy has to coordinate a number of different disciplines, which are explored in the following sections.

A. Information process management

In Chapter 1, the concept of the life cycle of data and information assets was introduced. Data and information assets need to be created, organized and stored, processed, accessed and used, and, at the end of their life, archived or deleted. Different business units in their day-to-day operations will carry out the processes associated with these stages. In some cases, for example, they may share the responsibility of collecting and storing information. Information process management is the stage of ensuring the effective management of all these processes throughout the organization so that not only is the right information delivered to the business units, but also it is available at the right time in the business process.

If you consider the different business processes that are carried out in an organization (e.g., preparing a product for dispatch to the customer), parts of these processes will intersect with the information processes. Focusing on information processes is like viewing the business processes through a filter that shows only the activities related to information. Managers can therefore direct their attention toward determining whether the required information is being provided at the relevant stages of the business process. Typical questions include:

- Is the right information being captured?
- Is the information being distributed to the systems that need it?
- Can the users get access to the information when they need it?
- Is the correct information being identified for archiving and deletion?



IMPORTANT

Information process management ensures the effective management of all the processes throughout the life cycle of data and information assets.

To ensure that the information processes deliver what is needed, the quality of the information and how this is affected by the different transformations (e.g., processing and distribution of information) needs to be considered.

B. Information quality management

Information quality management (IQM) is concerned with the question of how to sustain information that is fit for all user needs throughout the organization. This implies that in places where information does not meet user requirements, information quality improvement actions have to be initiated. Therefore, a major part of IQM is understanding what and why information is deficient and bringing it up to the required quality level. These activities are typically referred to as information quality assessment and information quality improvement.



IMPORTANT

IQM ensures that data and information assets are fit for use for all information user groups. Assessing data and information quality and then initiating changes to improve deficiencies in quality will achieve this aim.

One of the first data and information quality methodologies was Total Data Quality Management (TDQM) (Wang et al., 1998). Wang and colleagues define a TDQM cycle, which consists of four steps: define, measure, analyze, and improve. An information quality methodology can be data or process driven, can concentrate on assessment or improvement, and may follow a special purpose or a general purpose. A majority of information quality assessment techniques support only structured (i.e., in databases) or semi-structured (e.g., XML-formatted data) data but are not suitable for unstructured data,

such as presentation slides or word-processed documents. The assessment of information quality can be partly automated with existing software tools like data profiling that include column analysis, matching algorithms, and semantic profiling (see Chapter 12). However, there are limitations with regard to what problems these methods are able to detect.



ACTION TIP

Data quality software tools can often help assess the quality of data and information assets.

Information quality improvement uses the outputs of the assessment phase to determine what data needs to be improved and by how much. It may still be possible to operate with data that is not 100% accurate, and therefore the data should only be improved to the level that is needed to operate effectively. Additional

resources, time, and effort that are required to improve the data further would be wasted if other key data is waiting to be improved to satisfactory levels. In the long term, and when priorities dictate, organizations can strive for full fitness for purpose of all data and information assets.

C. Information architecture management

With multiple information systems at the organization's disposal and many informational demands from people in various business units, the problem of how to organize and lay out the assortment of systems is critical for effective working. It is not unlike the problems that architects of physical buildings aim to solve in that information architecture is about where the information should be placed and how the different pieces fit together.

In a hotel, where a bathroom is being shared by multiple bedrooms, the architect (hopefully!) places the bathroom where everyone who needs it can get easy access without disturbing others—usually, at the end of the hall. If the architect places the bathroom in one of the bedrooms, then the unlucky person who books the room with the communal bathroom will face unwelcome interruptions by those who want to use the bathroom.

Analogous problems and constraints are faced by the information architect, who must place the information needed by multiple parties in a place where it is easily accessible to those people. There are, however, usually many constraints that dictate factors, such as the size and location of information systems and how they can be connected. The information architecture needs to find the right balance between these constraints while satisfying user needs.



IMPORTANT

Information architecture management creates the blueprint for the design of the interaction among the different organizational information systems; it also provides recommendations to general EIM based on the insights generated from the blueprint.

At the more detailed level within each information system, the data must be arranged efficiently and effectively. Data modeling covers how the data will be arranged in the system, and by far the most common structure is the relational model (as evidenced by its use in numerous databases).

In this model the process of normalization is used to ensure that a structure is produced that ensures, for example, that data updates are propagated correctly and data redundancy is removed or mitigated.

Given the blueprint for the design of the interaction between the different organizational information systems and the data models, there are technical challenges regarding how best to integrate the information from one system to another.

D. Information integration management

Cast your mind back to the days when an organization only had one information system. Based on the efficiencies and potential that this system offered, it was not long before other departments in the organization followed suit and introduced their own systems; this brought with it the new technical challenge of how to share and merge the data between these systems. What is needed in this case is for the information from one system to be correctly integrated into the information in another system so that the users can access the new information seamlessly.

Information integration is needed in numerous different scenarios:

- Application consolidation (combining two or more information systems into one)
- Replacement of legacy systems (moving the data to the new system)
- Finding new uses for the data (moving the data to the new system)
- Archiving and moving data to a place where future analysis can be performed (a common destination is a data warehouse)
- Batch/continuous transfer of information between systems (to keep overlapping systems synchronized)

While information integration is needed for numerous applications, it is not an easy task, and the key challenges stem from the differences in syntax, semantics, and structure of the information.

Examples of syntax differences relate to data fields that may contain abbreviated values in one system and not in another, values that are formatted differently (e.g., U.S. and U.K. date formats), and telephone numbers that contain the area code in one system and omit the area code in another system.

Semantic differences are exemplified by data values that inadvertently change meaning when transferred to another system. For example, this can occur when each system references countries via different codes—in one system the United States could be allocated the code 1 and the United Kingdom the code 2, and in another system these could be reversed. Any data that is transferred between these systems that does not take this semantic difference into account will reference the wrong country.

Differences in data structures between the systems can occur, for example, where the field names and data types (e.g., text or numerical) for data values differ; the data values for a customer may be in a single row in one table in the destination system, whereas in the originating system, those values may be dispersed between different tables, and the originating source may hold data in an unstructured way; the latter would need to be given the relevant structure before it is integrated.

These challenges provide many opportunities to introduce errors into the data when transferring it to another system, and therefore close attention to any reduction in information quality is needed during

the integration process. It is not surprising, therefore, that organizations often take the chance during information integration to attempt to actually improve the quality of the data in the original system and clean up any problems before the data is loaded into the new system.

The general process of information integration involves extracting the information from the originating system, analyzing it, and making the necessary transformations. These activities are key to ensuring that information quality is not reduced during information integration before the transformed data is then loaded into the target system. This is commonly referred to as *extract, transform, and load* (ETL).

The loading process changes are dependent on the data type in the target system. For example, with data such as customer records, it would not be desirable to append multiple records of the same customer to the target system. The loading process needs to ensure that only a single customer record is retained. Whereas in the case of historical data, it may be desirable to append similar-looking records to facilitate temporal analysis.

E. Master data management

Certain data, such as customer records, are central to an organization and are utilized by multiple departments. Each department may have its own system that references the customer record. Master data management covers the procedures that are needed to handle this type of key organizational data to ensure that it is managed correctly and that each user has access to it when needed. The main challenge with master data is the detection and removal of duplicate records (e.g., customer names). Effective master data management should not allow different users of the systems to make changes to one customer record while disseminating a different customer record to other departments (or even the same department).

Master data management solutions to duplicate records involve either ensuring the correct synchronization between duplicates by ensuring that any data updates are propagated to the other identical record(s) or removing the duplicates altogether. Over the years, a significant amount of effort has gone into duplicate detection and removal, which is also known as identity resolution, the merge-purge problem, record linkage, etc. These techniques often involve comparing the records to determine whether the values are similar and then classifying two records as a match, nonmatch, or unknown. In the latter case, it is often necessary for human users to review and make the final decision as to whether the records refer to the same entity.

F. Metadata management

Metadata is data about data. Metadata management is about proposing, reviewing, agreeing to, endorsing, facilitating the observance of, rewarding compliance with, and managing metadata policies. Policies consist of a concept, a context, and a process. There are different types and layers of metadata:

- Business definitions of metadata include concepts, business terms, definitions, and semantics of data.
- Reference metadata includes conceptual domains, value domains, reference tables, and mapping. Data elements metadata includes critical data elements, data elements definitions, data formats, and aliases/synonyms.

- Information architecture metadata includes entity models, relational tables, and master object directory.
- Data governance metadata includes information usage, information quality, information quality service-level agreements (SLAs), and access controls.
- Services metadata includes service directory, service users, and interfaces.
- Business metadata includes business policies, information policies, and business rules.
- Metadata policies need to analyze, identify, document, and harmonize definitions and put shared repositories into place.

Another task area is providing naming standards for data (e.g., “PersonLastName”, “OrderMonthlyTotalAmount”), which can improve syntactical and semantic consistency, reduce lexical complexity, and help employ a controlled vocabulary. Furthermore, data model standards have to be designed for data elements (e.g., data element names, types, representations, formats, and entity modeling standards), which can include master data domains and standards attributes. Part of the activity process should also discover existing metadata (i.e., data values, business rules, and object relationships) and make it explicit. Data standards need to be harmonized into one coherent policy document that everyone in the organization has to comply with. A core aim should be to educate the rest of the organization that this policy document exists and how they can comply with it. Moreover, data and business rules are defined with due consideration to the business policy and context.

Metadata can support information integration across the enterprise, standardize the use of information, simplify data management, and make master data management consistent. It can, therefore, enable and improve effective business intelligence. Difficulties in metadata management appear because data policies are often defined but not enforced and complied with in practice.



ATTENTION

Many organizations neglect the importance of metadata. An enterprise-wide approach to metadata management is essential, otherwise all other EIM efforts may be jeopardized.

G. Business intelligence and analytics

Business intelligence has the goal of providing decision makers with timely and actionable business insights. The term refers to the capability of the organization to transform its information into useful knowledge. Business intelligence is often implemented using a data warehouse that can hold vast amounts of information, primed for various types of analysis.

Business analytics builds on business intelligence solutions and involves analyzing and interpreting organizational data with advanced methods (e.g., statistical analysis and data mining) to improve decision making and optimize business processes. When large data sets are analyzed, the notion of Big Data analytics is frequently used and often builds on new technologies, such as Hadoop, to enable the analysis of these large data sets.

**IMPORTANT**

Business intelligence has the goal of providing decision makers with timely and actionable business insights, often in the form of a data warehouse. Business analytics involves analyzing and interpreting organizational data with advanced methods (e.g., statistical analysis and data mining).

Since a successful business intelligence and analytics project can directly drive the success of core business activities, it is usually considered a strategic investment. To succeed, besides using new technology, business analytics projects usually require a change in organizational mindset as well as the up-skilling of employees in analytics and in the use of new technologies.

Data analysis, reporting, and query tools are all part of business intelligence and can help to deal with the volume of data. Although traditionally business intelligence is usually tightly connected to data warehousing, there are attempts to transform business intelligence by linking it with service-oriented architectures that can provide data from the furthest corners of the business.

With the significant effort that organizations invest in maintaining and analyzing their key data, another very important area in EIM is keeping this information secure.

H. Information security management

All organizations hold some information that is private to them and they would not want people external to the organization to gain access to, especially their competitors. Besides business secrets, organizations may be under obligations to protect parts of their information from public consumption, such as private customer information; the Data Protection Act in the United Kingdom is an example of regulations that can require this kind of protection. Information security is concerned with the practice of protecting this information from unauthorized access, use, disclosure, modification, or destruction.

Access to information within organizational information systems is granted (or withheld) by the access control mechanisms. Most of us are familiar with the process of logging into our computers with a username and password; this is a form of access control authentication. Authentication is used by the system to verify your identity—that is, determine that you are who you say you are. Once your identity has been established, the process of authorization is used to ensure that you only have access to the information in the system that you should have access to. Not all users should have access to all the information within a system, and a typical example is with military information. Depending on the value of the information, it is assigned different levels of classification from top secret to unclassified. The access control mechanism ensures that only those people who are cleared to see top-secret information can do so. This is referred to as mandatory access control. Most organizations use a slightly more convenient model called role-based access control where access to information resources is granted based on the role that the user performs within the organization.

Incorrect operation of access control can have consequences on data quality. For instance, if the access control mechanism unnecessarily withholds data from the users, then this affects the accessibility of the data, and the users may be forced to make decisions without all the necessary data. There is a constant trade-off between making the data accessible to the users and keeping it secure: to make the information in a system completely secure, you simply withhold all information from everyone, and to make the information accessible, you simply release everything. Clearly, most organizations need to find a balance between these two extremes.

I. Technology portfolio management

Data and information rely heavily on the support of information technology, which includes hardware, middleware (e.g., databases and server management programs), and software applications. The introduction of a new IT system is often very expensive and requires a lot of effort. As a number of IT projects are often run simultaneously, the technology portfolio has to be managed in a unified manner. Many organizations face challenges in evaluating IT investments in terms of costs and benefits as part of the investment decisions, since it is very difficult to identify all changes that will be attributable to the IT investment, and it is even more difficult to understand how to measure the changes in terms of value. The main benefits of IT investments typically include an enhancement of the business architecture and an improvement of business processes. Information risk management can provide important input to IT project portfolio management and planning. Technological changes are often needed to address data and information quality problems.

J. Change management

Most data and information management projects require changes in the organization, which is one of the most difficult things to do as humans are naturally resistant to change. The success of a strategy and a project is strongly dependent on the capability of the management to mobilize their employees to follow the strategy and the changes outlined in the project. Change management is an art of its own, with many excellent books written on the topic. It requires some basic knowledge of the theory of change management and a lot of practical experience in dealing with human psychology and the politics in an organization. Chapter 13 addresses these important “softer” factors of EIM.

BIG DATA AND HOW IT REQUIRES NEW THINKING IN EIM

We have discussed how the amount of data that is captured and stored is growing exponentially. Never before has so much data been available about so many different things. Data can be captured in all parts of real life by ubiquitous computing systems armed with different types of wireless sensors, data logs, cameras, mobile devices, GPS, microphones, or RFID tags (to name a few). In 2009, the data available on the web reached 500 billion gigabytes, and it is expanding fast day by day. At the time of writing, over 600 million people around the world are sharing information about their social life on platforms like Facebook, Google Plus, and Twitter. Scientific experiments have a growing need for computing capacity as they try to find unexpected patterns and interpret evidence in very large data sets. An example of the latter is provided in the following case study.

CASE STUDY: BIG DATA AT THE WORLD'S LARGEST EXPERIMENT

At CERN, the European Organization for Nuclear Research, the world's largest multinational science experiments take place in the Large Hadron Collider (LHC). These experiments aim to provide answers to fundamental questions about our universe. In very recent times the Higgs Boson particle was discovered at CERN, which has often been referred to as the "God particle" by the media, as it enables answers to be given to many important questions raised about the universe. Twenty European nations are currently members in the large experiments taking place in the LHC. CERN has its own farm of 10,000 servers plus an international network of over 150 data centers around the world. The data network processes 300,000 MB per second of experimental data that describes events happening in the accelerator tunnel as part of the ATLAS experiments. Due to limited storage capacity, of the 300,000, only 300 MB can actually be saved, thus decisions in real time have to be made about which event

data is actually saved. This requires very efficient selection algorithms that evaluate these events. Per year, 15 million gigabytes of data are saved in over 10 data centers across Europe, which are further processed and analyzed by the 150+ data centers. In parallel to the experiments, Monte Carlo simulations are run that simulate what the theory predicts will happen in the accelerator to enable comparison with what actually happens. This allows the testing of existing theories about high-energy particles, matter, antimatter, and our universe. Currently, CERN is evaluating if cloud computing could be used in the future, in addition to the existing grid of data centers, to form something that is referred to as the science cloud. CERN is only one example of how the volume of data is growing and the challenges that arise from this.

(Jones, 2012)



ACTION TIP

There are two simple but important rules for Big Data strategy:

1. You have to know what you want to get out of the data and information assets.
2. You have to know where data and information quality have to be improved so you are really able to get what you need out of your data and information assets.

Additionally, concepts such as cloud and mobile computing are emerging as potentially game-changing paradigms. Many real-world activities require interactions between humans and computers, and these occur in an online environment where a lot of data about these interactions is stored. When data sets become too big to handle, new methods are required for capturing, storage, retrieval, sharing, analysis, and visualization; these set new requirements for effective information management.

EIM is at a crossroads because we are entering a new era, the era of Big Data, in which many data sets are becoming too big to be managed with conventional

database management tools. Big Data has become a fashionable buzzword these days. It typically refers to the three V's of data: volume, variety, and velocity. In organizational management, Big Data is understood to be the challenge that is set by these large data sets that in turn leads to a requirement to develop a new strategy in information management. Traditionally, data has often been stored and processed without too much thought about what it is actually needed for, or for a primary purpose. However, other secondary usages have not always been taken into consideration (e.g., data that is collected in a sales process for accounting purposes) might also be of significance to make marketing decisions. Organizations have to rethink their approaches if they want to succeed in the era of Big Data. Because there is so much

data and information available, it is necessary to have a plan. You have to know what you want to get out of the data and information assets. Moreover, data and information quality is often not good enough, but it is simply impossible to improve the large volumes of diverse information and data. You have to know where data and information quality is most important for your business and have a clear focus.

FURTHER CHALLENGES FOR EIM

Besides Big Data there are many other changes that arise from technology, politics, society, and business that impact EIM and present new challenges. Some of the challenges are discussed in the following sections.

Globalization as a challenge and driver for better EIM

Friedman analyzed in his bestseller *The World Is Flat: A Brief History of the Twenty-First Century* how our world has recently become more closely connected as globalization has penetrated all parts of the economy (Friedman, 2007). Politically, there are fewer boundaries for international economic activities after the end of the Cold War, symbolized by the fall of the Berlin Wall. Technically, the rise of the Internet made information accessible and software-enabled organizations could collaborate in real time all over the world. Many products became digital, and can now be delivered to customers in the blink of an eye—most noticeably music (iTunes instead of CDs), magazines, and books (Amazon's Kindle replaces your newsstand and corner bookstore). A lot of economic activities are outsourced to third parties or offshored to new company sites to markets with cheaper labor. A typical manufacturing company often manufactures its products in production sites on more than one continent. It is also supplied with parts and materials by a net of suppliers spanning the globe. Customers are similarly distributed internationally. Increasing globalization sets high demands for information management in organizations. With this panorama, it becomes difficult and complex to orchestrate the supply chain and customer sales and delivery. Providing real-time high-quality information about what is happening locally in different sites of an organization and in the supply-chain network is not only helpful but essential. Consequently, being able to understand the different needs of customers that are globally distributed also sets new challenges for effective EIM.

Customers becoming more demanding

Customers become more demanding because they know that you actually have the information that is needed to fulfill their needs. Customers understand the possibilities that come with the Internet and increasingly sophisticated IT systems, as they are users of such systems themselves. Twenty years ago, a customer would have been much more understanding if he could not get an answer to his or her question about which shop of a retail store chain a particular product could be found in. Today, it is seen as something basic—that is, information about what is going on in a business is available at one click within seconds. Their customers increasingly perceive organizations that cannot provide timely information as being incompetent. Treacey and Wiersema identified customer intimacy as a third strategic way for competitive advantage besides product leadership and cost leadership, in a very influential *Harvard Business Review* article (Treacey and Wiersema, 1993). Customer intimacy is the capability to understand customers and react to their changing needs in a very responsive and flexible

manner; Big Data is a key enabler of this. Operational intelligence is not something that you can do, it is something that is expected by your customers because they know that it is possible.

Social networks and media

Within a few years, the Web 2.0 could see over half a billion people using social network platforms like Facebook, MySpace, LinkedIn, or Friendster on a daily basis to communicate with their friends, colleagues, and business contacts. In the first phase of the web, mostly factual information was shared among users. Today, a large proportion of information contains social information around private and professional lives—feelings and emotions, photos and videos, and things that people “like.” This large amount of data adds a new dimension to understanding your customers. Social data can be used to complement existing customer relationship management (CRM) corporate data to get a greater understanding of customers. It can enable very powerful marketing analytics. For instance, Twitter data can reveal what customers think about the organization, its products, and service, as well as provide an understanding of which issues affect its reputation. Another popular example is Facebook and LinkedIn data, which can give a richer picture about customers and customer segments, their social network, and their personal preferences. It is important for organizations to tap into this new rich source of personal information without offending their customers and employees.

Growing complexity in enterprise information architectures

When organizations are global, information needs to be shared globally. Different information systems have to be able to communicate with one another across time and geographical boundaries. The numbers of different IT systems, databases, and applications have grown significantly over the past few decades. In many organizations, the IT systems form a labyrinth that no one individual can fully oversee. The IT systems landscape has grown historically without an architecture that has been planned—the architecture simply just emerged. It is like starting the construction of a property without having an architect to design and oversee the development. Moreover, many systems are poorly integrated and are frequently unable to communicate with each other. Each application and database uses its own terminology, formats, and semantics. These matters are further complicated by the cultural environment in the function within which the system is administered and used, as well as its geographical location. IT departments often struggle to get an overview and to manage the systems consistently and effectively. Therefore, reducing the complexity and simplifying IT in a way that it becomes manageable again is one of the major challenges in today's workplace.

The burden of legacy data and systems

Closely related to this growing complexity is the challenge posed by legacy data and systems that are still required in a business but do not comply with today's standards. It can be very hard to replace the systems and migrate the data. For instance, approaches to data capture and data models change over time, but the data that has initially been captured according to these methods and models cannot be recaptured again. One has to live with this burden from the past. However, organizations need to control and mitigate the risks that come from these legacy systems and data.

The Internet of Things

"The Internet of Things" is a buzz phrase coined by researchers at the Auto-ID Center initiated by the Massachusetts Institute of Technology to describe the increasing digitalization of the real world (Gershenfeld et al., 2004). We will see sensors and chips being integrated more and more often into our "normal", meaning nondigital, life. For example, a refrigerator will become more intelligent in the future: it will know what food and drink it contains, when the "consume by" date expires, and which items are running low on stock. A car will know which replacement parts it needs automatically. Our own health could be monitored using sensors and chips strapped to our bodies. Many great opportunities will arise from this trend, but it will almost certainly lead to a new debate on consumer information privacy. Only if consumers trust the systems will they be willing to use them.

Leveraging IT for enterprise-wide transformation

Many new opportunities will arise through enhanced innovative technology. IT investments with innovative and rule-changing characteristics can transform an enterprise as a whole. Organizations have to identify their potential for radical transformation of their business processes. These improvements are not step-by-step improvements, but rather disruptive changes. Organizations need to make themselves ready for transformation; this is an important organizational capability that has to be developed over time. Change is challenging for most people, so effective leadership is key.

Poor alignment of business and IT

Traditionally, the culture in IT departments differs from that seen in other business functions. IT has an interfacing role because its main function is to support core business processes. However, employees who work in the IT department are often more interested in the technology and software than in the business processes supported by such. On the other hand, many business users do not willingly participate in IT projects if they do not have to, because it is a distraction from their day-to-day duties. The environment of the IT department often challenges them due to the lack of legitimacy, multiplicity of stakeholders, and pressures from strategy and financial control. As a consequence, often IT is poorly aligned with the business functions it supports and with the overall business strategies. Approaches such as information architecture management have been developed to improve the alignment between business and IT.

The movement toward the analytical and fact-driven enterprise

A data-driven culture is important for information management success. A metaphorical brick wall to an information-enabled enterprise is that management does not often demand the use of data-driven decisions. McCormack and Trkman draw upon an example of a hotel chain where the use of self-made simple spreadsheet analytics leads to lower employee efficiency because employees spend more time executing a task to make an analytical decision (McCormack and Trkman, 2012). However, this could conversely lead to better results for the organization. The employees stopped applying the analytics because the management did not recognize the value of it and perceived the analytics as a waste time.

The same decision can be made by gut feeling, using an Excel calculation or advanced business analytics, leading most often to better outcomes. Very often management does not push for data-driven

decisions. Similarly to the described case, it is sometimes even measured as employee inefficiency because employees need longer to undertake the analytics to reach a better decision. When value is not measured, there is no incentive to look for more analytical decisions.

SUMMARY

This chapter introduced key components of enterprise information management, commenting on current trends and challenges. EIM is the enterprise-wide coordinated management of data and information assets throughout their life cycle. Big Data and other major shifts, such as the globalization of all economies, the advents of social media, and “the Internet of things,” are placing new pressures on EIM.

REFERENCES

- Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009). Methodologies for Data Quality Assessment and Improvement. *ACM Computing Surveys (CSUR)*, 41(3), 16.
- Detlor, B. (2010). Information Management. *International Journal of Information Management*, 30(2), 103–108.
- Friedman, T. L. (2007). *The World Is Flat: The Globalized World in the Twenty-first Century* (2nd ed.). New York: Penguin Books.
- Galliers, R. D., & Leidner, D. E. (Eds.). (2009). *Strategic Information Management: Challenges and Strategies in Managing Information Systems* (4th ed). London: Routledge.
- Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things. *Scientific American*, 291(4), 76–81.
- Jones, B. (2012). *Big Data at CERN*. Barcelona: Keynote at the European Conference on Information Systems (ECIS 2012).
- Ladley, J. (2012). *Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program* (1st ed.). San Francisco: Morgan Kaufmann.
- Marco, D. (2012). *The First 11 Steps to Starting a World-Class Enterprise Data Stewardship and Governance Program*. San Diego: Tutorial at the Data Governance and Information Quality Conference (DGIQ).
- McCormack, K., & Trkman, P. (2012). *Business Analytics and Information Processing Needs: A Case Study*. Barcelona: European Conference on Information Systems.
- Pascale, R. T., & Athos, A. G. (1981). *The Art of Japanese Management* (Vol. 24.6). New York: Penguin Books.
- Treacy, M., & Wiersema, F. (1993). Customer Intimacy and Other Value Disciplines. *Harvard Business Review*, 71, 84–84.
- Wang, R. Y., Lee, Y. W., Pipino, L. L., & Strong, D. M. (1998). Manage Your Information as a Product. *Sloan Management Review*, 39, 95–105.

How Data and Information Create Risk

WHAT YOU WILL LEARN IN THIS CHAPTER:

- An introduction to the anatomy of information risks
- The sources of information risk
- Ways to mitigate information risk
- The upside of information risk
- Why quantifying information risk is worth the effort
- How risk management can help to improve EIM

INTRODUCTION

Information is increasingly becoming an extremely valuable asset in organizations. The dependence on information increases as it becomes more valuable. As value and dependence increase, so does the likelihood of risk. Information risk in this book is defined as the risk that arises from not having the right information of the required quality for a business activity available at the right time. Let's give you a few examples. If data regarding customer orders is not clearly and accurately captured, your ability to meet the orders at the required quality, quantity, cost, and time will be compromised. If you do not implement long-term strategic management of your physical assets, it can lead to asset failure and production or service loss (e.g., in a power or water network), compromise health and safety, or create environmental, regulatory, and compliance risks. If you are unaware of current market trends, you might invest in the wrong direction, make the wrong acquisitions, and develop the wrong strategies. It is not an exaggeration to claim that information has an important input to most organizational activities. It drives the decisions that we make on a daily basis at all levels of an organization. Therefore, when information is not managed and utilized properly, it can lead to countless risks all over the business. These risks may not always be new risks, however, information can be a key constituent of risks and their mitigation.

In many organizations, lack of data is often not the problem; indeed, the sheer volume of "legacy" data and information available on the web can in itself be quite overwhelming. The issue is how to capture the right data, of the right quality, and make it available to the right decision maker at the right time. Ensuring good data management practices and getting the quality of information right can be a key enabler of success. Many organizations have experienced the same issue: it is too easy to get lost in the overwhelming depth of data that is available, which makes it extremely difficult to choose the

right path—one that is closely aligned to the corporate and divisional business strategy—to overcome the obstacles created by poor information. Yet, in our world of constrained resources, it is simply not economically viable or timely to improve the quality of all information assets at the same time. Many activities aimed at improving the quality of information cost time and effort and can only succeed if resources are as targeted as possible to achieve the benefits. We have to prioritize wisely and decide what to prioritize (e.g., resources, activities, and/or information). For this, a thorough understanding of the risk arising from information is the principal key to success. This book will show you a practically proven way that can help you implement an effective information risk management program.

INTRODUCTION TO THE ANATOMY OF INFORMATION RISKS

To manage data and information risk, it is important to have an understanding of the way data and information impact an organization. Over the last few years, through consulting and researching with varied organizations across different business sectors, we analyzed hundreds of different data and information risks that we found in these organizations, and with all this material, we created a model that explains and helps to quantify these risks.

Figure 3.1 shows a high-level model of how information risk is created. As discussed in Chapter 2, information management is the organizational capability to manage technology, organization, and people cross-functionally to provide a high-quality level of information quality to all business users. To be successful in information management, for example, the right software tools need to be in place, data collection and processing processes have to be clearly defined, and all the other practices that good information management books teach you need to be promoted and implemented.



IMPORTANT

Poor EIM leads to data and information quality problems; this lowers business process performance and eventually leads to negative risks in organizations.

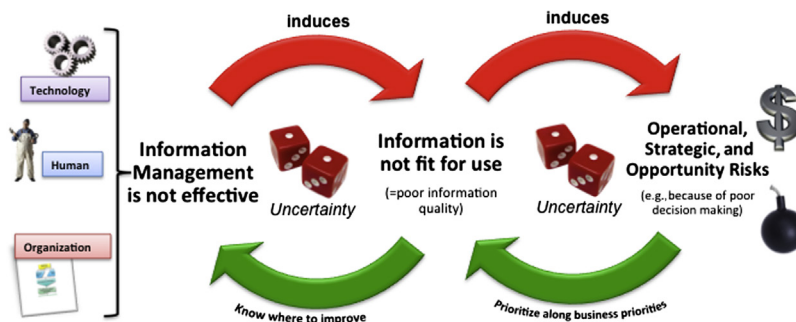


FIGURE 3.1

The anatomy of information risk. (Source: Based on Klassen et al., 2012.)

The consequence of ineffective information management is poor data and information quality

What happens when something does not work optimally in information management? It affects business users' experience of using information. When information processes are poorly defined and/or poorly implemented, then collected data may not be accurate or it may be ill-formatted or even not collected at all. These issues then create problems once the information needs to be used. When information quality is not monitored (e.g., when no business rules have been defined to check data), problems are not detected on time and they can adversely impact the business processes.

- An ill-defined information architecture can lead to information not being able to be exchanged between different software systems where needed.
- Poorly designed data models will make it more difficult to find the right information for users.
- Databases that are not fully integrated do not allow information to be combined where it makes business sense for that information to be combined. Therefore, you could create a situation where business users do not have access to the information they need to optimally run their business processes.
- A lack of high-quality business intelligence and analytics software leads to similar outcomes as those mentioned before.
- Missing metadata makes it more difficult to understand the context of the data and makes it more difficult to manage.
- Not providing well-defined access control to information can allow people to access data when they shouldn't be. Alternatively, rules that are not granular enough might prevent business users from being able to access critical information.
- Similarly, if employees do not follow data and business rules, it can also lead directly to data defects. Data and information that suffer from defects can be less fit for use.

The consequence of poor information quality is a lowered business process performance

As stated, ineffective information management leads to data defects and a lowered level of information quality. When information is inaccurate, incomplete, ill-formatted, inaccessible, insecure, difficult to understand, or simply unavailable, it is not fit for use and might create problems and lower the performance of business processes for which the information is critical or important. Take, for example, a call center agent who has to respond to a customer request. Not being able to explore the customer history with the company, or being provided with inaccurate information, makes it very likely that the agent will not be able to provide the high level of service that is expected by this customer. However, this does not necessarily always need to be the case. Let's assume that the address data of the customer making the telephone call is inaccurate in the database of the CRM system, as the zip code is incorrect. Only one-third of the calls might require just the address information. And maybe even fewer than one-third of customer queries really rely on having access to the correct zip code. When something is sent to a wrong zip code, it might still arrive at the right address, if the rest of the address information, such as the house number, street name and city, are correct. Therefore,

poor data and information quality can affect the performance of a business process. Yet, there is inherent uncertainty in the effects of information quality. The same information quality problem that leads to a business problem in one situation may not cause a business problem at all in a different situation.

Lowered business process performance creates operational, strategic, and opportunity risk

As we have previously shown, ineffective information management can cause information quality problems and lower business processes performance. This can eventually lead to increased organizational risk. When information is not fit for use in a business process, it can negatively affect many different business objectives as illustrated in Figure 3.2.

In the previous example of the call center, customers might not be served as well as desired. When the customer information record is inaccurate or incomplete, this might lower their satisfaction levels and could lead to fewer sales in the long term and therefore to poorer profitability. A company that tries to build its reputation and brand upon being very customer friendly might also have their corporate strategy compromised by such problems.

Moreover, if customers are telephoned with a sales pitch offering them a product that is unsuitable given their particular personal circumstances, then the call center agent's time is wasted; this will have a negative effect on operational efficiency. As before, the impact on business objectives is not deterministic, but in a case such as this, there is a likelihood that the business objective is actually affected by an information quality problem.

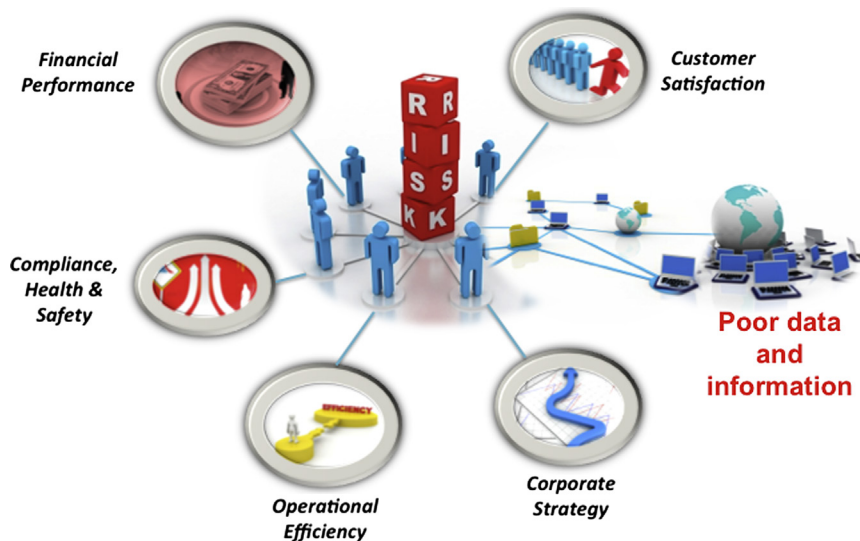


FIGURE 3.2

Poor data and information can affect many different objectives. (Source: jscreationzs / FreeDigitalPhotos.net.)

SOURCES OF INFORMATION RISK

Poor data quality can arise due to a variety of different reasons and sources, such as:

- Different types of systems in use
- Transfer of data between different (often incompatible) systems
- Accidental/intentional removal of data
- Improper data governance
- Lack of responsibility and authority for managing data
- Lack of awareness of value of information
- Lack of integration between IT and business processes
- Lack of training and motivation

A large amount of data has been collected over centuries using hand-based and computer-based systems. The average life cycle of an IT system is usually significantly shorter than the lifespan of the information it contains. Data that has been collected in the past often does not suffice and differs from today's data specifications and requirements, and is frequently inaccurate and incomplete. Data formats are often inconsistent and create difficulty when attempting to combine different data sources. Quality deteriorates, as often the data is not regularly maintained or updated. Data is often not considered a top priority for operational staff, but is rather a neglected side activity in the hectic day-to-day nature of operations.

Another reason for poor utilization of data and information assets is the lack of awareness of the value of data in an organization and how it can be used more effectively to drive business process performance. Many business processes rely heavily on managers' own experiences and gut feelings instead of being fact and information driven. Also, certain information usage habits are established once a business process matures, which are not changed without an internal or external impulse, even if there might be new or better ways to use the information to drive decisions in the process. Moreover, IT systems are often poorly integrated and usually not very well aligned to the true business needs. Historically grown, each department often has its own IT systems, its own data definitions, and its own terminology, which makes it hard to share data with other parts of the business. It is hard to convince managers to give up, voluntarily, some of their competencies. And, of course, in the Information Age, information means power, which prevents many people and business divisions from sharing information effectively. Finally, there is traditionally a wall of misunderstanding and miscommunication between the IT function and the rest of the business. The IT function has frequently to make assumptions about the IT users, which are often simply wrong or do not take the full situation into consideration.

DIFFERENT WAYS TO MITIGATE INFORMATION RISK

As we have seen, there are many metaphorical brick walls being hit that compromise the effective usage of information assets and cause risks in the business; however, there also are new opportunities in business and technology that have much to offer. In Chapter 2 we discussed the wide range of different components of EIM that span across multiple disciplines. All of these components of EIM can be used

to mitigate information risk. There is not only an increasing support for automated data quality assessment and the application of business rules in IT systems, but also for managing master data. Business intelligence technologies and data warehouses can combine data from different sources available in the enterprise.

An important recent development is the rise of the area of data and business analytics that aim to generate new insights from enterprise-wide data by using advanced data mining, statistics, visualization, and analytics tools. There is a clear trend in organizations to aim for more fact- and data-driven decisions, in operations as well as in corporate strategy. A rather novel development is *crowd sourcing*, a term coined by Jeff Howe of *Wired Magazine* in 2006. Drawing an analogy to computer-based computation, in the “cloud,” tasks that require human-based computing are outsourced to a “crowd.” This is a large human task force of Internet users who want to do the work for free because it is fun (games with purpose), or they want to support the work (e.g., users who write Wikipedia articles), or they are paid by the task-issuing party per task successfully completed on crowd-sourcing platforms like Amazon Mechanical Turk and Clickworker. There are many successful examples of crowd sourcing, including the classification of galaxies by Internet users, and it is a promising concept that has already proven to be useful for all sorts of human information processing.

THE UPSIDE OF INFORMATION RISK

Information risk also has a positive side to it: the opportunities that can be created. Your organization collects a lot of data every single day. Most of the data is stored in some kind of database and probably never used again. You should try to identify your hidden treasures in data and information. The basic approach is straightforward. Manage your data well so that it is of high quality, integrate your data, apply data analytics, and make your decisions more data driven to make them more successful, as suggested by Tom Davenport in his book *Competing on Analytics* ([Davenport et al., 2007](#)).

But where does information risk come into this? Understanding where information is not fit for use can help you to identify areas where you should focus on improving, using better information, or using information more effectively. It is hard to decide where to begin with data analytics as you have a lot of data and business processes that need data, so you should start where it creates the highest value—information risk management can help you with that. Wake up the unlimited opportunities that are sleeping in your databases. Knowing your customers better, and understanding your supply chain, products, shareholders, and competitors can give an edge to your business.

THE CASE FOR QUANTIFYING INFORMATION RISK

Do you need to quantify data and information risks? This is a legitimate question, because a lot of quantitative numbers need to be gathered to quantify information risk in a meaningful manner. You can save time and effort and just use a simple qualitative scale instead—for example, from 0 to 10 with 0 being no risk and 10 being very high risk. In some cases it can be the right thing to do, especially when reliable numbers for the probabilities and impact of risk cannot be obtained or where costs exceed the benefits of quantitative measurements. Hubbard, a widely acknowledged measurement

expert, who defines measurement as “a quantitatively expressed reduction of uncertainty based on one or more observations,” emphasizes, “the only valid basis to say that a measurement shouldn’t be made is that the cost of the measurement exceeds its benefits” (Hubbard, 2010).

In his book *How to Measure Anything: Finding the Value of Intangibles in Business*, Hubbard stresses that management loves quantitative measurements and he criticizes the use of purely qualitative scales for decision making in organizations (Hubbard, 2010):

One place I’ve seen this many times is in the “steering committees” that review proposed investments and decide which to accept or reject. The proposed investments may be related to IT, new product research and development, major real estate development, or advertising campaigns. In some cases, the committees were categorically rejecting any investment where the benefits were primarily “soft” ones. Important factors with names like “improved word-of-mouth advertising,” “reduced strategic risk,” or “premium brand positioning” were being ignored in the evaluation process because they were considered immeasurable. It’s not as if the idea was being rejected simply because the person proposing it hadn’t measured the benefit (a valid objection to a proposal); rather it was believed that the benefit couldn’t possibly be measured—ever. Consequently, some of the most important strategic proposals were being overlooked in favor of minor cost-savings ideas simply because everyone knew how to measure some things and didn’t know how to measure others. Equally disturbing, many major investments were approved with no basis for measuring whether they ever worked at all.

Hubbard also argues that taking quantitative measurements does not have to be too costly. We highly recommend the book to everyone who wants to understand the basics of quantitative measurement of intangibles such as information risk.

WHY RISK MANAGEMENT BECOMES IMPORTANT FOR INFORMATION MANAGEMENT

To summarize, data and information are powerful resources that you should utilize and care deeply about. Getting it right can provide you with almost endless new opportunities, but getting it wrong not only makes you miss out on these opportunities, but also creates risks all over your business that prevent you from performing well. Poor data and information assets can lead to operational and strategic risks in all of your business processes that are crucial to achieve the organization’s goals and objectives. There are a variety of techniques that you could use to improve the quality level of your data and information, as well as to increase the insights that you can gain for your business and eventually transform it into an information-driven enterprise. The problem lies in ensuring that you are making the right choice of techniques out of the mass available.

An extensive understanding of how information (with inadequate quality levels) can cause risks in your organization is crucial to ensure that the right IT investment decisions are made. Building information systems that can cope with various types of risks can cost a fortune, and it can take many years from the initial investment decision to the operationalization of the system. Data usually needs to be

migrated from legacy systems and this almost invariably involves high costs and risks. Many external services may be needed to introduce the system. Getting the wrong alignment to business needs in the planning stage of large IT systems is therefore an absolute no-go, something that most organizations simply cannot afford—financially, strategically, and culturally. Unfortunately, poorly planned IT investments do happen all too frequently.



IMPORTANT

Risk management methods should be applied to EIM to ensure the effective management of information risks.

Not everything can be planned and there will be always many risks involved in an IT project. However, a major reason for misguided investments is that business plans for IT systems and data quality projects are based on many general assumptions being made about what the business needs. Unfortunately, holding truth without a rigorous analysis of information risks does not often support such business needs. The most important inputs to such projects come from business users who undertake this endeavor only as a side activity in addition to their very demanding day-to-day occupation. Existing organizational processes do not allow business users to be sufficiently involved in the analysis of the business impact of data and information. Additionally, current methods that are available to undertake such an impact analysis are particularly weak and do not provide enough depth and structure.

There is a lot of cognitive bias on what people think about where and how information with inadequate quality levels affects their business. Well-structured methods for assessing information risk that deal with the inherent uncertainty in the relationship between information impact and business outcomes could help to overcome these biases. Such methods have, however, not yet been developed for a general-purpose usage. Fortunately, there is a whole discipline that can provide many helpful concepts, tools, and techniques to deal and manage the effect of uncertainty on business objectives: risk management, which we will introduce in the next chapter.

REFERENCES

- Davenport, T. H., & Harris, J. G. (2007). *Competing on Analytics: The New Science of Winning*. Cambridge, MA: Harvard Business School Press.
- Hubbard, D. W. (2010). *How to Measure Anything: Finding the Value of Intangibles in Business*. New York: John Wiley and Sons.
- Klassen, V., A. Borek, R. Kern, A. K. Parlikad. (2012). Quantifying the Business Impact of Information Quality: A Risk-Based Approach. European Conference on Information Systems, 11-13 June 2012. Barcelona, Spain.

Introduction to Enterprise Risk Management

WHAT YOU WILL LEARN IN THIS CHAPTER:

- What is risk and risk management
- What is a risk management process
- How to determine risk appetite and risk criteria
- How risk can be assessed and treated
- What is the role of chief risk officer

INTRODUCTION

To the best of our knowledge, this is one of the first books that shows, comprehensively, how well-established risk management methods can be applied to the relatively new discipline of information management to assess and understand the business impact of information and its quality. Additionally, we will demonstrate how the benefits of information risk treatment options can be systematically and rigorously evaluated based on a thorough information risk analysis. We will commence this journey by providing you with a brief introduction to the essentials of risk management.

WHAT IS RISK?

The International Organization for Standardization (ISO) in the ISO Guide 73 defines *risk* as the “effect of uncertainty on objectives” (ISO, 2009a).

Let’s digest this definition a little more by considering its individual elements and how they are defined in the *Oxford Dictionary* (<http://oxforddictionaries.com/>). First of all, risk is an effect, which the *Oxford Dictionary* defines as “a change, which is a result or consequence of an action or other cause.” So, a risk has to have a cause and it results in a change. If, for example, an individual smoke cigarettes, it increases the risk of lung cancer, which would certainly change his or her life if he or she were unfortunate enough to contract lung cancer.

The reason for a risk is uncertainty. Uncertainty is “the state of being uncertain.” Uncertain means “not able to be relied on; not known or definite.” Imagine that you would like to purchase a property in San Francisco, which is known for its susceptibility to earthquakes. You know that there is a risk of an earthquake occurring at any time, but you simply cannot say if there will be an earthquake during the next three years or not. It is uncertain.

And finally, this effect causes a change that has an impact on an objective. An objective is “a thing aimed at or sought; a goal.” In private life, that same individual may have an objective “to live a happy and healthy life.” Both an earthquake and contracting lung cancer would negatively impact the objective.



IMPORTANT

Risk is the effect of uncertainty on objectives ([ISO, 2009a](#)).

Risk can be negative or positive. Earthquakes and diseases are classic examples of negative risk. In contrast, when somebody plays roulette in a casino, he or she hopes for a positive risk. In a way, this is counterintuitive to the manner in which we use the word *risk* in our everyday language. We often talk about risk as something inherently bad, for example, health risks (e.g., smoking increases the risk of cancer), natural disasters like earthquakes and floods, and sudden economic downturns. But, in fact, the basis of our market economy is actually taking risks. A merger or takeover of a company is often pursued because the acquiring party expects that it is worth the price of acquisition because it anticipates that future financial returns will be favorable—this is positive risk taking.



IMPORTANT

An effect is a deviation from the expected—positive and/or negative ([ISO, 2009a](#)).

Risk can be measured, depending on its nature, using either a statistical approach that uses historical data or a subjective probability approach in an informed decision. Both approaches are frequently used in practice. When assessing risk, one has to keep in mind that risk is context-dependent since it reshapes when the system changes.

WHAT IS ENTERPRISE RISK MANAGEMENT?

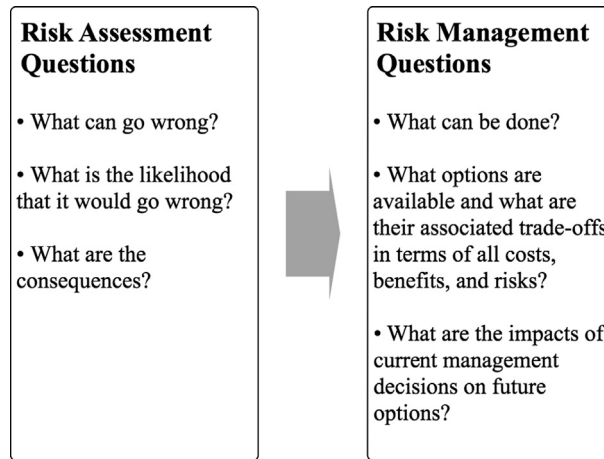
Enterprise Risk Management (ERM) is a relatively new discipline that requires “that an organization looks at all the risks that it faces across all of the operations that it undertakes” ([Hopkin, 2010](#)).

The ISO Guide 73 defines risk management as “coordinated activities to direct and control an organization with regard to risk” ([ISO, 2009a](#)). Risk management in an organization often has multiple objectives (e.g., high safety and low costs), which requires adequate modeling and optimization techniques that can take multiple objectives into account.



IMPORTANT

Risk management is a series of coordinated activities to direct and control an organization with regard to risk ([ISO, 2009a](#)).

**FIGURE 4.1**

Risk assessment and management questions. (Source: [Haimes, 2009](#).)

Haimes introduced the concept of total risk management, which he defines as “a systematic, statistically based, holistic view that builds on a formal risk assessment and management” ([Haimes, 2009](#)). Total risk management addresses four sources of failure:

1. Hardware failure
2. Software failure
3. Organizational failure
4. Human failure

Risk assessment and management questions that need to be addressed are shown in [Figure 4.1](#).



THEORETICAL EXCURSION: AN OVERVIEW OF RISK MANAGEMENT STANDARDS

There have been several risk management standards proposed in the literature, which are shown in [Table 4.1](#).

Table 4.1 Risk Management Standards

Standard	Description
CoCo(Criteria of Control)	Framework produced by the Canadian Institute of Chartered Accountants (1995)
Institute of Risk Management (IRM)	Standard produced jointly by AIRMIC, ALARM, and the IRM (2002)
Orange Book	Standard produced by HM Treasury of the U.K. government (2004)
COSO ERM	Framework produced by the Committee of Sponsoring Organizations of the Treadway Committee (2004)
Turnbull Report	Framework produced by the Financial Reporting Council (2005)
ISO 31000	Standard published by the International Standards Organization (2009)
British Standard BS 31100	Standard published by the British Standards Institution (2011)

Source: [Hopkin, 2010](#).

Continued



THEORETICAL EXCURSION: AN OVERVIEW OF RISK MANAGEMENT STANDARDS—con'd

A risk management standard consists of a risk management process together with a complementary risk management framework. Regarding the question as to which standard an organization should adopt, Hopkin gives the following advice: “Although some standards are better recognized than others, organizations should select the approach that is most relevant to their particular circumstances” (Hopkin, 2010). The key components of risk management standards are the risk management framework and process. Each standard is described in the following.

The CoCo (Criteria of Control) framework is a risk management standard that has been developed by the Canadian Institute of Chartered Accountants (Canadian Institute of Chartered Accountants, 1995). This framework follows a culture of risk awareness approach, in contrast to the risk management approach by ISO 31000, BS 31100, and IRM, and in contrast to the internal control approach developed by the COSO framework and Turnbull Report (1999).

The standard published by the IRM is a joint effort of the major risk management organizations in the United Kingdom: IRM, The Association of Insurance and Risk Managers (AIRMIC), The National Forum for Risk Management in the Public Sector (ALARM) (IRM, 2002). This framework provides a risk management terminology, process, and organizational structure and objective. As in the ISO 31000 standard, risk can be both upside and downside.

The Orange Book is a risk management standard for government organizations and has been developed by the HM Treasury of the U.K. government (HM Treasury, 2004). The standard comprises definitions, a comprehensive risk management model, and a clearly explained risk management process. It is

emphasized that risk management has to often go beyond the boundaries of an organization, since there are in any organization, a number of interdependencies with other organizational entities.

COSO ERM is an internal control framework for companies listed on the New York Stock Exchange; it is recognized by the Sarbanes–Oxley Act of 2002 (SOX), and as a result is the most used risk framework in the United States (Moeller, 2011). Key components of enterprise risk management are identified: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information, communication, and monitoring. The components do not form a serial process, but rather a multidirectional process.

The Turnbull Report, the official name of which is “Internal Control: Guidance for Directors on the Combined Code,” was created in 1999 with the London Stock Exchange for listed companies (Turnbull, 1999). It is an accepted alternative to the COSO ERM framework regarding Sarbanes–Oxley compliance.

ISO 31000 is a family of standards published by the International Standards Organization, which currently consists of the ISO Guide 73 “Risk Management—Vocabulary” (ISO, 2009a) that contains definitions for risk management terms; ISO 31000 “Risk Management—Principles and Guidelines” (ISO, 2009b) that contains guidelines for risk management and includes a risk management framework and process; and ISO 31010 “Risk Management—Risk Assessment Techniques” (ISO, 2009c) that summarizes established techniques for risk assessment.

Similar to ISO 31000, the standard BS 31100 published by the British Standards Institution proposes a risk management framework and process (British Standards Institution, 2011).

WHAT IS THE GENERIC RISK MANAGEMENT PROCESS?

A risk management process is the “systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, ... and reviewing risk” (ISO, 2009a).

Many different risk management processes have been proposed in the literature, which typically contain steps like: (1) identification of risks, (2) assessment/measurement of risks, (3) evaluation, choice, and

implementation of risk mitigation options, and (4) monitoring of risk mitigation. Risk management processes are often divided into the two main stages of assessing risk and treating risk.



IMPORTANT

A risk management process is a systematic process to assess and treat risks.

ASSESSMENT OF RISK

Risk management is concerned with ensuring that an organization recognizes and understands where weaknesses exist and/or where they might arise, and is proactive in addressing those to ensure that there is no adverse interruption to business continuity and/or damage to its reputation. An integral part is therefore the assessment of risk (ISO, 2009a):

- *Risk assessment* is the “overall process of risk identification, ... risk analysis, ... and risk evaluation.”
- *Risk identification* is the “process of finding, recognizing, and describing risks.”
- *Risk analysis* is the “process to comprehend the nature of risk ... and to determine the level of risk.”
- *Risk evaluation* is the “process of comparing the results of risk analysis ... with risk criteria ... to determine whether the risk ... and/or its magnitude is acceptable or tolerable.”

The starting place for organizations is to first identify the risks it faces, then monitor for risk, and develop policies and strategies for minimizing risk and planning for contingencies. Risk is managed through information and knowledge; knowing the inherent risks enables appropriate minimization policies and strategies, as well as early warning systems, to be designed.

There are different ways in which risk identification might take place. Typically, it will involve an internal assessment, ideally organization wide although some might wish to start in a specific (key) department where the risks are perceived to be the greatest. Some organizations might involve their auditors in such an exercise and others may call in external consultants to assist.

An organization that already has a good information and knowledge management strategy, where sharing information and knowledge is commonplace, will probably be more ready to identify risks than one where the concept of “information is power” prevails.

Involving employees at this early stage in the identification of risks will undoubtedly reap rewards. It is the people involved in the day-to-day operations who understand all the nuances of their operations who are normally best able to judge what is or is not a risk. That said, an external perspective is also good business practice as sometimes there is a danger that when an employee is working very closely with matters, he or she may not always have a clear appreciation of the risks involved in the day-to-day activities.



ACTION TIP

One of the key concepts in knowledge management is the custom of setting up communities of interest/practice to share knowledge, and these can be a very useful initiative to employ when thinking about ways in which to identify risk. Bringing together people who share a common interest to discuss and debate issues can produce invaluable insights and consider options upon which to move forward.

Table 4.2 Risk Allocation Matrix	
High impact/low occurrence	High impact/high occurrence
Low impact/low occurrence	High occurrence/low impact

Once risks have been identified, they should be analyzed in terms of their likelihood of occurrence and their impact. To some extent, the impact might be a quite subjective exercise. Perhaps one of the easiest ways in terms of thinking about impact is to think about it in association with the organization’s primary objectives; for example, in a commercial organization, what would the financial impact be? Another organization might focus on the cost of losing brand share or buyer/supplier relationships. Whatever method of evaluation is used, it should be consistent and clearly understood by all involved.

Consequently, risk has two important aspects:

- 1. Occurrence: think about the frequency—when will it occur? Daily, weekly, monthly, or annually?
- 2. Impact: will it be high, medium, or low?

Once these aspects have been calculated, we suggest that it might be a useful exercise to plot them on a matrix. After having plotted, the risks can be classified according to their impact into high, medium, or low categories. Table 4.2 (using a simple matrix) shows how risks are allocated: the high risk is the top right, low risk is the bottom left, and the two medium-level risks are top left and bottom right.

The risks have to be evaluated by comparing them to defined risk criteria. These criteria will differ from one organization to another and are closely linked to the risk appetite of the organization.

With the constantly changing environment, organizations should also be scanning the horizon on a regular basis to identify new risks.

There are many techniques available for risk assessment; a good overview is given in the ISO 31010 document (ISO, 2009c). They range from simple techniques like brainstorming and structured or semi-structured interviews to more sophisticated tools like fault tree analysis, Bayesian statistics, and Monte Carlo simulations. A thorough introduction to the more complex statistically based risk assessment tools is given by Haimes (2009). Chapter 11 of this book discusses how some of these risk assessment techniques can be used for managing information risks.

RISK APPETITE AND RISK CRITERIA

An important facet in managing risk effectively is to determine what your organization’s risk appetite is. Risk appetite is the amount of risk exposure, or potential adverse impact from an event/situation, that the organization is willing to accept/retain. Once an organization has established their risk appetite threshold, also called the risk criteria, if it is breached, risk management initiatives are prompted to bring the risk exposure back to an acceptable level.

In some instances, the risk levels will be high and in others a much more cautious stance will be taken. There will always be some risks that are unavoidable; in such cases you need to ensure that you have good contingency plans in place.



IMPORTANT

Only you can determine what level of risk you are willing to tolerate in a particular scenario. You should set the risk criteria based on your risk appetite.

There are no standard benchmarks for identifying what level of risk an organization should take; however, we hope that providing you with some guidelines in terms of questions that should be asked will help you to formulate your own risk appetite to the specific situations that might occur in your organization.

To help your organization determine its risk appetite and risk criteria, consider first the mapping that has already been done to determine occurrence and impact of risk and the assessment you have completed establishing whether it is a high, medium, or low risk, then consider the following questions:

- In which areas of risk should you prioritize your risk appetite? (Typically, this would be the areas you have already identified as high risk.)
- Where should you allocate your finite time and resources to minimize risk exposures? (Suggest that the high-risk areas are the ones to focus resources on.)
- Which risks do you consider need early attention to reduce the level of current exposure?
- What level of risk requires a formal response strategy to mitigate the potentially adverse impact?
- What level of risk requires escalation to a higher authority?
- How have you managed past events?
- What did you learn from earlier experiences?

TREATMENT OF RISK

Having identified and assessed the risks, the next stage is to decide how to treat those risks. Risk treatment (equivalent to risk response) is defined by ISO Guide 73 as the “process to modify risk” (ISO, 2009a). There are different ways described in the ISO Guide 73 as to how risk can be treated:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.
- Taking or increasing risk to pursue an opportunity.
- Removing the risk source.
- Changing the likelihood.
- Changing the consequences.
- Sharing the risk with another party or parties.
- Retaining the risk by informed decision.

Another popular easily recallable framework is the four T’s of hazard risk management: tolerate, treat, transfer, and terminate (Hopkin, 2010).

- *Tolerate (detective)* is basically the decision to do nothing, because no further action needs or can be taken—the risk is accepted and is further monitored.
- *Treat (corrective)* is acting upon the risk to control or reduce the risk (partially) and the frequent ways risks are addressed in an organization.
- *Transfer (directive)* means that the risk is shared or transferred completely to a third party (e.g., an insurance company) or by signing other types of contracts that transfer the risk.
- *Terminate (preventive)* is the option to stop the activities that lead to the risk.



EXAMPLE

Accept the Risk (Tolerate)

- Risk-taking is something that organizations often have to do to remain competitive, therefore, in some cases, decisions will be taken to accept these and absorb any losses. The same will apply in those situations where risks have not been identified and consequent loss occurs. In these types of circumstances there should be a contingency plan in place to address any adverse impact in the event that the risk becomes real.

Transfer the Risk (Transfer)

- Insuring against risk usually is the same as transferring the risk. Another method would be to share the risk with a third party (e.g., customers, suppliers, or subcontractors). Some insurance companies will lower premiums if they can see that there is a thorough risk management strategy in place. Organizations are legally obliged to seek cover for certain situations (e.g., employers' liability insurance, vehicles, etc.).

Reduce the Risk (Treat)

- The greatest number of risks will be treated in this way. This is where effective risk management comes into its own. Actions to reduce the risks to an acceptable level are set in motion. Examples include having backup staffing arrangements in the event of absence, maintaining equipment in good working order, installing automatic sprinkler systems, adhering to health and safety guidelines, keeping backup copies of computer software, building evacuation procedures, having contingency plans, working with pressure groups, etc.

Eliminate the Risk (Terminate)

- Some risks will only be managed effectively by eliminating them completely. This may not always be possible or indeed desirable; however, some risks in business operations may be so high that it is not judicious to proceed with them. Another way of eliminating some types of risks is to seek payments upfront.

CHIEF RISK OFFICER

With systematically high-profile corporate failures occurring with what seems like an alarming regularity, it is not at all unusual to see organizations in a wide range of industries appointing a chief risk officer (CRO). Traditionally, this position has been seen in sectors such as financial services and energy companies, however, recent years have witnessed the emergence of the CRO role in a growing range of industries. The CRO is responsible for formulating the information policies and information strategies associated with organization-wide risk management including information risk. The CRO is responsible for coordinating all risk management initiatives across the entire organization, guiding the organization's response to the increasingly regulated and legal environment, keeping the board of directors apprised of risk issues, ensuring that risks taken do not compromise business continuity, and guiding staff.

The CRO needs to be alert to what is happening in the wider environment and must monitor emergent risks that might impact on the organization and be proactive in developing

appropriate responses to such. It is not the CRO's responsibility to manage every risk in every part of the organization—accountability for management of risk lies collectively within the organization.

CROs come from a wide variety of organizational disciplines, for example, internal audit, finance, strategic planning, or legal. It is useful if the CRO has cross-functional expertise and an understanding of how the different parts of the organization fit together to form the whole. Having an overview of the risks facing the organization, having the authority to make change happen, being able to think strategically, having good analytical skills, and be able to influence activity across the organization are all key aspects of the role.

At first glance, the CRO role might seem to contradict the principle that risk management should be a collective responsibility; however, it is very helpful to have someone who steers matters, focuses on relevant activities, and coordinates initiatives that might otherwise be inefficient or even contradictory.

SUMMARY

Risk management is a well-established discipline that offers a number of publicly available and internationally recognized standards that are widely used in many organizations. Risk management standards usually consist of two main components. Risk management processes offer a structured, comprehensive, and standardized approach to manage risks, while risk management frameworks show how the risk management process can be integrated and used within an organization. Risk management processes can be divided into two main phases: *risk assessment*, in which risks are identified, analyzed, and evaluated, and *risk treatment*, which is about responding to the identified risks. There are many different tools that can be used for risk assessment; these range from simple tools to very sophisticated mathematical models. For example, risk management has been applied in the information systems discipline in two ways: (1) management of risks that result from IT malfunction, and (2) management of risks that arise from information security problems. A need to use risk management techniques for managing risks that arise from poor information quality has been identified, however, to our knowledge, there is currently no research available that shows how to apply risk management principles and tools to the information quality discipline.

Risk management, as a discipline in its own right, is moving higher up the business agenda. Tolerance for error in managing risk, from all organizational stakeholders as well as the general public, is lower than hitherto and senior management is now being held personally accountable for failure to manage risk effectively. Failing to manage risk effectively can quite easily become a critical issue, sometimes even fatal, so having policies and frameworks within which to manage risk is vital to continuity and success. The regulatory environment is becoming stricter with government and authorities placing ever-more stringent requirements on organizations to comply with legal and regulatory frameworks.

Organizations that have adopted risk management methodologies are better placed to ensure that operations are successful and the potential damage from risk is reduced.

Risk management should be integrated in day-to-day operations and become part of the culture, with everyone in the organization being responsible for managing risk in their sphere of work. This can be facilitated by a CRO who has overall responsibility for ensuring that risk throughout the organization is being managed effectively by developing and establishing appropriate policies, frameworks, and methodologies.

Risk management can no longer be taken lightly; it needs to be given due attention and it needs to be an achievable goal. With the right amount of effort, proper preparation, and planning, as well as resourcing, organizations should be able to formulate risk management strategies and policies, thus ensuring their readiness and ability to deal with adverse situations should they arise.

Remember too that managing risk is not a one-off exercise but rather something that should be done and, importantly, reviewed on a regular basis. Risks change and complacency is not an option. Organizations that implement risk management procedures mitigate the consequences of the worst disasters that might befall them.

REFERENCES

- British Standards Institution (2011). *BS 31100:2011—Risk Management*. Code of Practice and Guidance for the Implementation of BS ISO 31000. BSi.
- Canadian Institute of Chartered Accountants (1995). *Guidance on Control*. Canada. Available at, <http://www.rogb.ca/publications/item12613.aspx>.
- Carnegie Mellon University (2004). *Continuous Risk Management Overview*. Available at, <http://www.sei.cmu.edu/risk/overview.html>.
- Institute of Risk Management (2002). *A Risk Management Standard*. IRM, AIRMIC, and ALARM. Available at, http://www.theirm.org/publications/documents/ARMS_2002_IRM.pdf.
- International Organization for Standardization (ISO) (2009a). *ISO Guide 73:2009—Risk Management—Vocabulary*. Available at, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44651.
- ISO (2009b). *ISO 31000:2009—Risk Management—Principles and Guidelines on Implementation*. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.
- ISO (2009c). *ISO/IEC 31010:2009—Risk Management—Risk Assessment Techniques*. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.
- Haimes, Y. Y. (2009). *Risk Modeling, Assessment, and Management*. New York: John Wiley and Sons.
- Treasury, H. M. (2004). *The Orange Book: Management of Risk—Principles and Concepts*. Available at, http://www.hm-treasury.gov.uk/orange_book.htm.
- Hopkin, P. (2010). *Fundamentals of Risk Management: Understanding Evaluating and Implementing Effective Risk Management*.
- Moeller, R. R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes* (2nd ed.). New York: John Wiley and Sons.
- Turnbull, N., & Institute of Chartered Accountants in England and Wales (1999). *Internal Control: Guidance for Directors on the Combined Code*. Institute of Chartered Accountants in England and Wales. London, United Kingdom.

Overview of TIRM Process and Model

WHAT YOU WILL LEARN IN THIS CHAPTER:

- What is the TIRM process
- What are the stages of the TIRM process
- How to communicate and consult during information risk management
- How to monitor and review the TIRM process
- How to quantify information risks using the TIRM model
- How to determine the risk appetite of your organization

INTRODUCTION

In this part of the book, we show ways to assess and treat information risk by following the Total Information Risk Management (TIRM) process. The TIRM process is a best-practice procedure for managing information risks. It contains the most important aspects that you need to consider to be successful in managing information risk. The process is explained in detail in the following commentary. The TIRM process can be divided into three stages:

- A.** Establish the context
- B.** Information risk assessment
- C.** Information risk treatment

This chapter provides a step-by-step guide on how to implement the TIRM process in your organization.

Every organization follows business processes, even if this often happens on a subconscious level. A business process has been defined as “a specific ordering of work activities across time and place, with a beginning, an end, and clearly identified inputs and outputs: a structure for action” (Davenport, 1993). An information risk management process is a management process that focuses on controlling and monitoring organizational risk that arises through data and information assets inside and outside an organization. Information is used in abundance in your business and it is hard to keep track of where it might cause risk. Luckily, we have gained a great deal of experience on how to manage information risks effectively through our work with a number of organizations in different sectors. We will share the experiences gained during our research at the University of Cambridge and provide you with guidance on how to assess and treat data risks effectively. In Chapter 3, we discussed why an

information risk management process is probably the right way forward for your organization. In the next few chapters, we will show which steps should be followed in an information risk management process that we call the TIRM process.

The TIRM process is compliant with the widely accepted ISO 31000 risk management standard. This has the advantage of sharing the same risk terminology and concepts. For risk managers, many of the concepts should be well known and therefore easy to apply.



IMPORTANT

The TIRM process aims to systematically manage risks arising from data and information assets of all possible types and sources—that is, external and internal, tacit and explicit, and structured and unstructured. It is based on the widely accepted ISO 31000 risk management standard.



IMPORTANT

Information risk is the effect of uncertainty on an organization's business objectives that arises from information quality.

WHAT DOES THE WORD *TOTAL* STAND FOR IN TIRM?

We believe that you should consider all types of information used in all operational and management processes that are important to your business, no matter whether they are stored in:

- Databases
- Word-processed files
- Slideshows
- Spreadsheets
- Videos
- Audio recordings
- XML and HTML files
- Social networks
- Twitter
- Websites
- Paper hardcopies
- Email
- Mail
- Fax
- Telephone
- Face-to-face communications

The only condition is that the information that is considered in the TIRM process should be significant enough for your business (you have to determine for yourself what you consider significant

information). Moreover, you should not limit your information risk management efforts to a single function or business process (although it might be a good starting point from which to extend to the whole organization). If something goes wrong in one of your core business processes it affects the rest of the business.

With the word *total*, we also emphasize that *all* core business processes have to be considered in the information risk management process, making TIRM an enterprise-wide program, rather than a local one. However, you may choose to begin implementation in a single defined area.

STAGES OF THE TIRM PROCESS

The TIRM process consists of three main stages and two continuous activities that are executed throughout these stages, as illustrated in [Figure 5.1](#).

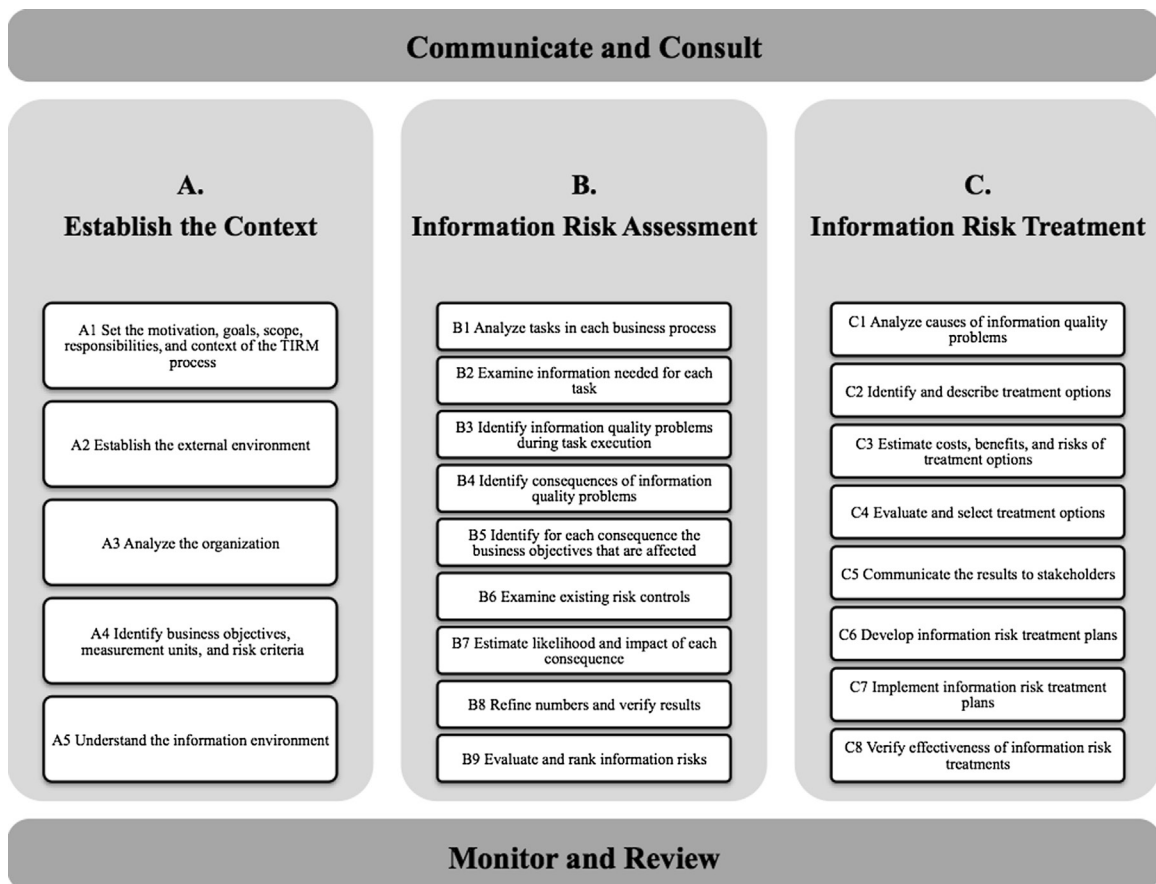


FIGURE 5.1
TIRM process.

When starting a TIRM initiative, the first thing that needs to be done is to establish the context—this is *stage A*. Every organization exists in different internal and external environments that are specific to it. To understand an information risk, establishing the organizational context is absolutely necessary. A major risk in one organization—for example, due to regulatory requirements, a particular competitive environment, or organizational culture—can be a low risk in another organization that operates in a different context.

Information risk is assessed in *stage B*. Information risks have to be identified and analyzed qualitatively and/or quantitatively and then evaluated. This is the heart of the TIRM process. In this stage, you will collect the inputs that are needed to model and quantify data and information risks.

In *stage C*, information risk treatment options have to be examined, selected, and implemented.

Communicate and consult is the basis of the process needed in all three stages. Without support of relevant stakeholders, your efforts are destined to fail. You also need senior management backing for the TIRM process.

The TIRM process should be constantly monitored and reviewed to verify and improve the effectiveness of the process and adapt it to the organizational context.

All stages and continuous activities are required for a successful TIRM initiative.

If you are already familiar with the ISO 31000 standard, you might have observed that the stages of the TIRM process do not differ much from the ISO 31000 risk management process stages. This is because the TIRM process is based on and refines the ISO 31000 risk management process for managing information risk, and therefore looks very similar to a general risk management process at a high level.



IMPORTANT

There are three stages in the TIRM process that follow each other: The process starts with (A) establish the context, followed by (B) information risk assessment, and ends with (C) information risk treatment. There are two activities that are actually executed throughout the process: communicate and consult and monitor and review.



ATTENTION

All three stages of the TIRM process and the two continuous activities are required to successfully manage information risk.

Chapter 6 deals explicitly with establishing the context in stage A, Chapter 7 explains how to assess information risk in stage B, and Chapter 8 shows how a procedure for information risks can be treated in stage C.

The two continuous stages communicate and consult and monitor and review are discussed in the following sections. Moreover, we will explain how to determine the risk appetite of your organization.

COMMUNICATE AND CONSULT

An ongoing activity throughout the TIRM process that is absolutely essential for the success of the TIRM process is to communicate and consult with all relevant stakeholders. Relevant stakeholders can include personnel from the business function(s) involved, IT management, risk management, as well as senior executives. As the TIRM process crosses functional boundaries, it is a key requirement that senior management will be committed to the information risk management initiative. It is also important that the IT management and risk management executives are aware of and willing and able to support the initiative. The goals and benefits of the information risk management program need to be clearly communicated to all people involved in, or affected by, the TIRM process to gain active support.

To assess risk, information has to be gathered from across the whole organization. If it is not clearly and transparently communicated how information risk is assessed, people will not believe the figures and findings from the assessment, and it will be very hard to convince them to support information risk treatments that are required or beneficial. Communicating and consulting has to be done in parallel with all other stages.



IMPORTANT

Not everyone appreciates the importance of information. You need to explain and demonstrate the business value of the information you are using.



EXAMPLE

A senior executive is hostile and blocks your efforts to implement an information risk management program. You start to investigate and find out that a failed information governance program in the past has turned the senior executive into a strong opponent of any

further initiatives related to information governance. The communication plan has to incorporate solid arguments that are communicated to this executive to convince him why the mistakes that occurred in the past will not be repeated once again.

Identifying information stakeholders

Information stakeholders are all people and groups of people who have a stake in the information that is managed or the management of information in the organization. The only exception would be if TIRM was applied to part of an organization. A list of all information stakeholders should preferably be created. New stakeholders might be added during other stages of the TIRM process.

Make a list of all stakeholders (using as a basis the one provided in [Figure 5.2](#)) that are relevant for your TIRM initiative. Investigate and document the attitude of each stakeholder group toward the initiative (e.g., supportive, enthusiastic, neutral, or opposed) and what you think might motivate their attitude, and draw up a plan that articulates how to effectively communicate matters to each of the stakeholders



Who are Information Stakeholders?

- Information producers
- Data intermediaries
- Knowledge workers
- Process owners
- Business information stewards
- Internal and external auditors
- Business partners
- End customers
- Third-party information providers
- Distribution channels
- Regulatory bodies
- Communities and general public

FIGURE 5.2

Information stakeholders. (Source: *English, 1999*.)

to best gain their support. Also, organize presentation and training sessions so that they are tailored to each specific group of stakeholders.



ACTION TIP

Identify relevant participants and organize information and training sessions at the start, and run them during the TIRM initiative.

Involve stakeholders in stage A

In stage A, a check needs to be made to identify whether the perceptions of the external and internal environment of the organization, the business objectives, and risk criteria are shared among key stakeholders.



ACTION TIP

Develop a communication plan: Who needs to be informed about what and at which stage? See [Table 5.1](#), which can be used as a template.

Involve stakeholders in stage B

Stakeholders are involved during information risk assessment to get additional information and advice, and to ensure that everyone accepts the findings from this stage. In particular, the validity and plausibility of results from the information risk assessment stage should be validated with relevant stakeholders.

Involving stakeholders in stage C

During information risk treatment, it needs to be explained with care why particular options have been chosen or not chosen and why a particular way is selected in which to implement the option. A participative approach is of benefit here. Potential information risk treatment options should be discussed

Table 5.1 Information Stakeholders

TIRM Stage	Stakeholder	Communication and Consultation Needed	Form of Communication
Stage A: establish the context	IT executives	Explain what TIRM is and why it is important to IT executives	Presentation
...	...	...	...

with all involved parties to better understand their weaknesses, risks and strengths, and to get support during implementation.

MONITOR AND REVIEW

Finally, the implementation of the TIRM process itself should be constantly improved based on the experiences gained during its application in your organization. Some problems can be more easily identified from an external perspective. By interviewing a wide range of stakeholders, the TIRM process can be better enhanced and improved.

The ISO 31000 risk management standard (ISO, 2009a, p. 20) highlights the purpose of monitoring and review:

- Ensuring that controls are effective and efficient in both design and operation.
- Obtaining further information to improve risk management.
- Analyzing and learning lessons from events (including near-misses), changes, trends, successes, and failures.
- Detecting changes in the external and internal context, including changes to risk and the risk itself, which can require revision of risk treatments and priorities.
- Identifying emerging risks.

TIRM MODEL: QUANTIFYING INFORMATION RISK

In Chapter 3, we discussed, at a high level, how information risks are created. To be able to assess and quantify risks, an even more granular view is needed. We will now take a look “under the hood” by presenting a model to quantify information risks.

TIRM modeling symbols

We explain here the components of the TIRM model. In our experience, it helps to draw diagrams to visualize information risks. Therefore, we introduce TIRM modeling symbols to represent each of the constructs graphically.

Business process

The first construct is the business process, for which we use a (six-sided) hexagon (Figure 5.3).

**FIGURE 5.3**

Business process construct.

Task

A business process can consist of several tasks, which are represented as a circle (Figure 5.4).

**FIGURE 5.4**

Task construct.

Data and information assets

We represent a data and information asset with a star (Figure 5.5).



FIGURE 5.5

Data and information asset construct.

Information quality problem

We use a diamond for the information quality problem construct (Figure 5.6).



FIGURE 5.6

Information quality problem construct.

Consequence

We use a square to represent a consequence, no matter if it is a direct or an intermediate consequence (Figure 5.7).



FIGURE 5.7
Consequence construct.

Impact on business objective

We use the callout symbol to show that a consequence has an impact on one or more business objectives in our modeling (Figure 5.8).



FIGURE 5.8
Impact on business objective
construct.

Putting it together: the TIRM model

Figure 5.9 shows how the components of the TIRM model are integrated and interlinked.

Each business process contains any number of tasks that are carried out as part of that business process. To execute a task, data and information assets are required. Each piece of information may contain information quality problems, such as having missing entries (completeness of the data), which result in direct consequences. Further undesirable ramifications may result from the direct consequence, and each of these may still have any number of other, intermediate consequences. This, in turn, could adversely impact the achievement of a business objective.

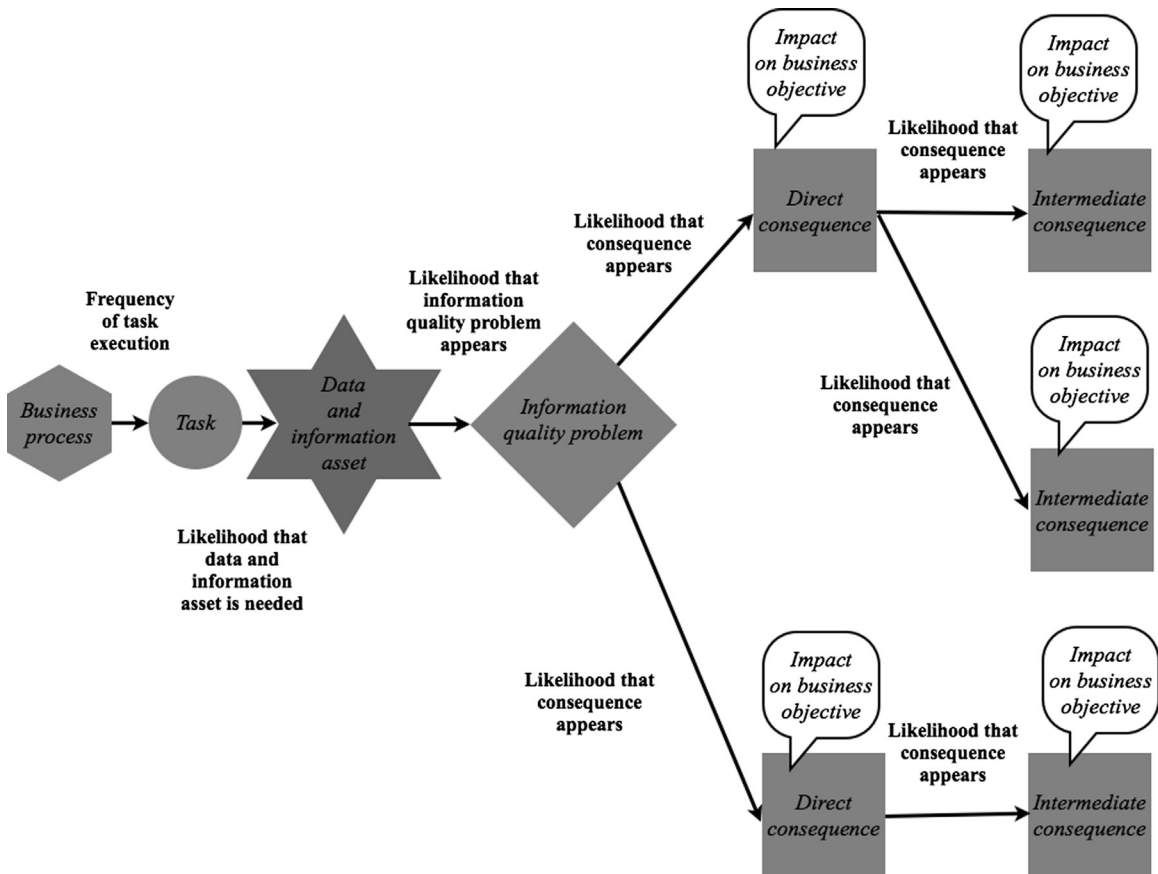


FIGURE 5.9
TIRM model.

There are also parameters that specify the link between the components in the model. The first parameter is the frequency of task execution, which is recorded for each task that is part of a business process, and is the number of times (e.g., per month) that the task is actually carried out. Each time the task is executed it may require different data and information assets, and therefore, the probability that the data and information asset is needed is recorded for each task–information pair. Furthermore, the specified information quality problem may not always appear in the particular subset of information used. For example, for a particular type of part, the information (asset) could list all of the suppliers without gaps, and therefore, the problem would not manifest itself in some cases. Therefore, the likelihood that the information quality problem appears in the information that is used for the task needs to be specified. In a similar manner, the likelihood that the problem leads to the direct consequence is recorded along with the likelihood that each consequence leads to other, intermediate, consequences. The last parameter is the severity of the impact in the impact on business objective component.

A demonstration of how risk totals can be calculated using the components and parameters of the TIRM model is given in Chapter 7 in TIRM process step B9.

Providing estimates for the TIRM model

Providing estimates for each of the parameters can be done in three different ways, as discussed in the “Providing Estimates” box. Option 1 is to estimate the expected mean value and will be used in our examples in Chapter 7 when we illustrate how the TIRM model can be put into action for information risk assessment. Options 2 and 3 require a Monte Carlo simulation to be run to calculate the risk totals, which is explained in detail in Chapter 11. A Monte Carlo simulation produces repeatedly random numbers of an estimated distribution to compute their results. If you want to use options 2 and 3, adequate software support is needed. A pilot software tool InforAS for the TIRM model that we developed to support the TIRM process is presented in Chapter 12.

PROVIDING ESTIMATES

There are three options to provide quantitative estimates as part of the TIRM process:

Option 1: Estimating the expected value. Often the expected value is not known accurately or is volatile. In these cases, option 2 or 3 can be more suitable.

Option 2: Estimating a lower and an upper boundary. There is a high likelihood that between these boundaries will be the real value. In this case, it is assumed that the expected value is equally

distributed between the two boundaries (i.e., it is distributed uniformly). A slight possible variation to option 2 is that one assumes that the values are distributed normally between the two boundaries (i.e., a normal distribution is used in this case).

Option 3: Estimating the most likely value (mode) and a lower and upper boundary. The advantage of having these three estimates is that they can be used to calculate the so-called triangular distribution.

If the task is executed by somebody other than the business process representatives participating in the information risk assessment workshop, this information can be obtained by asking the person who usually executes the task. This can sometimes also be supplemented with data that documents the execution of the task, if it is available.

How the TIRM model is used as part of the TIRM process

The TIRM model is used to support the assessment and quantification of information risks in stage B of the TIRM process, which is presented in Chapter 7. The required parameters for the TIRM model will be gathered as part of the process steps in stage B. The risk totals can then be calculated for each information risk, which is explained and demonstrated in TIRM process step B9 in Chapter 7.

DETERMINING RISK APPETITE FOR TIRM

Before starting with the TIRM process, the risk appetite should be determined. Once the risk appetite has been determined, the organization will be on its way to establishing a robust TIRM process. The risk appetite will be needed to set up risk criteria in step A4 of the TIRM process. Providing clarity about tolerance levels and who is responsible will:

- Ensure that better-informed business decisions are made.
- Provide clear communication channels, alerting senior levels of management to potential information risks at an early stage.

Table 5.2 Example Risk Appetite Scale

Level 1	Level 2	Level 3	Level 4
No risk appetite Not willing to accept risks in <i>any</i> circumstances	Low risk appetite Not willing to accept risks in <i>some</i> circumstances	Medium risk appetite Willing to accept risks in <i>some</i> circumstances	High risk appetite Willing to accept risk in <i>any</i> circumstances

- Alleviate the possibility of being exposed to unmanageable information risks.
- Allow the organization to prioritize actions in those areas where risk is deemed to exceed the defined appetite.
- Help to develop a culture where information risk awareness becomes embedded in day-to-day operations.
- Establish the right balance between being bold and being cautious.

Risk appetite could be expressed on a scale—you can of course decide how to measure your risk appetite but you may wish to consider the following suggestion of a 1 to 4 scale, an example of which is shown in [Table 5.2](#).

Communicating the tolerance level in this way should also be accompanied by guidance in terms of the discretion available. For example, who can take the decision to tolerate the risk? When does a decision need to be escalated to a higher level of management?

More tangible scales are set in the form of risk criteria for each business objective in step A4 during the establish the context stage.

Many experienced employees will have an intuitive feel for the risk level they may expose the organization to, but it is unwise to rely on this, and boundaries need to be established with clear guidelines put in place so that misunderstandings and bad risks are mitigated.

The level of risk appetite will vary; it will not remain static, not only in respect of specific issues but also over time.



EXAMPLE

As an example, with speculative projects you may be prepared to tolerate a higher level of risk appetite than that for mission-critical projects. Over time, an activity

or project that may have been deemed to be a level 1 risk in year 1 may become level 3 in year 3 as expertise in managing that specific situation is developed.

SUMMARY

This chapter presented an overview of the TIRM process and generic aspects that need to be considered during all three stages of the TIRM process, such as communicating and consulting with stakeholders of the TIRM, monitoring and reviewing the TIRM process, and determining an organization's risk appetite.

We also presented a model for TIRM that will be used to assess and quantify information risks as part of stage B of the TIRM process. Chapter 6 presents stage A—establish the context—of the TIRM process.

REFERENCES

- Davenport, L. (1993). *Process Innovation: Reengineering Work Through Information Technology*. Boston: Harvard Business School Press.
- English, L. P. (1999). *Improving Data Warehouse and Business Information Quality: Methods for Reducing Costs and Increasing Profits*. New York: John Wiley and Sons.
- International Organization for Standardization (ISO) (2009). ISO 31000:2009 Risk Management—Principles and Guidelines on Implementation. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.

TIRM Process Stage A: Establish the Context

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to set the motivation, goals, initial scope, responsibilities, and context of the TIRM process
- How to establish the external environment
- How to analyze the organization
- How to identify business objectives, measurement units, and risk criteria
- How to get a thorough understanding of the information environment

INTRODUCTION

Motivation and goals for stage A

The goal of this stage is to establish the context for Total Information Risk Management (TIRM). Imagine you want to build a new house. You probably would initially need to make a number of preparations before the actual building of the house commences. You need to purchase a plot of land to build the property on and hire an architect to design the house. The assessment and treatment of information risks also requires some preparation. As in the analogy of the construction of a house, some of the key decisions in the TIRM process are made at the very beginning, when establishing the context. For instance, you need to decide early on what the motivation and goals are of applying the TIRM process in your organization. You need also to set a scope and define the responsibilities and context of the process. But, this is not enough. If you want to successfully facilitate the process, you have to develop a good understanding of the environment your organization is in, both internally and externally.

It should not be too surprising that you also require a good understanding of the important IT systems and information management processes in your organization. As risk is the effect of uncertainty on business objectives, you need to understand the information aspects of the core business objectives in your organization and you also need to determine how these should be measured. The benefit of this stage is that you can execute the succeeding stages more effectively. Please take this stage seriously. If the architect has done a poor job at the start, it will be very difficult to compensate for that initial poor job at a later stage. Once the building of the house has commenced and is in progress, you could lose a lot of time and waste resources if things have not been done properly from the start.

Overview of stage A



IMPORTANT

A lot of the information that needs to be collected as part of stage A will be already documented in your organization, so you just need to find the right documents, extract the essentials from these, and refer to the documents so that the details can be easily accessed if needed.

Stage A consists of five steps as shown in [Figure 6.1](#). First, the motivation, goals, scope, responsibilities, and context of the TIRM process are set in step A1. The external environment needs to be established in step A2, followed by an analysis of the organization in step A3. Moreover, business objectives, measurement units, and risk criteria need to be identified in step A4. The final step, A5, establishes the information environment.

Some of the information to establish the context can be collected by interviewing managers from different functions, those who have a good overview of the organization. A lot of the information will already be documented in most organizations, so you just need to find the right documents, extract the essentials from these, and refer to the documents so you or somebody else can look up the details if needed.

Stage A: Establish the Context

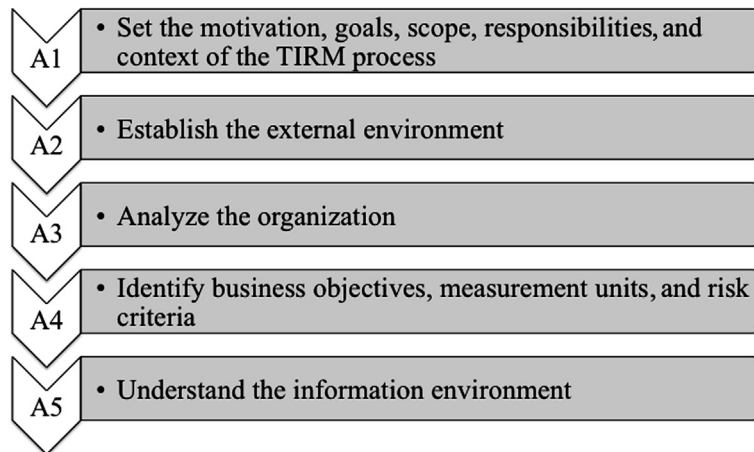


FIGURE 6.1

Five steps to establishing the context.



IMPORTANT

The time and resources you spend establishing the context in stage A should be proportional to the scope of the TIRM process. Make sure that the majority of the time and resource allocation is reserved for stages B and C.

Output of this stage

- The motivation and goals for implementing the TIRM process.
- A defined scope, responsibilities, and context for applying the TIRM process.
- An understanding of the organization's external, internal, and information environments.
- Identified key business objectives in your organization and measurement scales to quantify the objectives.
- Risk criteria for each business objective.
- General information management issues.

TIRM PROJECT KICKOFF

To implement the TIRM process in your organization, you need first to convince and educate other people about the usefulness of the TIRM process and explain at a basic level how it works. In particular, you need to establish senior management support. Therefore, a sensible tactic is to invite people who have expressed an interest in being involved to a presentation about the TIRM process (e.g., the one that you can find in the online book companion website). Then, organize a two- to three-hour workshop with the interested parties during which you convince them to participate in step A1.

WHAT IF YOU DO NOT HAVE SENIOR LEADERSHIP COMMITMENT FOR TIRM?

Often, it is hard to convince senior leadership to engage, as they are preoccupied with too many things. It is usually easier to gain the support of the leadership of a smaller business unit rather than the support of top executives. Choose leaders of business units who show the most enthusiasm for data and information improvement projects. Restricting the scope of the TIRM process application to a particular, smaller

business unit or segment can be a useful strategy; this is particularly appropriate if you have not been able to get the support of the executive leadership to the implementation of the TIRM process. If the implementation of the TIRM process in the small initial scope is successful, this might give you the opportunity to convince other business units to participate in the future, as you will have a success story to tell.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

We will illustrate all the steps in the following commentary, using a fictitious case study of a call center, which is under constant pressure to fully satisfy customers but suffers from decreasing profit margins. A data quality manager believes that higher customer satisfaction at a lower cost

can be achieved if data and information is of higher quality and is used more effectively. He convinces the managing director of the call center to implement the TIRM process to identify optimal data and information quality improvement investments that promise the best benefit-to-cost ratio.

STEP A1: SET THE MOTIVATION, GOALS, INITIAL SCOPE, RESPONSIBILITIES, AND CONTEXT OF THE TIRM PROCESS

The first step (Figure 6.2) contains a number of activities to kick off the TIRM process, shown in Figure 6.3.

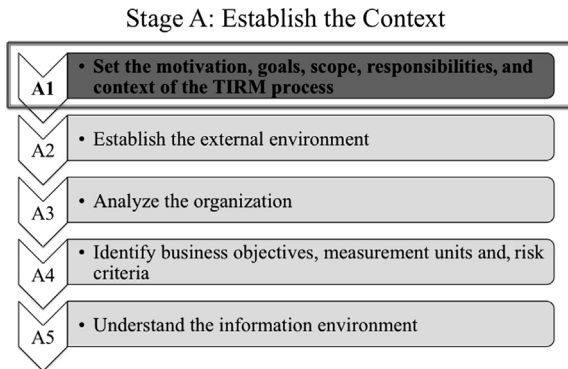


FIGURE 6.2
Step A1 in context.

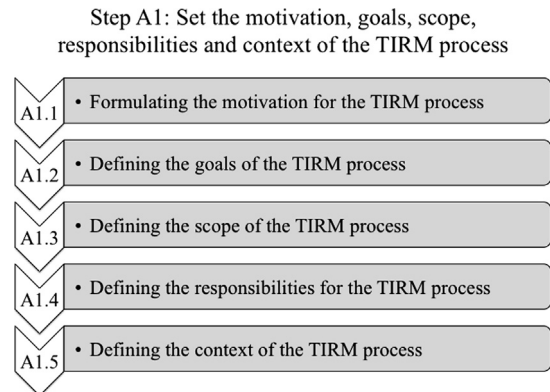


FIGURE 6.3
Activities in step A1.

A.1.1: Formulating the motivation for the TIRM process

The TIRM process can be started by asking the question “What is our motivation for implementing the process?”

There is a reason why you want to implement the TIRM process in your organization. Other people who you have convinced to participate in and support the implementation will also have a reason why they support you. In this step, it is all about agreeing on a common motivation that serves as a mission for the entire process implementation. In practice, the senior executive who will sponsor the implementation has a major say in what the motivation for the process will be. The motivation is typically grounded in one or more problems that the organization faces, such as:

- The executive board does not see the value of having high-quality information.
- The organization thinks that it is doing a bad job in managing information quality and would like to know where and how to improve to help the business.

- The organization is worried that poor data is creating risks in a particular business unit and wants to know what to do to control or mitigate the risk.
- The organization recognizes that there are significant risks arising from poor information and aims to control them.

Once you have agreed on a common motivation, the next step is to formulate a brief mission statement that captures this motivation. An example could be:

Recognizing that information is a critical asset for our organization, we aim to achieve a full understanding of what information is, and how to control the risks that arise through poor information in our core business processes.

The mission statement can be used as an “elevator pitch,” the first sentence that is communicated to somebody who asks what the program is about. By embracing the mission statement, the senior executive shows his or her support for the TIRM program. It can also be helpful to set a common vision that you aim to achieve in the very long term.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

In a kickoff meeting, the call center management decides to formulate the following motivation for the application of the TIRM process in the organization:

Our vision is to provide every business process that has relevance for our client relationships with the optimal level of data and information quality.

A.1.2: Defining the goals of the TIRM process

Next, the goals for the process have to be determined. The goals should be derived from the motivation and in their way operationalize the mission statement and make it really actionable. A few examples of goals for the TIRM process are:

- “The goal of our TIRM program is to quantify the impact of poor data and information in our organization.”
- “The goal of our TIRM program is to improve information where it most impacts the time to delivery of our products.”
- “The goal of our TIRM program is to align IT investments with information needs in business processes.”
- “The goal of our TIRM program is to optimize business process performance through focused information quality improvement.”
- “The goal of our TIRM program is to establish a risk register of all major risks that arise from information.”
- “The goal of our TIRM program is to remove redundant information processes.”

Note that there can be more than one goal for the application of the TIRM process. It really depends on what your organization aims to achieve. Of course, these goals should be realistic, achievable, and specific, and furthermore reflect the overall goals and values of the organization. They should also be prioritized to provide clarity where any conflicts arise.

**EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER**

The call center decides to focus on optimizing customer satisfaction and operational efficiency:

The goal of our TIRM program is to improve data and information where it impacts customer satisfaction and operational efficiency. We want to

understand which data and information are critical for our key business processes and which data and information quality problems hurt the business most.

A.1.3: Defining the scope of the TIRM process

A clear scope should be defined for the TIRM initiative. The scope is dependent on the motivation and goals set for the TIRM process and on the resources that you are willing to invest.

At the outset it is important to define which parts of the business should be included in the scope. You might decide to permanently include only a particular business unit, product line, geographical site, etc., or you might implement the TIRM process in the entire organization. It really depends on the goals and the resources you have available for implementing the TIRM process. It also depends on how important information is regarded in your organization by senior leadership and how severe the known information quality issues are. If you have the resources and necessary support of your senior leaders, then the best strategy is to try the TIRM process in a small, but important part of the business, and then expand it gradually to the rest of the business. Bear in mind that the selection of business processes based on the scope that should be included in the analysis is made in step A3, when business processes are examined in more detail.

If the goal of the TIRM process application is to identify all information risks related to a particular part of your business, you might want to include all data and information assets that are used for the business processes in this business unit. This has the advantage that you do not miss out on data and information assets that are important for a business process but you have not thought about before.

If the goals of your process application are more tightly linked to particular IT systems, you can choose to focus on data and information assets in these IT systems. You can also decide to limit your analysis to, for instance, master data, transactional data, or other data types. So, it really depends on what your mission and goals are when you choose the scope regarding data and information assets.

Particularly, however, when the TIRM process is implemented with the goal of improving the effectiveness of IT systems and is, for instance, sponsored by the CIO or the business intelligence unit, it is easy to forget about data and information assets that are not stored and processed by IT systems. This is often not the best way to proceed, as omitting less structured information (e.g., that is shared via email and hardcopy documents or through personal communication) limits your view about which information is actually used in key business processes.

One example that we encountered in our work is that of an industrial engineer who telephones the planning department instead of looking directly at the planning data in the Enterprise Resource

Table 6.1 Standard Set of Information Quality Dimensions for TIRM

Information Quality Dimension	Description
Accuracy	Is the data and information asset correct? Does it correspond to the real value that it represents?
Completeness	Is the data and information asset complete? Does it contain all the information it should contain?
Consistency	Is the information stored in a consistent format?
Up to date	Has information changed since the last time it was been updated in a way that it is incorrect now?
Interpretability	Is the content of the data and information asset easily interpretable by the users? Is it represented in a way that is easy to understand?
Accessibility	Can I access the data and information asset in a timely manner?
Availability	Is the information that I need available in my organization?
Security	Can somebody else access the information who should not be able to access it? How likely is it that the information gets lost?

Planning (ERP) system, because the planning information stored in the ERP system is hard to find and interpret. The planning department then looks up the information for the industrial engineer in the system, which is a waste of time and resources, and sometimes leads even to greater problems. The IT department would not be aware of these significant information quality problems if the role of unstructured information for the effectiveness of IT systems is downplayed and the actual usage of all types of data and information assets is not considered.

An important decision needs to be made regarding the information quality dimensions that you would like to focus on in the information risk assessment. We recommend you choose from the set of dimensions shown in [Table 6.1](#). However, you can also define your own additional dimensions or use other information quality frameworks (e.g., [Wang and Strong, 1996](#)) that are relevant to the context in which the TIRM process is being applied.

Choosing information quality dimensions at this stage can be a bit tricky. How do you know beforehand which problems are the greatest? It is easy if the goal of your TIRM initiative specifies particular information quality dimensions explicitly or implicitly. But even then, you probably need to clearly state which information quality dimensions are included or excluded from the analysis. For example, if the goal of the TIRM process is to identify the risks that arise from incorrect information, you have to decide if this includes just the accuracy dimension, or should it also include the completeness and up-to-date dimensions. If you are not sure, the safest option is to go with the standard set of information quality dimensions for the TIRM process shown in [Table 6.1](#). You could also decide to exclude the security dimension from this list, if you only want to focus on risks that arise through information usage. Please bear in mind that the selection of information quality dimensions is only preliminary at this stage, and will be potentially refined in step A5 and during information risk assessment in stage B.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The call center decides to focus on the part of the business that has direct contact with end customers. It is also decided to include all types of data and information assets that are important for the business processes in the scope. The information quality dimensions to be

included are accuracy, completeness, consistency, up to date, interpretability, accessibility, and availability. The security dimension is put out of scope since information security is satisfyingly managed within the organization.

A.1.4: Defining the responsibilities for the TIRM process

Once you have defined a scope for the TIRM process application, it is time to identify the roles and responsibilities involved in the execution/performance of the process. The detailed organizational setting is discussed in Chapter 9. The following roles and responsibilities have to be undertaken by adequately capable representatives who should be suitable with regards to the chosen scope and goals of the TIRM process initiative.

ROLES AND RESPONSIBILITIES

TIRM Process Sponsor

The TIRM process sponsor is in charge and is responsible for making available the necessary resources to implement the process and is interested in the results. This should be an executive or a very senior manager who has budget responsibility.

TIRM Process Manager

The TIRM process manager manages the resources and is responsible for the implementation of the process. A senior- or middle-level manager should undertake this role.

TIRM Process Facilitator(s)

The TIRM process facilitator organizes and facilitates the workshops. This can be a middle- or lower-level

manager or consultant. If the scope is large, several process facilitators might be necessary.

Business Process Representatives (chosen in step A3)

For each business process in the scope, one to two subject-matter experts should be chosen who have a good knowledge of the business process they represent.

IT System and Database Representatives (chosen in step A5)

For each IT system and database in the scope, a representative should be chosen who has good knowledge of the IT system and/or database and of the data and information assets that are related to the IT system and/or database.

As a rule of thumb, the larger the scope of the application, the more human resources are required and the higher up the TIRM process sponsor should be (in the organizational hierarchy). This is appropriate because the sponsor needs to have the seniority and authority to provide both the budget and support needed. The process manager has the task of overseeing and coordinating the application of the TIRM process, but does not need to do this full time. In some cases, the TIRM process sponsor might also act as the process manager. The process facilitators support the operationalization of the TIRM process “on the ground.” They help to run the workshops, undertake analysis and evaluation, and produce reports for the TIRM process manager, the TIRM sponsor, and the rest of the organization. They need to read this book and should also be experienced in the discipline of

information management in general. They are also responsible for coordinating the business process representatives and IT representatives.

Business process representatives are subject-matter experts in a particular business process in the scope. If you have many smaller business processes, it might be sufficient to have just one business process representative for each business process. For larger business processes (with many parties involved and many different activities), more business process representatives could be selected, since one business process representative might not have the full oversight over the business process. Bear in mind that if there are different departments involved in one business process, it would make sense to choose one business process representative from each of the departments.

The IT representatives should jointly have a good oversight of the IT landscape and all important applications and databases in the scope of the process. They should be experienced in IT project management. None of these roles and responsibilities necessarily requires a full-time commitment (the TIRM team is likely to be full time while the business stakeholders are not) but this, again, depends on the scope of the application. In medium-size businesses or if the scope is limited to a handful of business processes, it can be done as a side activity in addition to the normal day-to-day job. But, of course, it will always require a significant time commitment by the actors who fill out the roles for the TIRM process. The structure of different committees who are ultimately responsible for the TIRM process is introduced and debated in Chapter 9.



ACTION TIP

When you try to find suitable people to fulfill the different roles required for the TIRM process, excitement and interest of the employees about data and information assets is as important as their expertise.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

At the call center, the data quality manager convinces the managing director of the call center to become the sponsor of the TIRM program and offers himself as the TIRM manager and facilitator. Two data enthusiasts

from the IT department volunteer to become the IT and data representatives, and together they cover all major IT systems. Finally, the managing director chooses two business process representatives for each business process.

A.1.5: Defining the context of the TIRM process

Finally, the context of the process itself needs to be defined—that is, how the TIRM process should be integrated within the organization. In particular, the relationships to other programs or projects that are interrelated have to be defined. This is covered in more detail in Chapter 9.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM initiative at the call center is run as an executive-sponsored business performance improvement program and reports directly to the

management board. The recommendations should be presented to an information governance council, which is headed by the corporate operation officer.

STEP A2: ESTABLISH THE EXTERNAL ENVIRONMENT

In this step, the external environment of the organization needs to be established (Figure 6.4). This can include aspects ranging from social and cultural, political, legal, regulatory, financial, technological, economic, natural, and the competitive environment, whether international, national, regional, or local (International Organization for Standardization, 2009, p. 31000).

Risk management, in general, requires a good understanding of the context of the organization, both internal and external. The external environment has a significant influence on the success of every organization. Therefore, organizational behavior is often geared toward the external environment. It sets requirements and necessities for the organization. Information is often essential to comply with these requirements and necessities. For example, financial information often needs to be submitted to regulators, which is a requirement that comes from the external environment of your organization. If the customers in your specific market require customized support and a high level of service, this sets higher demands for your customer information management. There are many other examples to demonstrate the interplay between the external environment and information management. This step will, therefore, help to assess and treat information risk in the succeeding stages. The external environment of an organization can have a major influence on how information risks are evaluated.

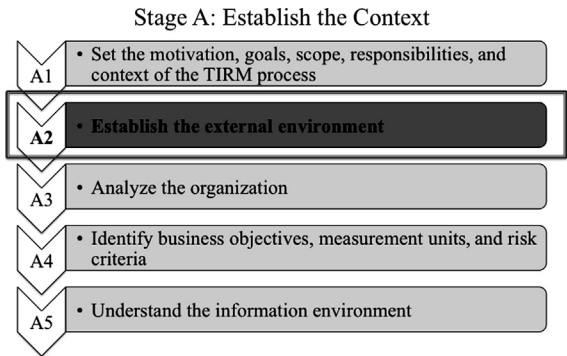


FIGURE 6.4
Step A2 in context.

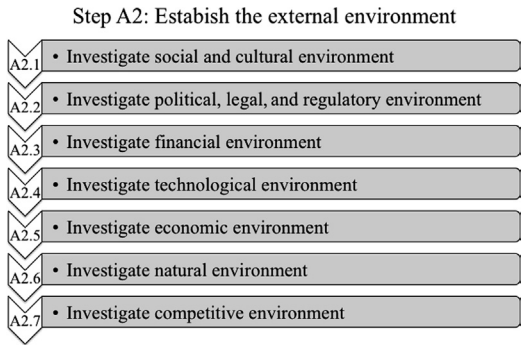


FIGURE 6.5
Activities in step A2.



EXAMPLE

A publicly listed company A has to comply with different financial requirements and rules than the privately owned family business B. Accounting information that

is 10% inaccurate can lead directly to huge penalties by financial regulators in the case of company A, but might pose only minor risks in the case of company B.



EXAMPLE

The U.K. utility industry is a sector that is heavily regulated with regard to price and service quality. Information about the age and reliability of physical

assets plays a crucial role as evidence that investments to modernize the assets are really necessary, which is important to justify the increase in prices.

The focus should be on aspects of the external environment that are relevant and significant for the scope set in step A1—that is, the business processes and data and information assets. Every organization will have other external factors that are important. The art is to identify the most relevant drivers in the external environment. Brainstorming can be used as a creative technique (see Chapter 11). As shown in [Figure 6.5](#), the external environment can cover a very wide range of aspects, including social and cultural, political, legal, regulatory, financial, technological, economic, natural, and the competitive environment, whether international, national, regional, or local.



ACTION TIP

Every organization will have other external factors that are important. The art is to identify the most relevant drivers in the external environment. Brainstorming can be used as a creative technique (see Chapter 11).

A.2.1: Investigate social and cultural environment

The social and cultural environment can play an important role for your organization. For example, if you are selling products to consumers or other companies, it depends on the social and cultural background of the customers as to how the behavior of your organization is perceived. For example, in some countries, corruption and unethical behavior is more tolerated than in others ([Rose-Ackerman, 1999](#)). Customers (either consumers or business customers) might stop buying your products if they perceive your organization as unethical. This does not necessarily mean being involved in corrupt activity. For some, it might be enough that your company harms the environment and ecological systems in some way. Or, that your organization obtains its supplies from suppliers that are not perceived to respect human rights. For instance, the consumer products giant Apple has been heavily criticized for the working conditions at Foxconn; Samsung has also been criticized for excessive overtime and fines for employees in China. Sometimes, you can get penalized by the society (consumers and/or the government) when you move parts of your production away from the country (France would be a typical example; see [Trumbull, 2006](#)). Thus, the way you market your products will be heavily dependent on the cultural and social background of your customers.

A.2.2: Investigate political, legal, and regulatory environment

The political, legal, and regulatory environment can be very influential insofar as the way you carry out business activities. Organizations need to comply with each country's laws and regulations in which they do business. Rules and regulations can change frequently and are often ambiguous; they also depend on the political culture in a country. Many industries are heavily regulated around the world, such as banking and finance, utility, transportation, oil and gas, and mining. The regulations will have

a major influence on your business model. Moreover, the legal system can differ from one country to the other (e.g., civil law, common law, religious law) and often requires very specialized expertise. The introduction of new taxation laws can change the basis of your investment decisions. Furthermore, in some countries, it might be more difficult for you to protect your organization's intellectual property. A more extreme example is if the countries in which you undertake business get involved in conflicts, such as war, civil war, and revolutions—these can completely invalidate what initially were very sound business decisions.

A.2.3: Investigate financial environment

The financial environment affects how an organization can raise finance, transfer risk, trade financial securities, allow international trading in different currencies, and share profits with its investors. It can include many different markets, such as commodities, real estate, bonds, cash, and many others. In many ways, the success of an organization is dependent on the financial environment. For example, if it is easier and cheaper to access money, a company is more flexible in undertaking investments. Lower borrowing rates can offer a substantial competitive advantage. For many organizations, the ability to get access to money is crucial for their survival.

A.2.4: Investigate technological environment

Technology is a key driver for innovation in many markets. Disruptions in technology can often be game-changers. Kodak, a company founded in 1889 that popularized modern photography, had to file for bankruptcy in 2012 because of its tardiness in transitioning to digital photography (ironically, it invented digital photography). Technology is important not only in engineering industries. For instance, computers revolutionized investment banking as they allowed traders to automatically and almost instantaneously react to changes in the market. Whatever technologies drive your particular market, it is important to remain cognizant of new developments, as technologies can change very quickly.

A.2.5: Investigate economic environment

Businessdictionary.com defines the economic environment as “the totality of economic factors, such as employment, income, inflation, interest rates, productivity, and wealth that influence the buying behavior of consumers and institutions.” The economic environment is, of course, important for commercial corporations, however, the economic environment is also important for nonprofit organizations because they are dependent on the financial health of the population (private individuals and institutions) to attract donations and income.

A.2.6: Investigate natural environment

Natural disasters such as hurricanes, earthquakes, tsunamis, and volcanic eruptions can disrupt the functioning of many organizations, for instance, by interrupting the supply chain of a company. Sectors such as insurance and banking can be directly affected by large-scale natural disasters. Moreover, natural resources are important in many industries.

A.2.7: Investigate competitive environment

Not every industry is equally competitive. Every industry and market will have its particular demands and challenges. Acting as a monopoly can be a blessing for profit margins, but it can also mean that the regulatory control is likely to be tighter. In highly competitive fast-moving markets, price competitiveness and large research and development costs can lead to very low margins. The manner in which your organization conducts business will be heavily dependent on the competitive environment it is exposed to.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The call center has to respect the cultural and social norms of the country from which the end customers are calling. Also, rules about data protection differ from

country to country. With many players penetrating the market, business is becoming increasingly competitive.

STEP A3: ANALYZE THE ORGANIZATION

After having established the external context of your organization, it is time to have a closer look at the organization itself (Figure 6.6). Understanding the business model, business processes, organizational structure, and culture are all important elements in understanding the internal environment for information management (Buchanan and Gibb, 1998). These activities feature in step A3 as shown in Figure 6.7.

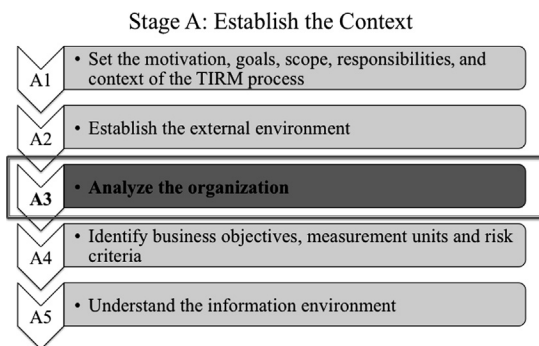


FIGURE 6.6
Step A3 in context.

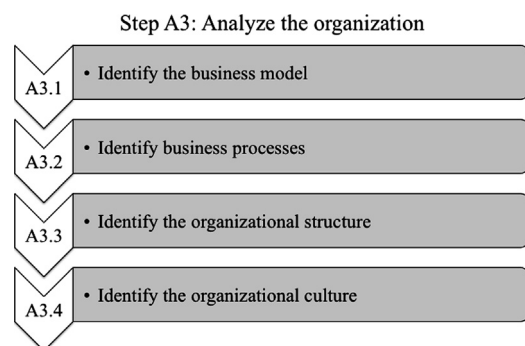


FIGURE 6.7
Activities in step A3.

A.3.1: Identify the business model

A good place to start is to take a look at the business model. Most organizations will have a carefully developed business model, which all staff should have an awareness of.

Consider what is it that your organization is actually doing? What kind of capabilities has your organization built up to do these things? How is it creating value for its customers? And if your organization has competitors, what is it that makes your organization competitively special? Business strategy is about utilizing the unique internal capabilities to best fit them to the opportunities and requirements of the market. So, what kind of business strategy is your organization pursuing?

If your organization is nonprofit, there is still some kind of business model. A charity must still often compete against others, for example, to raise money and attract donations. A governmental organization has (hopefully) a reason to exist by providing some sort of value to the taxpayers. Even a church can have a business model (although it probably would not call it so by name), as it needs to operate with limited resources and usually aims to provide high-quality services to its congregation.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The call center is a regional market leader in the premium segment of call center services. It offers inbound and outbound outsourcing services for large corporations that, on the one hand, have high volumes of telephone calls, and

on the other hand, require very high-quality responses. The call center's main points of competitive advantage are rigorous processes and careful selection and training of human resources to ensure high quality at large volumes.

A.3.2: Identify business processes

Business processes need to be identified and included in the scope. Information creates risk since it is used in business processes in the organization. Your business model explains *what* your organization is doing. Examining the key business processes in your organization will give insight into *how* your organization is implementing its business model.

Remember to focus only on identifying business processes that are in the scope of the TIRM process outlined in step A1. If you are not fully aware of your key business processes in the scope, you will be able to identify them by examining your business model and the key activities that deliver value in line with it.



ATTENTION

Avoid wasting time. Focus only on identifying business processes that are in the scope of the TIRM process outlined in step A1.

In general terms, there are four different types of business processes ([Earl and Khan, 1994](#)):

- Core processes (servicing external customers)
- Support processes (servicing internal customers)

- Business network processes (crossing company boundaries)
- Management processes (establishing the strategic framework for the other processes)

Each type of business process is explained further in the following box.



THEORETICAL EXCURSION

As a general rule, there are four different types of business processes:

- Core processes, also called operational processes, execute the tasks that deliver value to the customers.
- Supporting processes support the core processes, and only indirectly contribute to providing customer value.
- Business network processes go beyond the boundary of an organization. Often, value is delivered through collaboration with other external entities through business network processes. The supply chain is a good example.
- Management processes make decisions on which, how, when, and to what extent core processes are executed, as well as by whom. Also, on how they should be orchestrated to deliver value—this is done through administration, allocation, and control of resources. Thus, management processes are the steering wheel of an organization.

In each category of business processes, there are some that are more important than others. Once business processes have been identified, the most relevant ones are selected. They can be ranked according to their criticality and importance in the business model. The selection should take the motivation and goals for the TIRM process into account, as set out in step A1. It is essential that senior management is involved in some form in this ranking and prioritization process and gives approval, for example, by participating in a workshop or by simply reviewing and suggesting corrections to the ranked list of business processes once it is created.

Additionally, collect the documentation that is available in your organization about the selected business processes. It is very likely that your organization has previously modeled some business processes. In many instances it will be possible for you to reuse documents that already exist in your organization. Make sure, however, that the business process models are up to date.



ACTION TIP

There are many different types of modeling and visualization techniques that can be used to model these processes, such as use-case diagrams, activity diagrams, event-driven process chains, and many more. Any models of business processes are good enough for the purpose of the TIRM process, as long as they get acceptance in your organization.



IMPORTANT

Most organizations have models of their important business processes. Make sure you collect the documented models.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The call center identifies three core business processes in the scope, which should be in the focus:

1. The customer inquiry response process, which deals with end customer requests of the client company that has outsourced the support function to the call center.
2. The product sales process where the call center contacts potential end customers on

behalf of the client company to sell their products.

3. The customer survey process, which executes predefined customer surveys with end customers on behalf of the client company.

Other types of business processes should not be considered at the initial implementation of the TIRM process.

A.3.3: Identify the organizational structure

Next, the organizational structure relevant to the chosen scope in A1 is identified. The organizational structure is usually documented in existing diagrams. The organizational structure should be analyzed to identify relevant insights for information management. For example, an organization's structure that is not well aligned to business processes can lead to functional silos, which prevent information from flowing optimally throughout the business processes.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The call center is divided into two departments: inbound and outbound. The inbound department is responsible for taking care of incoming customer calls

for the client. The outbound department deals with calls that are actively made, for example, to sell client products to end customers or to conduct surveys.

A.3.4: Identify the organizational culture

Organizational culture is always important for organizational success and every organization has its own distinct culture. To manage information risks, you have to understand the culture in the particular organization, then adapt and choose the methods that you are using for assessing and treating information risks so that it really fits with the organizational culture.

According to [Buchanan and Gibb \(1998\)](#), there are two different approaches to identify organizational culture:

- Stakeholder analysis ([Grundy, 1993](#))
- Force-field analysis ([Lewin, 1947](#))

While stakeholder analysis helps to diagnose key stakeholder influences on the information strategy, Lewin's force-field analysis identifies the enabling and restraining forces that affect the information strategy. However, you do not need to analyze organizational culture with formal methods. The easiest way is to keep your eyes and ears open when you talk to people and try to identify cultural patterns.

Keep these cultural patterns and characteristics in mind when you conduct the information risk assessment and treatment and whenever you communicate and consult with stakeholders as part of the TIRM program.

Finally, the attitude toward information and its perceived value is an important element of organizational culture for information management and should be investigated during interviews with employees and managers.



ACTION TIP

The acceptance of different methods for business process modeling differs from one organization to another. Aim to understand the culture and adapt the choice of methods and techniques to it. Make sure you communicate in an appropriate language, one that not only the stakeholders speak but also that reflects their culture.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The culture in the inbound department is very cooperative and therefore information is freely shared whenever needed. As call center representatives often get rewarded on the basis of the level of

their individual sales performance in the outbound department, the culture there is less collaborative with call center representatives being less eager to help each other and share information and knowledge.

STEP A4: IDENTIFYING BUSINESS OBJECTIVES, MEASUREMENT UNITS, AND RISK CRITERIA

Risk is the effect of uncertainty on the objectives of an organization (Figure 6.8). To manage the uncertainty you have to identify your organization's business objectives and appropriate ways to measure how each is being achieved or not. Moreover, you need to define what the different points in the measurement scales actually mean to your organization by setting risk criteria. Figure 6.9 shows the associated activities of step A4.

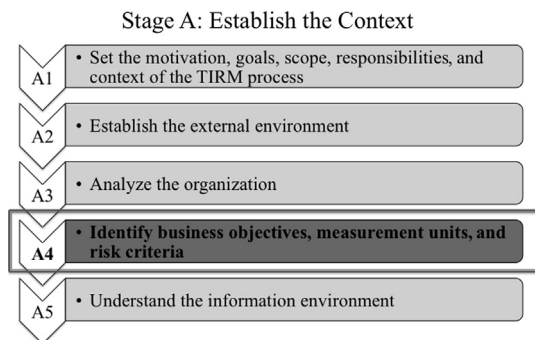


FIGURE 6.8
Step A4 in context.

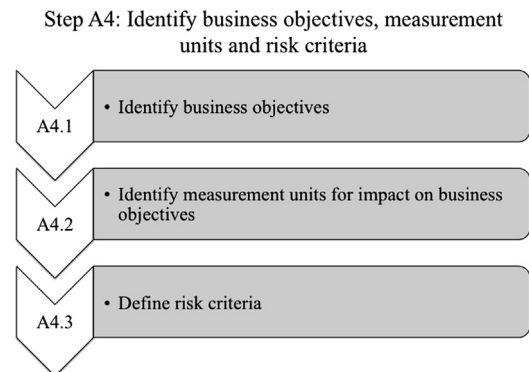


FIGURE 6.9
Activities in step A4.

**IMPORTANT**

Without identifying business objectives and ways to measure the achievement objectives, it is not possible to assess risk.

A.4.1: Identify business objectives

Business objectives are the goals that an organization aims to achieve and the organization's leadership sets them. They are often described in the organization's mission statement—in such cases, it is appropriate to start the identification of business objectives by extracting the goals articulated in the mission statement.

The business objectives should be classified into distinct categories, such as health and safety or revenues. However, the mission statement might not accurately reflect the goals and targets set by the leadership. Therefore, it is important that the business objectives, which have been identified, are reviewed and refined by senior management.

**EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER**

The mission document of the call center states three different goals.

Our company is united in three goals that are guiding us throughout all parts of our business:

1. Our goal is to have sustainable sales growth.
2. Our goal is to always operate in a cost-efficient manner.
3. Our goal is to always satisfy our customers to the fullest possible extent.

Based on the goals in the corporate mission, the TIRM steering committee identifies three categories of business objectives:

1. Sales growth
2. Operational efficiency
3. Customer satisfaction

A.4.2: Identify measurement units for impact on business objectives

A metric to measure impact needs to be defined for each business objective. You should start by identifying measurement scales that are already in use in your organization. For some of the business objectives, there will probably be some, but it may take some effort to find them. Measurement scales will have to be defined if there is no measurement scale already available.

To be able to make all statistical calculations needed for calculating the total risk figures, the measurement metric needs to be at least an interval scale (see "Theoretical Excursion" box for an introduction to the different types of measurement scales). For the purposes of the TIRM process, a nominal scale would not be sufficient, as risk values would not be comparable. You simply cannot say if one value is worse or better than another value on a nominal scale. Since risk is calculated as the product of the impact multiplied by the probability, an ordinal scale is also unsuitable, because this calculation would not be meaningful. Take the example of a three-point scale: small damage, medium damage,

and big damage. If there is a 30% probability of medium damage, it is not possible to multiply these to calculate the expected average value.



IMPORTANT

Measurement metrics that are used as part of the TIRM process should preferably be interval scales or ratio scales if you want to quantify and calculate risk as an output of the TIRM process.



THEORETICAL EXCURSION

Over more than half a century ago, Harvard psychologist Stanley Smith Stevens published an article on the theory of scale types in the prestigious *Science Journal* (Stevens, 1946), which is still, to this day, the most dominant work on measurement scales. His theory proposed that there are four different types of measurement metrics (Table 6.2).

The first type of scale is called nominal or categorical, which is an unordered set of qualitative values. An example would be the categories male or female, for which you cannot say which of the values is bigger; therefore, it is unordered. Another example could be a list of colors (e.g., red, gray, yellow, or blue). The only statistics that you can do on a nominal scale is to calculate a mode, which is

the value that appears most often, and the chi-square to check if there are any correlations between the values. There is no transformation allowed on this scale.

The second type of scale is called ordinal, which is a totally ordered set of qualitative values. This could be, using a simple example, the scale consisting of three age values: young, middle aged, and old. You can assign an ordered rank to each value, for example, 1 is young, 2 is middle aged, and 3 is old. A higher number equals an older age, but there are only three possible values in the data set. If you multiply these with any number, the ordering of the values will stay intact. Let's say in our example we multiply by 5 the numbers that represent our three values; the rank of each attribute will still stay the same—that

Table 6.2 Four Different Types of Measurement Metrics

Scale Type	Mathematical Structure	Permissible Statistics	Admissible Scale Transformation
Nominal categorical	Standard set structure (unordered)	Mode, chi-square	One-to-one (equality (=))
Ordinal	Totally ordered set	Median and mode, percentile, rank order correlation, nonparametric analysis of variance	Monotonic increasing (order (<))
Interval	Affine line	Mean, standard deviation, correlation-r, regression, analysis of variance, factor analysis	Positive linear (affine)
Ratio	One-dimensional vector space	All statistics permitted for interval scales plus the following: geometric mean, harmonic mean, coefficient of variation, and logarithms	Positive similarities (multiplication)

Source: Wikipedia. http://en.wikipedia.org/wiki/Level_of_measurement.



THEORETICAL EXCURSION—cont'd

is, 5 is young, 10 is middle aged, and 15 is old. In such scale, it is possible to calculate the most common value (mode), and additionally the middle-ranked item, the so-called median. However, as you cannot, for instance, say on this type of scale how much older an “old” person is compared to a “young” person, the differences and sums cannot be calculated. It follows that it is not possible to calculate the average value (also called the mean).

The third type of scale is called interval, which is an ordered quantitative scale that allows positive linear transformations. An interval scale is similar to the ordinal scale ordered, but additionally, it tells us about the size of the intervals between data points. For those readers who like mathematics, you can do the following transformation of all data points x without changing

the meaning: $y(x) = a \times x + b$ with a and b being any real numbers. A commonly used example is the Celsius temperature scale. For this scale, it is permissible to perform many more statistical operations, such as the mean (the average value), the standard deviation (how far values are scattered around the average), linear correlation, regression, analysis of variance, and factor analysis.

Finally, the fourth type of scale is called the ratio, which in addition to having the attributes of an interval scale has a true zero point. Using the example of the temperature as before, it would only be the Kelvin temperature scale that fulfills this criterion, as it has a true zero point. This type of scale allows additional statistical operations, such as the geometric and harmonic mean, and the coefficient of variation and logarithmical transformations.

An example of a self-defined scale for the TIRM process is shown in [Table 6.3](#). If you define a scale of your own for one or more impact domains, you should give examples of what a value actually means.

Table 6.3 Example of a Self-defined Measurement Metric

Point scale	Interpretation	Examples for Health and Safety
0	No impact	No impact.
$0 < x < 1$	Very minor impact	Potential minor injury. Potential minor impact on health and safety of employees, customers, society, etc.
$1 < x < 10$	Minor impact	One minor injury. Minor noncompliance to health and safety laws. Minor impact on health and safety of employees, customers, society, etc.
$10 < x < 100$	Medium impact	Several minor injuries. One near miss. Medium impact on health and safety of employees, customers, society, etc.
$100 < x < 1000$	High impact	One severe injury. Severe noncompliance to health and safety laws. High impact on health and safety of employees, customers, society, etc.
$1000 < x < 10,000$	Very high impact	One casualty. Very high impact on health of employees, customers, society, etc.
$x > 10,000$	Extreme impact	Several casualties in accident. Extreme impact on health and safety of employees, customers, society, etc.

In some cases, it could also be useful for estimating the impact in stage B to define measurement metrics as the product of the impact per unit multiplied by the number of units. For example, instead of saying that a flooding event creates an impact of \$1,000,000 damage, the impact per square meter is given (e.g., USD \$10,000) and then the number of square meters that are affected by the flood needs

only to be estimated (e.g., 100 square meters), which is then used to calculate the impact ($\$10,000 \times 100 \text{ m}^2 = \$1,000,000$).



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM steering committee chooses the following measurement metrics for the three business objectives:

1. Sales growth impact is measured as lost sales revenues in U.S. dollars.
2. Operational efficiency is measured as increased operational costs in U.S. dollars.
3. Customer satisfaction is measured using the number of unsatisfied callers; this metric can be measured using surveys with end customers conducted at the end of a telephone call, and considering also the number of active customer complaints.

A.4.3: Define risk criteria

Finally, the risk criteria need to be defined for TIRM. Risk criteria make sure that the risk appetite of your organization is considered during risk evaluation. Losing \$1,000,000 in sales can be a pretty bad thing for, let's say, a medium-size furniture manufacturing company, but is not such a significant risk for a gigantic retailer like Wal-Mart. Risk criteria are therefore needed as "the terms of reference against which the significance of a risk [...] is evaluated" (ISO, 2009, p. 6). They are "based on organizational objectives, and external and internal context" and can be "derived from standards, laws, policies, and other requirements" (ISO, 2009, p. 6).

Risk criteria include the level at which a risk becomes acceptable or tolerable (e.g., a monetary value), the way likelihood is defined (which follows the way in which likelihood is defined in the model), and the timeframe that should be considered.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM steering committee chooses the following risk criteria in a one-year timeframe:

The following are the risk criteria for business objectives of sales growth and operational efficiency measured in yearly lost revenue in USD and yearly higher operational costs in USD.

Very low	\$0	—	\$50,000	
Low	\$50,001	—	\$250,000	
Medium	\$250,001	—	\$500,000	
High	\$500,001	—	\$1,000,000	Not tolerable
Very high	\$1,000,001	—	Unlimited	Not tolerable

The following are the risk criteria for the business objective of customer satisfaction measured in the number of dissatisfied callers.

Very low	0	—	1000	
Low	1001	—	2000	
Medium	2001	—	3000	
High	3001	—	5000	Not tolerable
Very high	5001	—	Unlimited	Not tolerable

STEP A.5: UNDERSTAND THE INFORMATION ENVIRONMENT

The aim of this step is to gain a better understanding of the information environment, which focuses on the following aspects: information management processes, IT systems, and known data issues in the scope (Figure 6.10).

Depending on the scope and goals of the TIRM process, some aspects of the information environment might require more attention than others. It is recommended that you follow the three activities shown in Figure 6.11 and to add further activities based on your own judgment of your organization's situation.

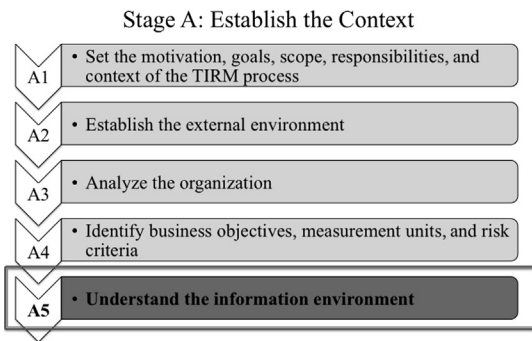


FIGURE 6.10

Step A5 in context.

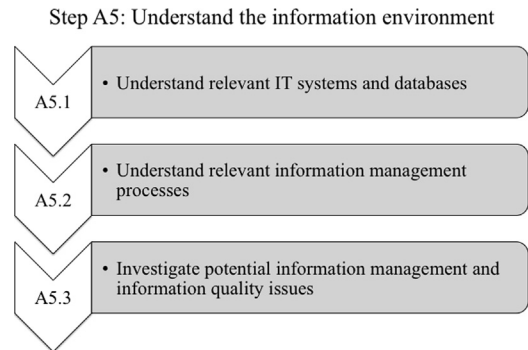


FIGURE 6.11

Activities in step A5.

A.5.1: Understand relevant IT systems and databases

This activity is really about gaining a better understanding of the IT systems and databases that collect, store, and process the data and information assets that are in the scope of the TIRM process.

You can start this activity by creating a list of IT systems and databases that are relevant for the scope (defined in A1.3). This is not always as straightforward as it might sound, mainly because of two reasons. In many organizations a complete and up-to-date register of IT systems and databases does not exist or is difficult to get ahold of. Moreover, you need to find out which IT systems and databases in your organization are actually relevant for the scope of the TIRM process. For some it will be obvious, but for others it will be a bit more difficult. Which data and information assets are needed for business processes in the scope will be analyzed later in stage B, thus is not appropriate at this stage.

Once an initial list of relevant IT systems and databases is created, you should gather information that helps you understand each of the relevant IT systems and databases. For each IT system and database, a representative should be identified and chosen who is a subject-matter expert and who will be incumbent to share the knowledge about a particular IT system and/or database throughout the application of the TIRM process. Any relevant documentation, such as IT system architecture, data models, information flow diagrams, etc., should be collected. Moreover, a demonstration of important software applications should be organized in this substep, because it makes it easier to facilitate the information

risk assessment workshops in stage B and allows for a better understanding of information usage problems related to a particular IT system or database. You should also investigate how IT systems and databases are interlinked with each other.

Linking your TIRM program to an enterprise architecture model can help you get stronger senior management support (see the following box). It can also make it easier to identify suitable information risk treatment options in stage C.



THEORETICAL EXCURSION: ENTERPRISE ARCHITECTURE

The best overview of what and how an organization does is a model of an enterprise architecture, which is defined by the MIT Center for Information Systems Research as “the organizing logic for business processes and IT infrastructure reflecting the integration and standardization requirements of the company’s operating model. The operating model is the desired state of business process integration and business process standardization for delivering goods and services to customers” (Weill, 2007).

Enterprise architecture is a bird’s eye view of the enterprise, which shows strategic objectives, business

processes, organizational structure, IT landscape, databases all at one glance, and puts a context to it. Two commonly used models for enterprise architecture are Zachman and TOGAF (Zachman, 1987; Harrison, 2007). An important part of the enterprise architecture is the information architecture, which is “the art and science of organizing and labeling data including: websites, intranets, online communities, software, books, and other mediums of information, to develop usability and structural aesthetics” (Information Architecture Institute, 2013).



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM process manager together with the TIRM facilitators organize meetings with IT managers, data managers, and information architects to identify the most important IT systems in the scope, which are used for all three core processes:

1. Computer Telephony Integration System (CTI), which enables autodialers by using the customer contact information from the database and automatically helps to comply with country-specific call periods. It also brings up basic information about the caller and the history of interactions with the caller. The system also allows the running of automatic call feedback surveys with customers on the telephone; these can evaluate how good the service provided by the call center agent was.
2. Knowledge Base System (KBS), which is a knowledge base of frequent problems and questions with potential solutions. Subject-matter experts are identified who can be contacted for second-level support.
3. Issue Tracking System (ITS), which allows the call center agents to record issues that are reported by customers and to manage these issues. The system is connected to the CTI, which allows the CTI to show issues recorded in the past with a customer automatically on the screen. The KBS feeds automatic suggestions about how to resolve an issue that is recorded in the ITS.
4. Customer Relationship Management System (CRM), which manages customer data and tracks and supports sales activities. The system feeds data into the CTI and the records are connected with issues tracked in the ITS.

Moreover, there are three main databases within the scope of the TIRM process identified that support the IT systems:

1. The customer master database contains all end customer-related information, such as contact details, date of birth, and any other master data. It supports mainly the CTI and CRM.

Continued



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER—cont'd

2. The customer interaction database contains transactional data from interactions with end customers, including issues that are reported by customers and also any feedback that is given in automatic surveys with customers after a call. The database is used for the ITS and CTI systems.
3. The expert database is a data warehouse that contains the data about answers and

solutions to frequent problems and that feeds into the KBS.

For each IT system and database, relevant documents are identified during the initial meeting and are shared with the TIRM stakeholders. For each IT system and database, a subject-matter expert is chosen to be the IT system and database representative.

A.5.2: Understand relevant information management processes

Information management processes handle data and information assets as they are created, organized, stored, processed, accessed, used, archived, or deleted. As part of this activity, you should identify key information management processes that are relevant for the scope of the TIRM process. This can

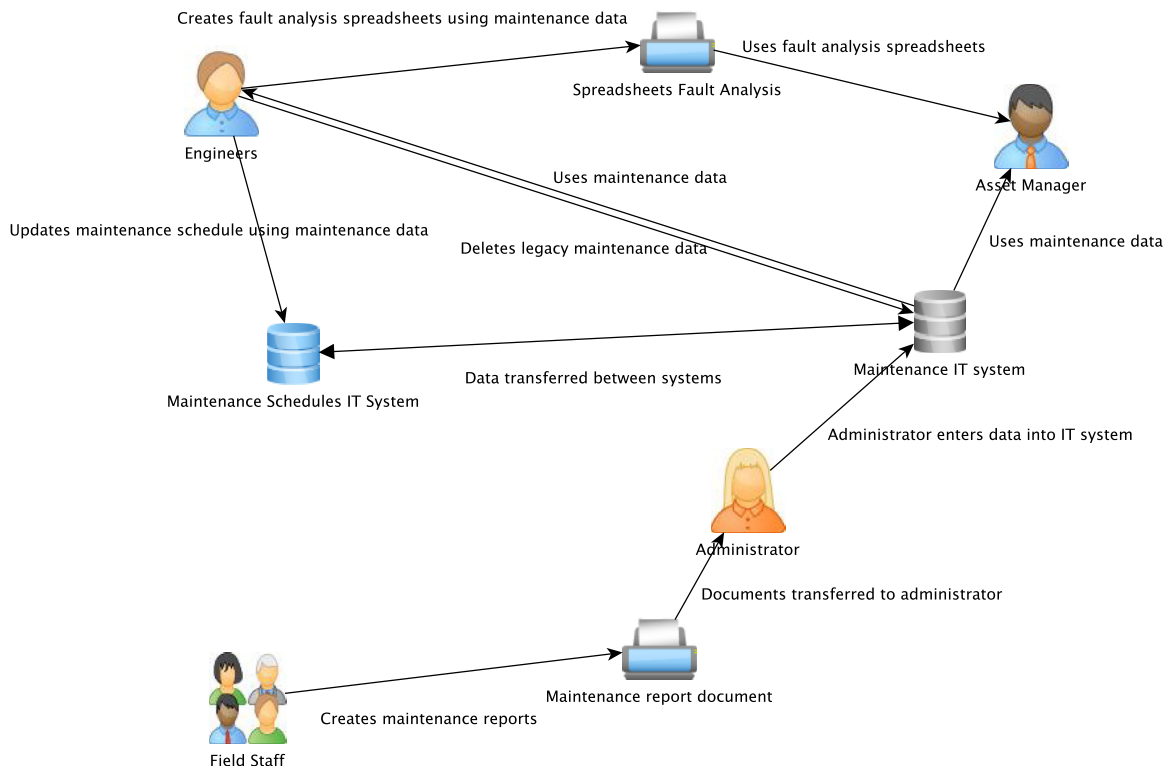


FIGURE 6.12

Example of an information flow diagram.

be done by interviewing information managers in the organization. Documents about at least some of the information management processes can be found in many organizations, so they are worth investigating.

Another method that can help you understand the information management processes is to model how information flows throughout the enterprise over the information life cycle. It should show each significant step when information is created, collected, processed, transferred, stored, accessed, used, maintained, and deleted, and also describe who or what system and database is involved in the step. An example of an information flow diagram is shown in Figure 6.12. For instance, the field staff creates a maintenance report, which is entered into the maintenance IT system by an administrator and then used by engineers and the asset manager.

Another method that can help you understand the information management processes are so-called information management maturity models, which give an overview of information management process capabilities in the organization (see following box).



THEORETICAL EXCURSION: MEASURING THE MATURITY OF INFORMATION MANAGEMENT

Information management maturity models can help identify weaknesses in the information management processes in an organization. A maturity model is used to assess capabilities by evaluating the maturity of processes and to identify priority areas for improvement. A typical model consists of five maturity levels: initial (level 1), repeatable (level 2), defined (level 3), managed (level 4), and optimizing (level 5), although levels are sometimes named differently. Within these models, each maturity level is based on a comprehensive set of criteria of information management; these comprise concept, function, behavioral aspects, requirements to be met, and measurement.

To assess maturity, for each level and criteria evidence is collected for analysis, reflection, and synthesis. Measurement of both quantitative and qualitative factors is used that includes a defined process for building the

outcomes from each level to monitor progress, and to take corrective actions at each level when necessary. Increased maturity evolves then through a progression of levels or stages with transformations over time. Both the assessment of maturity levels and the understanding of how to attain higher levels of maturity are central to increasing the maturity level of an organization.

An example of a maturity model for information management is the IT-Capability Maturity Framework (IT-CMF, see <http://ivi.nuim.ie/it-cmf/>). Based on capabilities and categories along 32 critical processes, this framework is designed as a systematic framework that enables senior management and chief executives to interrogate, understand, and improve an organization's maturity, thus ensuring realization of IT capabilities and optimal delivery of business value from IT investments.



ATTENTION

Information management maturity models will compare your processes with current good practices and tell you how well (or otherwise) you comply with them. However, every organization is different! Maturity models do not show you which improvements will bring about the most value in the context of your organization.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

Together with a TIRM facilitator, the IT system and database representatives analyze and document the fundamental information management processes for the IT system and databases they represent. This can be summarized as:

1. Data in the customer master database is initially obtained from the client company and then updated by the call center agents. Customer data has to be deleted when a client company decides to stop using the services of the call center.
2. Data in the customer interaction database is automatically recorded during interactions with

end customers. The call center agents enter issues raised by customers into the system. The data comes from the ITS and CTI systems.

3. The data in the expert database is generated and updated manually by a working group of team leaders and business analysts who go through the most frequently faced issues on a monthly basis, by analyzing data from the customer interaction and customer master databases.

The TIRM facilitator and the IT system and database representatives also create an information flow map, a sample of which is shown in [Figure 6.13](#).

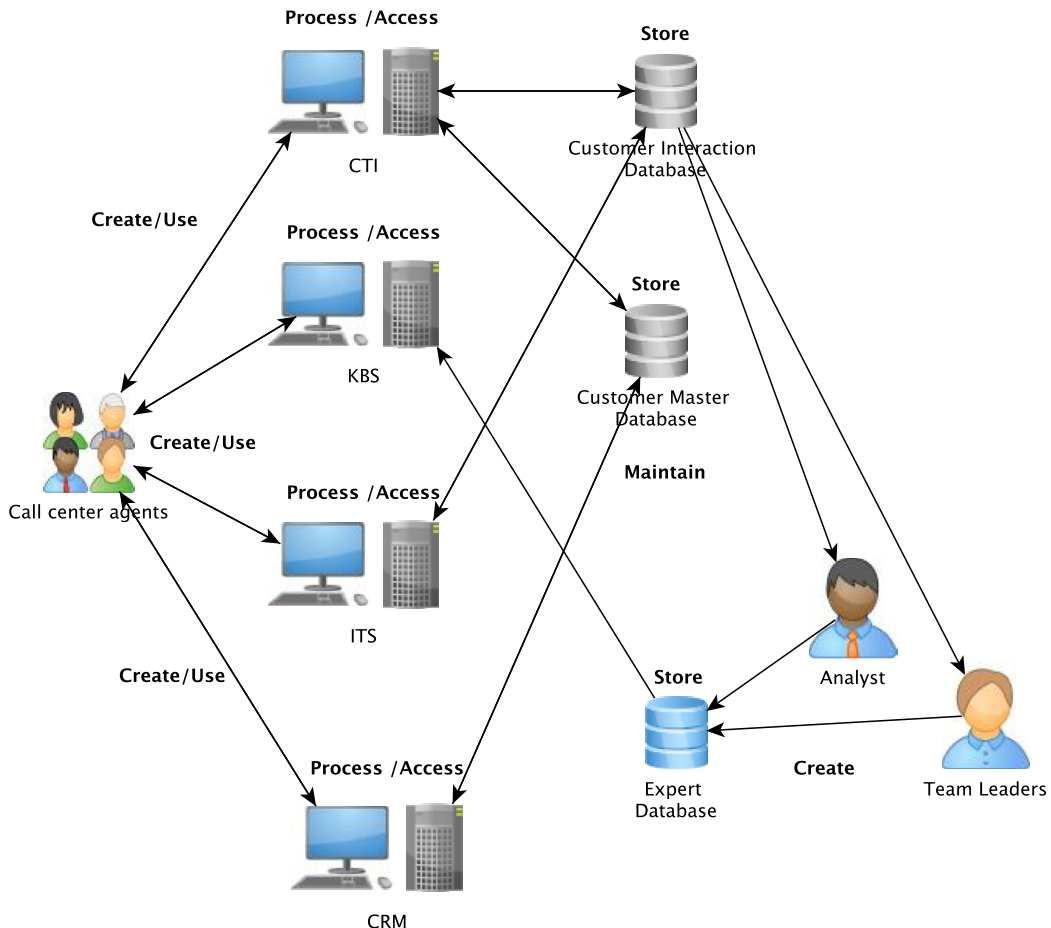


FIGURE 6.13

Sample information flow diagram for call center.

A.5.3: Investigate potential information management and information quality issues

This activity investigates general information management and information quality issues that can potentially lead to information quality problems in the business processes. It is the first part of a data and information quality assessment in the scope of the TIRM process, which is done from an information manager's perspective. The results of this activity will be used in step B3 to help identify data and information quality problems in the most important business processes from an information user perspective. They can also be used later to identify the causes of information quality problems in step C1.

First, it is appropriate to note any general information management issues that might potentially lead to information quality problems; this can be done by interviewing IT representatives—for example, you might identify a general awareness of a data entry process that is not being executed as well as it should be. Some of the problems might have already been identified during the earlier activities undertaken in substeps A.5.1 and A.5.2. Interviewing data and information managers may identify some other issues. The identified issues should be documented in a list, which should include a detailed description of the problems.

Second, known issues with the quality of data and information assets themselves should also be documented independent of the actual usage of the data and information assets—for example, many data fields in a table are empty or data is captured with many typing errors. There might already be software tools running to profile and check data (see Chapter 12 for an introduction and overview of how software tools can help you). If data profiling results relevant for the scope are easily available, they should be analyzed and documented.



ATTENTION

Be aware that data quality software tools (e.g., for data profiling) can only identify a small fraction of data and information quality problems!



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

By interviewing information managers for each IT system and database in the scope of the TIRM process, a number of general information management issues could be identified:

1. Call center agents often leave data fields empty.
2. Call center agents fill data fields with default values instead of the accurate values to reduce the amount of work they have to do.
3. Call center agents make spelling errors when they enter new customer master data.
4. Call center agents do not spend enough time describing the solution to an issue when a customer issue has been resolved.
5. The customer data that is provided by the client company is often in an incompatible format and needs transformation, which sometimes leads to problems.
6. The knowledge base is populated manually by the team leaders and business analysts; they include the keywords but often miss out the

Continued



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER—cont'd

recording of some relevant information that exists. It could be more analytically driven.

A data profiling software tool is applied to the three databases—customer master, customer interaction, and expert—that reveals many data quality issues, such as:

1. There are many duplicate customer records.
2. Many fields that can be used to describe an issue reported by a customer contain null values,

blank fields, or invalid values (descriptions that have less than three words).

3. Data on potential subject-matter experts also contains empty records for many keywords.

Having successfully established the context, the TIRM process sponsor and process manager decide that it is now time to move on to stage B to conduct the actual information risk assessment.

SUMMARY

This chapter presented how to establish the context for TIRM. It explained how to set the motivation, goals, initial scope, responsibilities, and context of the TIRM process, and how to establish the external environment. Then, you learned how to analyze the organization and how to identify business objectives, measurement units, and risk criteria as part of the TIRM process. Finally, it discussed how to establish an understanding of the information environment of your organization. The outputs of stage A will be used to facilitate information risk assessment in stage B and information risk treatment in stage C. The next chapter will present the core of the TIRM process, which is the identification, analysis, and evaluation of information risks.

REFERENCES

- Buchanan, S., & Gibb, F. (1998). The Information Audit: An Integrated Strategic Approach. *International Journal of Information Management*, 18(1), 29–47.
- Earl, M. J., & Khan, B. (1994). How New Is Business Process Redesign? *European Management Journal*, 12(1), 21.
- Grundy, T. (1993). *Implementing Strategic Change: A Practical Guide for Business*. London: Kogan Page.
- Harrison, R. (2007). *TOGAF Version 8.1*. Zaltbommel, Netherlands: Van Haren Publishing.
- Information Architecture Institute (2013). *What is Information Architecture?* Available at, http://www.iainstitute.org/documents/learn/What_is_IA.pdf.
- International Organization for Standardization (ISO) (2009). *ISO 31000:2009 Risk Management—Principles and Guidelines on Implementation*. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.
- Lewin, K. (1947). Frontiers in Group Dynamics: Concepts, Method, and Reality in Social Science; Social Equilibria and Social Change. *Human Relations*, 1(1), 5–41.
- Rose-Ackerman, S. (1999). *Corruption and Government: Causes, Consequences and Reform*. Cambridge: Cambridge University Press.
- Stevens, S. S. (1946). On the Theory of Scales of Measurement. *Science*, 103, 667–680.
- Trumbull, G. (2006). *Consumer Capitalism: Politics, Product Markets, and Firm Strategy in France and Germany*. Ithaca, NY: Cornell University Press.

- Wang, R. Y., & Strong, D. M. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*, 12(4):33.
- Weill, P. (2007). *Innovating with Information Systems: What Do the Most Agile Firms in the World Do?* Presentation at the Sixth e-Business Conference. Barcelona: Spain.
- Zachman, J. A. (1987). A Framework for Information Systems Architecture. *IBM Systems Journal*, 26(3), 276–292.

TIRM Process Stage B: Information Risk Assessment

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to identify information risks
- How to analyze and quantify information risks
- How to evaluate and rank information risks

INTRODUCTION

Motivation and goals for stage B

In many management seminars and lectures, it is taught that you can't manage what you can't measure. Information risk assessment measures information risk and is therefore at the heart of the TIRM process.

The goal of this stage is to conduct a thorough identification, analysis, and evaluation of information risks; this is crucial if you are to effectively manage information risks.

Information risk identification is important; you have to understand how and where information risks occur. This identification process addresses the following questions:

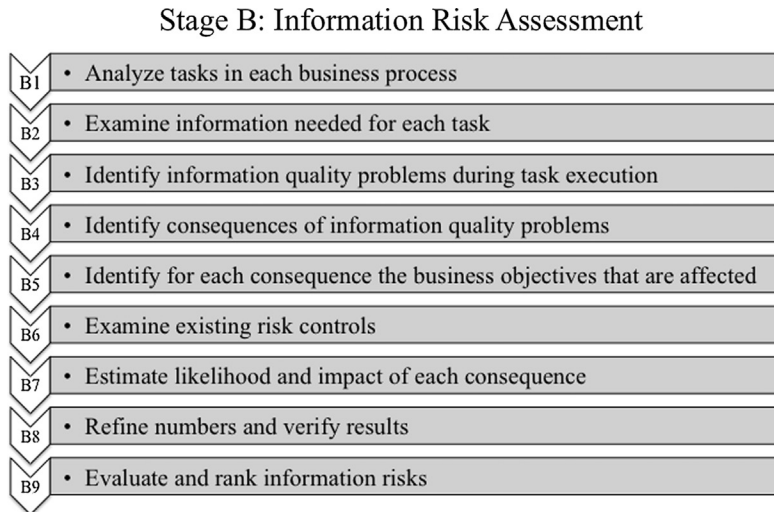
- Which information is critical for my business processes?
- Which information quality problems affect my organizational performance?

Information risk analysis is important in gaining an understanding of the likelihood and impact of these information risks. The analysis deals with the questions:

- What is the likelihood of each consequence of an information quality problem?
- How much does it affect my organizational performance?

Finally, information risk evaluation interprets the results into something that is truly meaningful. It focuses on answering the questions:

- So, what does it mean for my organization?
- How damaging are the identified information risks for my organization?
- Do I need to take action?

**FIGURE 7.1**

Nine steps to assessing information risk.

Overview of stage B

The goal of this stage is to identify, assess, and evaluate information risks in the scope previously agreed on in step A1; this is undertaken by following the nine steps shown in [Figure 7.1](#). Steps B1 to B4 identify information risks by analyzing the tasks executed in business processes, the data and information assets needed for those tasks, and the information quality problems during task execution. Then, the identified information risks are analyzed in steps B5 to B8 to gauge the probability of occurrence of consequences and the impact on business objectives. In step B9, information risks are evaluated against the identified risk criteria from step A4 to judge how significant they are for the organization and to compare different information risks with each other. This helps set the priorities for information risk treatment.

Output of this stage

The final output of this stage is a list of evaluated information risks. To measure information risks, it is essential to establish an understanding of:

- Analyzed tasks of selected business processes
- Information needed for those tasks
- Information quality problems when executing tasks
- The consequences of the information quality problems
- The impact of these consequences on business objectives

Information risks should be quantified, where possible, and verified by additional subject-matter experts. Eventually, information risks have to be evaluated regarding the information risk criteria set in stage A and a ranking of information risks has to be created that sets the priorities for information risk treatment.

Organizing stage B

For steps B1 to B7, a workshop has to be organized for each business process that was selected in step A1 with one or more business process representatives (who were also chosen in step A1) and the TIRM process facilitator. The business process representatives bring an in-depth understanding of the business process that is examined, whereas the TIRM process facilitator brings the procedural knowledge on how to identify and analyze information risks. For step B8, a workshop with additional subject-matter experts should be organized for each business process in the scope. Finally, an information risk evaluation workshop is required for step B9 with the TIRM process manager, process sponsor, and process facilitators. Additionally, selected important stakeholders should also participate because they will need to be involved in making the decisions as to which information risks should be treated and in which priority.



IMPORTANT

Steps B1 to B7 of the TIRM process, which identify and analyze information risks, have to be conducted separately for each business process.

STEP B1: ANALYZE TASKS IN EACH BUSINESS PROCESS

In this step ([Figure 7.2](#)), the tasks in each business process in the scope set in A1 are analyzed in preparation for the identification of information quality problems and risks in the business process, following the three activities shown in [Figure 7.3](#).

B1.1: Define tasks in business process

First, it is necessary to identify tasks, which are the key activities in a given business process. In a business process that deals with production planning, tasks can be, for example, drawing up a sales forecast; estimating the required output; determining the required methods, machines, manpower, and materials;

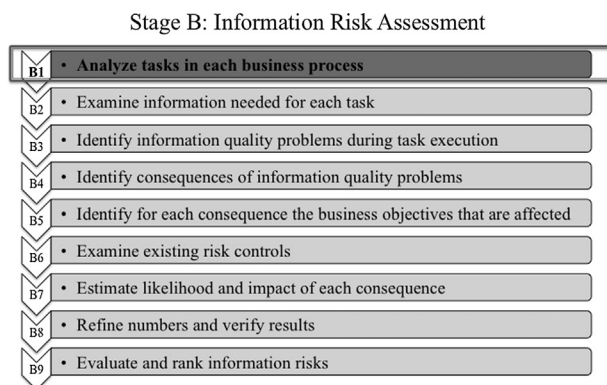


FIGURE 7.2
Step B1 in context.

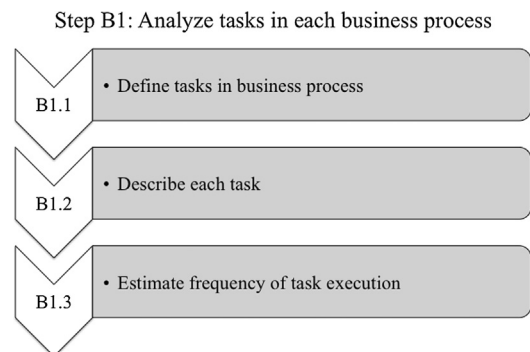


FIGURE 7.3
Activities in step B1.

and planning the production layout. In a business process that deals with machine maintenance, tasks can be, for example, the development of a maintenance strategy, the creation of maintenance schedules, the execution of the scheduled maintenance, and the requirement to undertake unplanned repairs.

Some tasks are executed automatically or by a single person, whereas other tasks can involve many people from different parts within or outside the organization. Sometimes tasks do not need to be executed by human beings; they can be performed by automated systems that require information input. A key activity in a business process can be monitoring a system that has been designed to intervene if something goes wrong.

It depends on the preferences of the organization as to which level of granularity tasks should be defined. There is no right or wrong here. A higher granularity has the advantage that the information risk model could be less complex at the end. A lower granularity makes it easier for the business process representatives to understand what is being examined. It is recommended that tasks are preferably defined at a high level of granularity to decrease the level of complexity in the analysis, but the tasks should be specific enough to be meaningful to relevant subject-matter experts.

To give an example, a sales forecast might be divisible into monthly and yearly sales forecasts. If these two tasks require completely different data and information assets, or are executed by different departments, or are actually totally different activities, it would make sense to divide the sales forecast task into two separate tasks for monthly and yearly.



IMPORTANT

The preferences of the organization will dictate the level of granularity on which tasks should be defined.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

In the call center, one of the business processes in the scope is the customer inquiry response process, which consists of

three tasks: identify customer, resolve problem, and collect customer feedback.

B1.2: Describe each task

Each task should be described in detail—there are four reasons why this should be done:

1. Executives and managers from other organizational functions who do not know the specifics of a business process should be able to read and understand the results from the information risk assessment.
2. It makes the tasks easily identifiable for other subject-matter experts. Everyone should clearly understand which task is being referred to, independent of the title of the task, which can be ambiguous.
3. It makes the communication with the process facilitator easier and avoids confusion.
4. And finally, even for the subject-matter expert, it is better to be very clear as to what the task is about before delving deeper into the analysis of information requirements.

So, how can we describe a task? It can be done simply by asking questions that start with *what*, *why*, *who*, *where*, and *when*, for example:

- What is done (and in what sequence)?
- Why is it done (what is the goal of the task)?
- Who executes/is responsible for/participates in the task?
- Where is the task executed?
- When is the task executed?



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

This is an example of a description for the task identify customer:

- *What is done (and in what sequence)?* When a customer telephones the call center, the customer needs to be identified. The customer is asked for his or her name and address.
- *Why is it done (what is the goal of the task)?* The query needs to be linked to a customer record, so that the system can provide the appropriate support that enables the query to be resolved and other call center agents know what took place when the customer made contact.
- *Who executes/is responsible for/participates in the task?* The call center agent is responsible for the task. The participants are the customer and the call center agent.
- *Where is the task executed?* The task is executed in the call center, on the telephone with the customer and by using the CRM system visible on the computer screen to identify the customer.
- *When is the task executed?* Every time a customer calls with an inquiry.

B1.3: Estimate frequency of task execution

To enable the quantification of information risk, the absolute frequency of task execution for each task should be estimated in a defined timeframe (e.g., per day, per month, per year, etc.); this estimation uses as its basis, the business process representatives' previous experiences.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

Each of these tasks always has to be executed when there is a customer inquiry (Figure 7.4). There are, on average, 430,000

customer inquiries per year, therefore, this is also the yearly frequency of task execution for all three tasks.

STEP B2: EXAMINE INFORMATION NEEDED FOR EACH TASK

In this step (Figure 7.5), for each task, data and information assets that are needed for the task are identified, described, and existing data and information assets are entered into a registry of data and information assets (Figure 7.6). Moreover, the likelihood that a data and information asset is needed for a task has to be estimated.

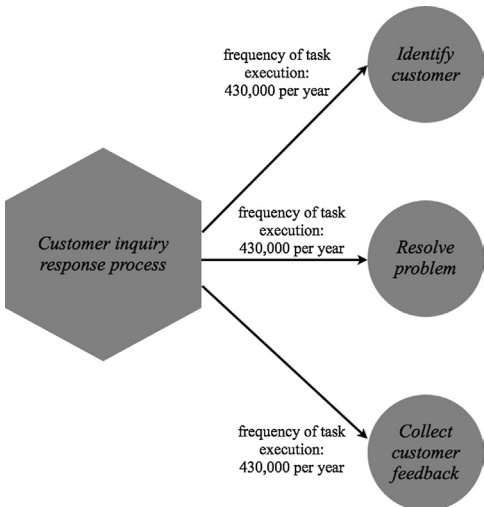


FIGURE 7.4

Example of tasks executed as part of a business process.

Stage B: Information Risk Assessment

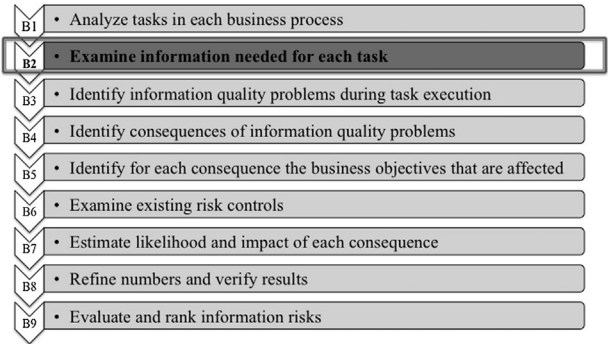


FIGURE 7.5

Step B2 in context.

Step B2: Examine information needs for each task

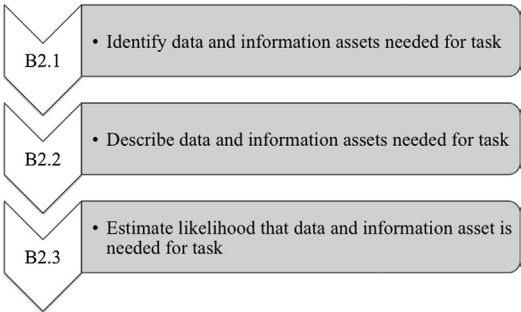


FIGURE 7.6

Activities in step B2.

B2.1: Identify data and information assets needed for task

This activity requires you to identify data and information assets that are required, or provide value for each task of a business process in the scope.

A data and information asset can be provided by a computer system—for example, CRM, ERP, or business intelligence (BI). The asset can also be stored and accessed as a file or document on the computer, such as a text document, presentation, or spreadsheet. Moreover, a data and information asset can be a physical document, such as, a hardcopy of a book, a form, a letter, a magazine, etc. Many

data and information assets are typically accessed as a web page. Information assets are also shared via mail and email or through personal communication, face to face, and via telephone. Information can also be obtained through observation. When a machine is broken, often a first step for an engineer is to take a look at it. If the production is not efficient, undertaking a tour of the production hall and carefully observing the production processes can sometimes generate information about what is wrong.

Should only data and information assets be considered if they are actually used for tasks? If so, this would miss out on some important information quality issues. Often, data and information assets are not used for a task, because of their poor quality or because they are not available when needed, although they would be of significant value for the success of the task. Imagine this situation: You are interested in buying a new TV and you have already selected a particular model that you wish to purchase. Knowing the prices in each store would certainly be highly useful information in this situation. There are websites where you can compare prices without much effort. But, what could happen if you knew that the information on price-comparison websites is actually inaccurate? You might use this information with the risk that you might end up paying a higher price. Or you could go to the websites of each retailer separately, which would take some time to find the model and price. If you had previous poor experiences with the accuracy of the price-comparison information, you could also decide not to use this information at all. Instead, you might check the price in a number of selected stores that you know and then make the purchasing decision. Yet, not using data and information assets although they are needed can create risks, as having information of poor quality would frequently lead to a better decision or performance of the task. It is, therefore, important to remember that data and information assets do not have to actually be used to be considered.



IMPORTANT

Data and information assets that would be of great value for a task are sometimes not available in an organization. They have to be included in the analysis since there might be a business case for an investment to make these data and information assets available.

Depending on the task, there can be hundreds or even thousands of different data and information assets that could potentially be useful for a task. But which data and information assets should really be included in the information risk analysis? In general, data and information assets should be only included when they are considered significant for the task by the business process representatives, which means that the use, or not use, of the information significantly influences the success of the task execution. The threshold to consider a data and information asset significant enough to be included depends on the amount of time you have available for the information risk assessment phase, as well as the opinions of the business process representatives. It is advisable to focus on the data and information assets most important for a task. Some data and information assets might not be considered at all as they are out of the process scope.

**ACTION TIP**

Try to think outside the box when you decide which information should be included in the analysis. Talking to business users and brainstorming with them can help.

**ACTION TIP**

Focus on the data and information assets that are the most important for the business process.

**EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER**

For each task, the business process representatives for the customer inquiry response process are asked to identify exactly which data and information assets are needed to execute the task. For customer identification purposes, customer relationship information is needed, which comes from the CRM system and the ITS, and is automatically shown on the screen by the CTI. For resolving a customer problem, information about previous solutions is needed, which is accessed using the ITS; this connects the

customer issue automatically with suggestions from the KBS. If the information is insufficient, advanced expertise is required from a subject-matter expert who needs to be identified using the KBS and contacted by the call center agent. Finally, for analyzing customer feedback, customer relationship information is also needed together with the data on customer feedback that is collected by the Computer Telephony Integration System (CTIS).

B2.2: Describe data and information assets needed for task

Each data and information asset should be described, in particular:

- Does the data and information asset exist in the organization?
- What is the type of data and information asset?
- Why is it important for the task?
- How can the information be accessed during task execution?

Moreover, if the data and information asset already exists in the organization, it should be included in a register of data and information assets, and if it is already in the register, the register should be updated. Therefore, this step creates a database with the data and information assets that you have identified. This can be done with a spreadsheet or with more sophisticated tools if required. It should capture the following items for each existing data and information asset:

- *Create a unique ID:* Each data and information asset should have a unique value that functions as an identifier. This makes sure which data and information asset is exactly meant and gives the relevant context to it.
- *Data and information asset title:* The title of the data and information asset should be a short textual description. If you are referring to a data and information asset that is describing the preferences of your hundred most important customers, a catchy title could be, for example, "Top 100 customer preferences."

- *Description of the content of the data and information asset:* A textual description that gives details about the content of the data and information asset is also required. It should describe, semantically, what the data and information asset is about, abstracted from its physical representation. For instance, a number field that is labeled “year” in a database is actually the physical representation of the year in which the product was introduced into the product catalog.
- *Description of how the data and information asset is captured and processed:* Describe how the data and information asset is created. In the case of data, there are applications that capture, process, or use the data (if information is saved as data).
- *Description of the storage of the data and information asset:* It is necessary to describe the format and place in which the data and information asset is stored. If the data and information asset is saved as data, a reference to the appropriate data fields and tables within the database is required. Documents require either a physical location (in case of hardcopy documents) or an electronic location (in case of electronic files).
- *Description of the way in which the data and information asset is accessed:* It is necessary to describe the different options available to access the data and information asset. This can be, for example, using a particular desktop or Internet software application to extract data directly from the database or a data warehouse. Information can also be accessed by communicating with other people via email, telephone, or face to face, or by accessing hardcopy documents.
- *Description of how the data and information asset is maintained and deleted:* This describes how information is kept up to date, modified, and deleted when required, and who is responsible for taking care of these activities.
- *People and business divisions that use this data and information asset:* This describes who uses the information and for which purpose. This field is built up incrementally. It is updated each time a task in the scope of the TIRM process requires this data and information asset.
- *Business processes that use this data and information asset:* This aims to describe which business processes the data and information asset is used in. This field is built up incrementally. It is updated each time a new business process in the scope of the TIRM process requires this data and information asset.
- *Degree of importance of data and information asset for this particular task:* This is used to rate how important the information is for the organization on a five-step scale from very low, low, medium, high, to very high. To complete the grade of importance it is necessary to also give a textual reasoning for the rating.
- *Degree of volatility:* This aims to store a rate of the degree of volatility of the data and information asset on a five-step scale from very low, low, medium, high, to very high, which is the speed at which the information is changing. Give a textual reasoning for the rating.
- *Identification of alternative data and information assets:* This is used to document if there are any other data and information assets that can be used as substitutes for the main one.
- *List of complementary data and information assets:* This is used to document if there are other complementary data and information assets that have to be used.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM process facilitator together with the business process representatives describes each data and information asset. An example is as follows:

- Create a unique ID: DIA.B.1.
- Data and information asset title: “Customer relationship information.”
- Description of the content of the data and information asset: This contains details about the customer, such as name, address, and date of birth, as well as details about the interaction history with the customer, including past issues raised by the customer and how they were resolved.
- Description of how data and information asset is captured, processed, stored, maintained, and deleted: See Chapter 6, substeps A5.1 and A5.2. Data is stored in the customer master and customer interaction databases. Data in the customer master database is initially obtained from the client company and then updated by the call center agents. Customer data has to be deleted when a client company decides to stop using the services of the call center. Data in the customer interaction database is automatically recorded during interactions with end customers. Issues raised by customers are entered by the call center agents into the system. The data comes from the ITS and the CTI system.
- Description of the way in which the data and information asset is accessed: It is accessed using the CTIS, which integrates the ITS and CRM system into the user interface.
- People and business divisions that use this data and information asset: Call center agents use this information.
- Business processes that use this data and information asset: The customer inquiry response process uses customer relationship information.
- Degree of importance of data and information asset for this task: This is very high since the customer cannot be identified without this information.
- Degree of volatility: This is medium since the customer master data does not change often, whereas issues reported by the customer are more volatile.
- Identification of alternative data and information assets: There are no real alternative options that can be used instead.
- List of complementary data and information assets: Data from the customer master and customer interaction databases are complementary, therefore, it is summarized as one data and information asset.

B2.3: Estimate likelihood that data and information asset is needed for task

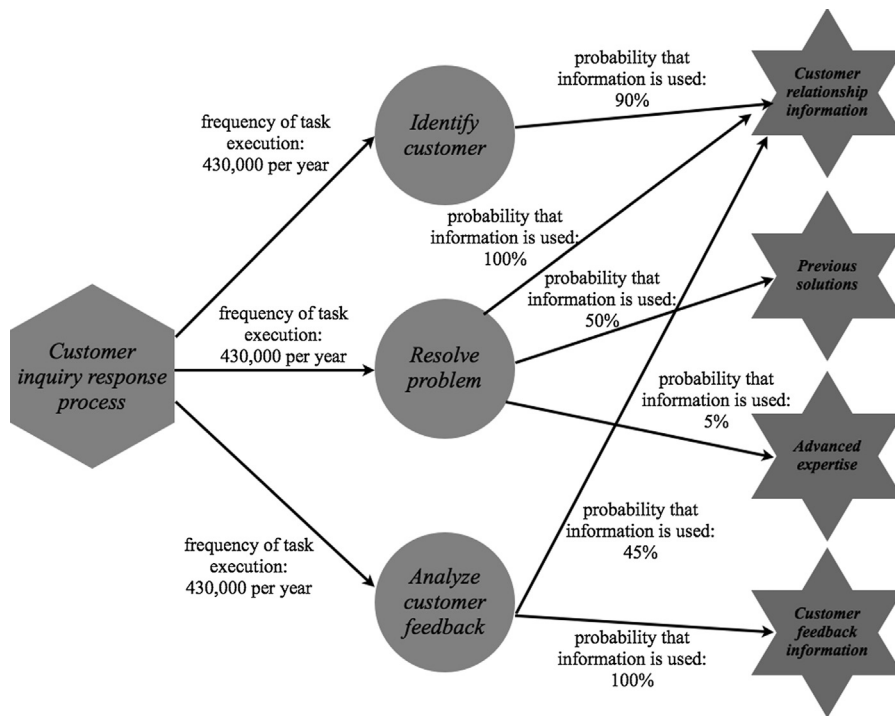
To be able to calculate the total risk at a later stage, the likelihood that the data and information asset is needed for the task has to be estimated. If a data and information asset is not needed, the probability is zero per definition. The numbers can be given in the same form as in step B1 of an exact value, a range, or as a three-parameters estimate.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

Figure 7.7 shows the four data and information assets that are needed in the customer inquiry response process and the likelihood that they are needed for the tasks. The data and information asset customer relationship information is needed with a likelihood of 90% when the identify customer task is executed. The customer relationship information is always required, while the data and information asset of previous

solutions is needed 50% of the time for the resolve problem task. The data and information asset of advanced expertise hotline is also needed for the resolve problem task, but only in 5% of cases. Finally, customer feedback information is always used (100%) for the analyze customer feedback task, while customer relationship information is needed only in 45% of cases when this task is executed.

**FIGURE 7.7**

Example of data and information assets used for tasks.

STEP B3: IDENTIFY INFORMATION QUALITY PROBLEMS DURING TASK EXECUTION

In this step (Figure 7.8), the quality of data and information assets needed for the task is evaluated. Additionally, potential information quality problems are identified and described and their likelihood of appearance is estimated (Figure 7.9).

B3.1: Evaluate quality of data and information assets needed for task

In the first step, each data and information asset that is required for a task should be evaluated from an information user's perspective by the business process representatives. Information quality is evaluated along the chosen dimensions in A1.3 to get a general impression of the information users' perceptions (Table 7.1). A five-level scale—very low, low, medium, high, or very high—can be used that indicates how fit for use a data and information asset is.

So what does this rating mean? It illustrates the perceptions of the business process representatives of the fitness for use of each data and information asset. The dimensions help to capture

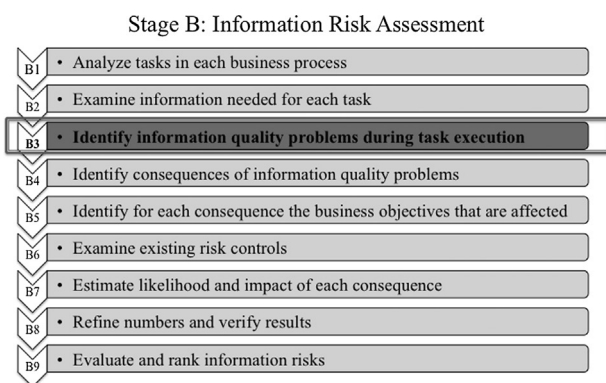


FIGURE 7.8
Step B3 in context.

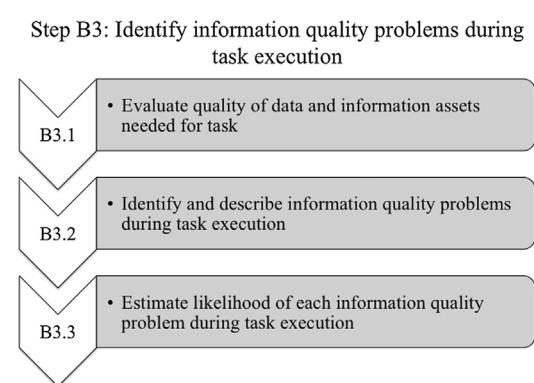


FIGURE 7.9
Activities in step B3.

Table 7.1 Standard Set of Information Quality Dimensions for TIRM	
Information Quality Dimension	Description
Accuracy	Is the data and information asset correct? Does it correspond to the real value that it represents?
Completeness	Is the data and information asset complete? Does it contain all the information it should contain?
Consistency	Is the information stored in a consistent format?
Up to date	Has information changed since the last time it has been updated in a way that it is incorrect now?
Interpretability	Is the content of the data and information asset easily interpretable by the users? Is it represented in a way that is easy to understand?
Accessibility	Can I access the data and information asset in a timely manner?
Availability	Is the information that I need available in my organization?
Security	Can somebody else access the information who should not be able to access it? How likely is it that the information gets lost?

the different aspects of quality as required by the corresponding users. There is, of course, the possibility of adding more information quality dimensions during this step, if it emerges that there are aspects of information quality that are not covered by the selected information quality dimensions.

The evaluation should take into account the known information management and information quality issues that were identified in substep A5.3 by interviewing information managers and using data quality software tools. Software tools that are intended to measure data and information quality usually measure some characteristics of the data stored in databases (see Chapter 12), which can be symptoms of poor data and information quality. The examples in the following box demonstrate that some

data defects can lead to varying levels of quality of the data and information asset depending on the task for which it is used. So, only by asking the information users can you really find out if a data and information asset is of high enough quality for a task.



ATTENTION

If half of the values of data fields are null, which means they are empty, this will probably have an effect on the fitness for use of that information for the many tasks that use this data and information asset. Similarly, if, for example, customer addresses are incorrect in the database, it will also affect the many tasks that use this information. However, some other tasks might not be affected at all. In the case of goods being sent to customers, spelling errors in the address, if not significant, do still lead to the goods being delivered to the right address. Yet, if an address has changed (i.e., is not up to date), it will prevent the goods from being delivered to the right address.

But, there might be instances where it is the other way around. Imagine you are running a sales campaign. The addresses of your customers might be an indication of where your future customers are concentrated, which enables you to send out your salespeople to the most promising geographical areas. An out-of-date address is still valid for this purpose, because it tells you where customers lived when they bought the product. Addresses with spelling errors, especially in the post code, might lead to an inaccurate analysis, which will compromise the task even more.

It should be emphasized that all this does not reduce the value of data profiling software and other data quality software tools. Knowing the data defects can often help identify information quality problems and prompt business process representatives to identify problems that they might not have been consciously aware of.

Having a good understanding of what high quality of a data and information asset in the light of each task means is something that can be very valuable for an organization. It tells the information managers how they should interpret the results of data quality software tools in the future and sets the requirements for data management. It also tells them which data defects they should put a special focus on in the future.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

For each task, business process representatives and information users evaluate the quality of each data and information asset; this takes into account general information management and information quality issues identified in substep A5.3. The results are shown in [Table 7.2](#). For example, the data profiling results revealed that data about previous solutions in the KBS is often incomplete, and contains many invalid or incorrect values. This is now confirmed by the users

of the information. As noted before, the quality of the same data and information asset might be high enough for one task, but low for another task. Each rating that is below high is described in more detail, for instance, medium accuracy of customer relationship information means that the name and contact details are often misspelled or incorrect, which has also been identified as a general information management issue in substep A5.3.

Table 7.2 Information Quality Assessment from a User's Perspective

Data and Information Asset	Customer Relationship Information			Previous Solutions	Advanced Expertise	Customer Feedback Information
Task	Identify Customer	Resolve Problem	Analyze Customer Feedback	Resolve Problem	Resolve Problem	Analyze Customer Feedback
Accuracy	Medium	High	High	Low	High	Medium
Completeness	Medium	Medium	Medium	Low	Very high	High
Consistency	Low	High	Medium	Medium	Medium	Very high
Up to date	Medium	High	Medium	Medium	High	High
Interpretability	High	Medium	High	Low	High	Medium
Accessibility	Medium	High	Medium	Low	Low	Very high
Availability	High	Very high	High	High	Low	Very high

B3.2: Identify and describe information quality problems during task execution

After having obtained an initial impression of the quality level of the data and information asset from the business process representatives, information quality problems are identified. An information quality problem arises when a data and information asset is not fit for the specific purpose of a task and this potentially influences the outcome of the task. Again, this is something that requires the judgment of the business process representatives who should have a good understanding of when a task can be significantly affected by poor information quality. If the level of information quality for a given set of dimensions was rated medium or lower, the business process representatives are asked to point out any resulting information quality problems. But, even if information quality is high or very high, the business process representatives should be asked if they are sure that there are no information quality problems resulting from poor information quality in some specific cases.

Each information quality problem should be described in more detail to make sure that other users can refer to the right information quality problem. Such a description should contain the defect that makes the data and information asset not fit for use (e.g., material codes used in production are inconsistent), but also how the task is potentially affected by this defect (e.g., the task of finding the materials that have the highest consumption rates in the production can lead to an incorrect analysis when it is based on inconsistent material codes). It should be explained under what circumstances the information quality problem can appear. Each information quality problem should be given a short title and be clearly linked to a particular data and information asset and specific task.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM process facilitator helps the business process representatives and information users identify a number of information quality problems that appear during the execution of each of the tasks.

An example is presented for the resolve problem task. The data and information asset of previous solutions is stored information about how previous customer inquiries have been resolved. However, it is sometimes hard to find the right record in the database, as there are hundreds of thousands of records of previous solutions. Searching for the right record requires a problem description of the current customer inquiry using a few keywords that are matched against words in the title of the problem description of previous customer inquiries. If, however, keywords are used that are

not contained in the title (e.g., when synonyms are used), the record will not be found—this is an information quality problem called finding the solution is difficult.

Another information quality problem with the data and information asset of previous solutions is that even once the right record is found in the database, it is often incomplete, called solution description incomplete.

The data and information asset of advanced expertise, which is only sometimes required for the resolve problem task, suffers from the information quality problem that experts are not available, which means that a subject-matter expert who has the advanced knowledge on the customer issue is not directly available when needed.

B3.3: Estimate likelihood of each information quality problem during task execution

Moreover, the likelihood that an information quality problem appears when information is used has to be estimated by the business process representatives. This can be done in the same way as in steps B1 and B2. For example, in 5% of cases, when the material codes are used for finding the materials that have the highest consumption rates in the production, the information is not fit for use for the task.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

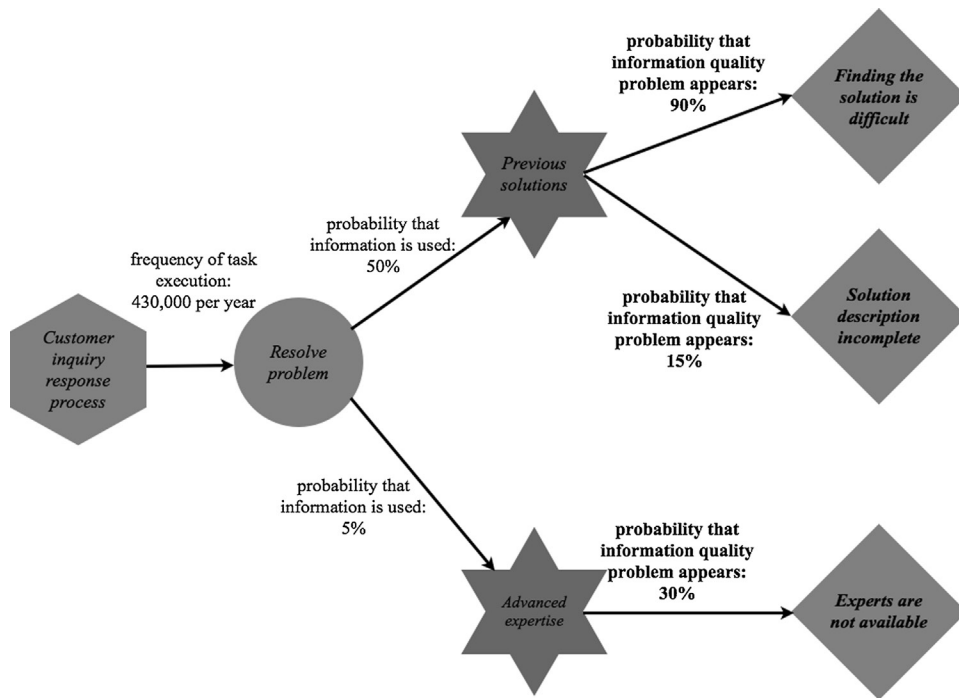
The information quality problems have been identified and now the business process representatives and information users estimate the likelihood of each problem.

Figure 7.10 shows, once again, the example of information quality problems appearing during execution of the resolve problem task.

The information quality problem finding the solution is difficult appears in 90% of cases when the information is needed for resolving a problem as part of the customer inquiry response process.

In 15% of cases when the data and information asset previous solutions is used for the resolve problem task, the information quality problem solution description incomplete appears.

Finally, the information quality problem experts are not available means that the required information is not instantaneously available in 30% of cases and, therefore, a delay occurs until an expert becomes available.

**FIGURE 7.10**

Example of information quality problems appearing during task execution.

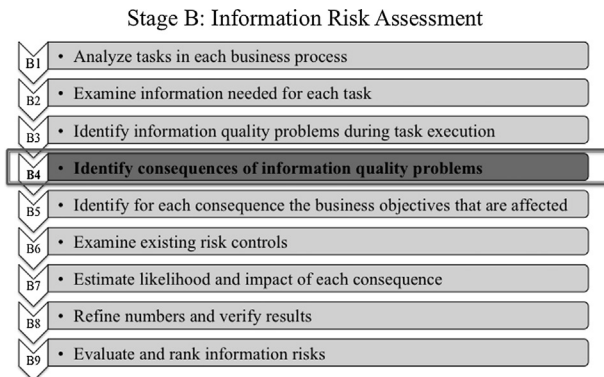
STEP B4: IDENTIFY CONSEQUENCES OF INFORMATION QUALITY PROBLEMS

In this step (Figure 7.11), the business process representatives identify and describe the direct and intermediate consequences of each information quality problem (Figure 7.12).

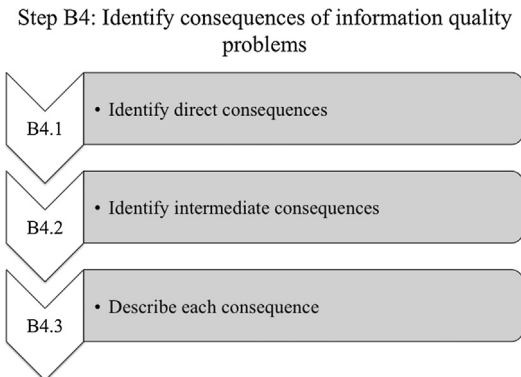
B4.1: Identify direct consequences

First, the business process representatives identify the direct consequences of each information quality problem.

The *direct consequences* should be directly related to the task in the business process in which an information quality problem appears. A direct consequence is usually that the task is delayed, it needs more resources for execution, or it is executed poorly, leading to an inferior task outcome. For example, when inconsistent material codes are used for finding the materials that have the highest consumption rates in the production, a direct consequence that can follow is that wrong materials are identified as the main cost drivers. There can be several direct consequences following from

**FIGURE 7.11**

Step B4 in context.

**FIGURE 7.12**

Activities in step B4.

an information quality problem. For instance, inconsistent material codes could also lead to more time and resources being spent when executing the task of analyzing the key materials cost drivers, because different material codes that represent the same material need to be unified before the actual task is executed.

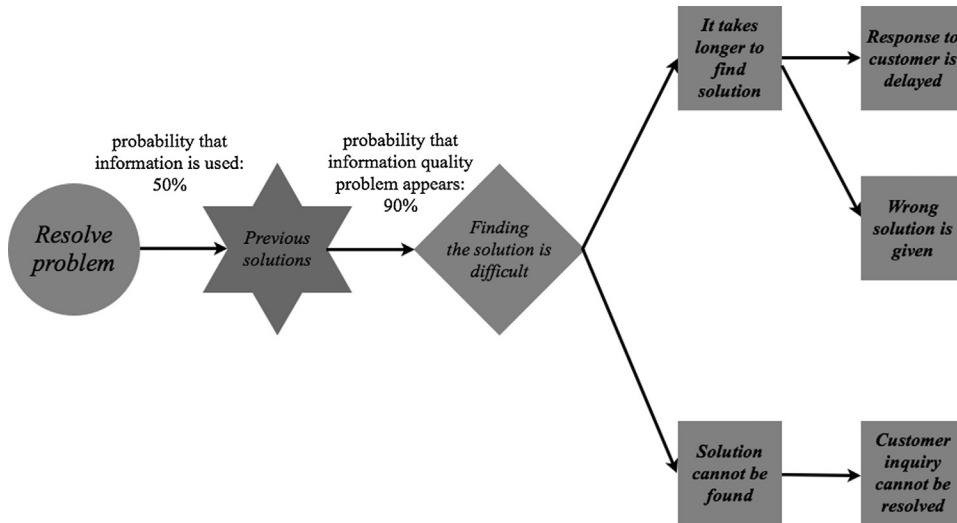
B4.2: Identify intermediate consequences

Second, the business process representatives identify the intermediate consequences of each information quality problem.

A direct consequence can lead to several further consequences, which can lead, in theory, to a never-ending chain of consequences. All consequences that do not result directly from an information quality problem, but are consequences of another earlier consequence, are called *intermediate consequences*. Other than the direct consequences, the intermediate consequences can appear in other activities, outside the business process or even beyond the boundaries of the organization. This could be, for instance, the inaccurate analysis of the amount of materials needed, which could lead not only to wrong purchasing decisions, but also to suppliers potentially optimizing their production by using misleading information. This could lead to price increases and it might ruin a relationship with a supplier and adversely affect future dealings.

B4.3: Describe each consequence

Each consequence should be given a textual description. The circumstances under which the consequence appears should be written down (when does it happen) and the consequence itself needs to be clearly described (what happens). The consequences should be visualized graphically to show how they are interlinked with the information quality problems and with each other, as shown in the example in [Figure 7.13](#).

**FIGURE 7.13**

Example of consequences of information quality problems.



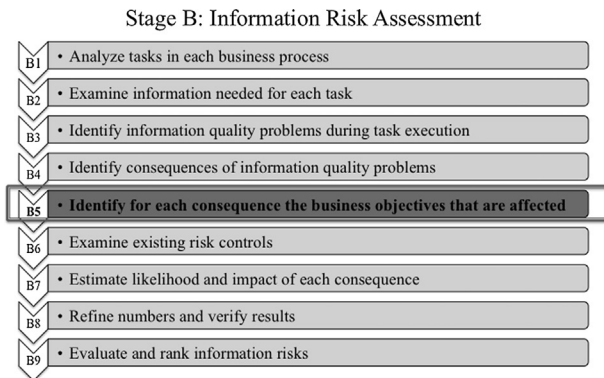
EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The information quality problem finding the solution is difficult can lead to two different direct consequences. The first direct consequence is that it takes longer to find a solution if the information quality problem appears during the task. This consequence causes a further intermediate consequence of the response to the customer is delayed. It can also sometimes lead to the consequence of the wrong

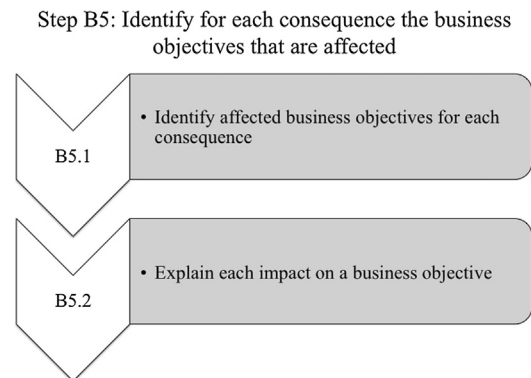
solution is given to the customer, because, after searching for a while, the service employee settles on a response that does not exactly fit the problem. The second direct consequence is that the solution cannot be found. This can lead to the intermediate consequence that the customer inquiry cannot be resolved.

STEP B5: IDENTIFY FOR EACH CONSEQUENCE THE BUSINESS OBJECTIVES THAT ARE AFFECTED

Business objectives represent what your organization aims to achieve, no matter whether these are financial or nonfinancial goals (Figure 7.14). Therefore, understanding which of the business objectives are impacted by which consequence will help you to evaluate the overall impact of an information risk on your organization's goal to achieve its business objectives (Figure 7.15).

**FIGURE 7.14**

Step B5 in context.

**FIGURE 7.15**

Activities in step B5.

B5.1: Identify affected business objectives for each consequence

For each consequence, you need to ascertain whether the consequence has a direct impact on one or more business objectives that were identified in substep A4.1.

Each consequence, independent of whether it is a direct or an intermediate consequence, can have an impact on one or more business objectives. So, the procedure is to go through each consequence one by one together with the business process representatives and discuss if the consequence could have an impact on one of the identified business objectives. A description as to how the consequence impacts the business objective is required—for example, the consequence of an ordered product cannot be delivered to the customer will surely impact on the business objective to achieve high customer satisfaction, as the customer cannot receive the product as expected.

But what happens if a consequence only has an impact sometimes, such as if customers are only dissatisfied when the delivery delay is greater than a week? This can be dealt with by adding a further consequence—for example, if an ordered product cannot be delivered to the customer, the consequence of the customer is dissatisfied as delivery delay is greater than a week can sometimes follow. Only the consequence of the customer is dissatisfied as delivery delay is greater than a week has an impact on the business objective to achieve high customer satisfaction.

B5.2: Explain each impact on a business objective

Explaining why and how each consequence has an impact on the business objective has to be documented. For instance, the consequence of the customer is dissatisfied as delivery delay is greater than a week has an impact on the business objective to achieve high customer satisfaction, because previous experience has shown that the average customer does not care too much about a delivery delay of less than one week, but usually gets angry and disappointed if the delivery delay is longer than one week.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

Together, the business process representatives and the TIRM process facilitator identify the impact of each of the direct and intermediate consequences of the discovered information quality problem on the business objectives that were defined in substep A4.1.

Figure 7.16 shows the previous example related to the resolve problem task extended to show the impact of consequences on business objectives. The direct consequence that it takes longer to find a solution has an impact on the business objective of operational

efficiency, as employees' time is wasted unnecessarily. The direct consequence of a solution cannot be found has no direct impact on a business objective. All three of the intermediate consequences of the response to the customer is delayed, the wrong solution is given, and the customer inquiry cannot be resolved have an impact on the business objective of customer satisfaction, as the customer is unhappy about the problem not being resolved in a timely fashion, resolved incorrectly, or not resolved at all.

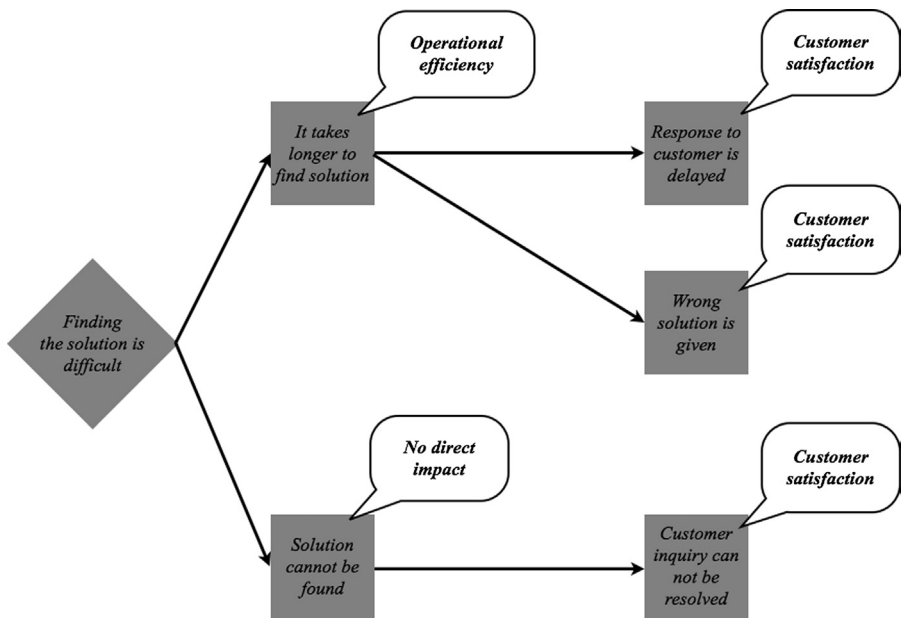
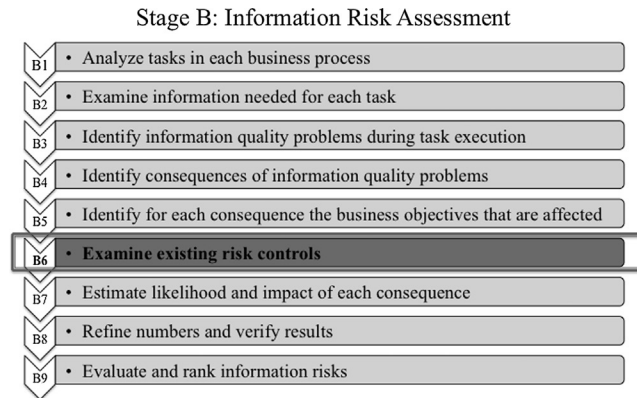


FIGURE 7.16

Example of consequences of impact of consequences on business objectives.

STEP B6: EXAMINE EXISTING RISK CONTROLS

This step (Figure 7.17) examines if there are existing risk controls in place to prevent information quality problems and/or their consequences from occurring. An example of a risk control can be an

**FIGURE 7.17**

Step B6 in context.

engineer who reads the opinions of other engineers published on the Internet before he or she uses an asset manual provided by a new supplier, because the asset manual can be unreliable.

This is important for step B7, when the likelihood and impact of each consequence are estimated, because you should take into account which risk controls are already in place. Moreover, it is also important for the selection of information risk treatment options in step C2, because choosing new options requires you to know which risk controls have already been implemented and how effective they are.

Also, note that if an existing risk control uses significant resources, the risk control can be checked for effectiveness and cost efficiency by modeling it as a consequence of an information quality problem (e.g., when time is wasted to improve the information). In some cases, risk controls can then be extended or replaced by a new risk control as part of the risk treatment in stage C.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

For each business process and task, the existing risk controls for consequences of information quality problems are identified by the business process representatives together with the TIRM facilitator. An example is shown in Figure 7.18. A risk control for the direct consequences of it takes longer to find a solution and a solution cannot be found is that another colleague is asked to help find the

solution in the KBS. This means that a second call center agent cannot make telephone calls during this time period. Furthermore, another risk control is that the problem is delegated to a subject-matter expert, because a solution cannot be found that uses the limited capacity of subject-matter experts, whose hourly rate is much higher than that of a call center agent.

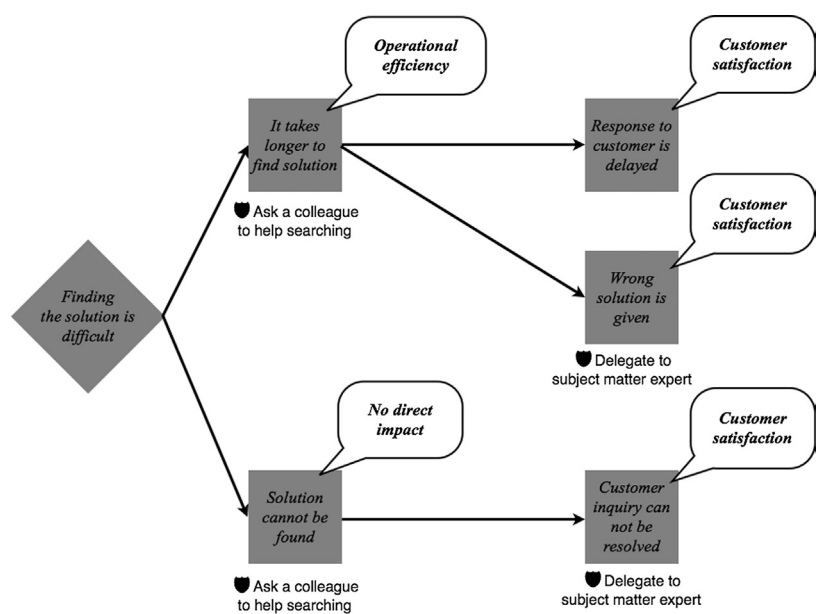


FIGURE 7.18
Example of risk controls.

STEP B7: ESTIMATE LIKELIHOOD AND IMPACT OF EACH CONSEQUENCE

In this step (Figure 7.19), for each consequence, a likelihood of occurrence and its corresponding impact are determined by giving due regard to the current risk controls that are in place; these determinations are based on previous experiences, existing data, and expert judgments (Figure 7.20).

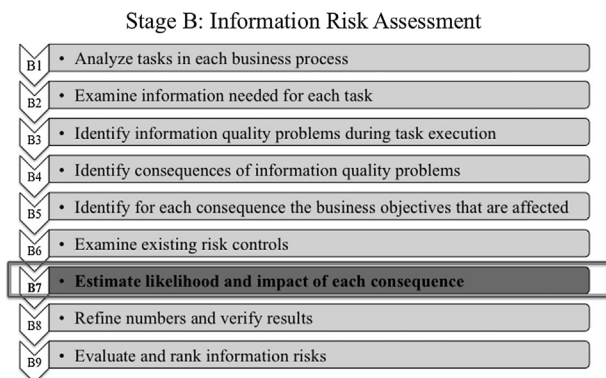


FIGURE 7.19
Step B7 in context.

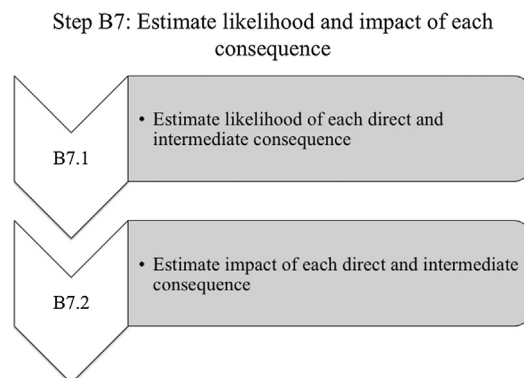


FIGURE 7.20
Activities in step B7.

B7.1: Estimate likelihood of each direct and intermediate consequence

First, the likelihood for each consequence has to be estimated. For a direct consequence, this is the likelihood that, when the information quality problem occurs, the direct consequence follows. For an intermediate consequence, this is the probability that a direct or other intermediate consequence leads to the intermediate consequence.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

As in the previous steps, the TIRM process facilitator together with the business process representatives estimate the figures. The example of the resolve problem task is continued (Figure 7.21).

There is a likelihood of 15% that the information quality problem of finding the solution is difficult leads to the direct consequence that it takes longer to find a solution. The direct consequence of a solution cannot be found follows from this information quality problem with a likelihood of 5%.

Afterwards, the likelihoods of the intermediate consequences have to be estimated. In the example shown, the direct consequence that it takes longer to find a solution leads to the intermediate consequence of a response to the customer is delayed with a likelihood of 70% and to the intermediate consequence that a wrong solution is given with a likelihood of 3%. Furthermore, the direct consequence that a solution cannot be found leads to the intermediate consequence of a customer inquiry cannot be resolved with a likelihood of 20%.

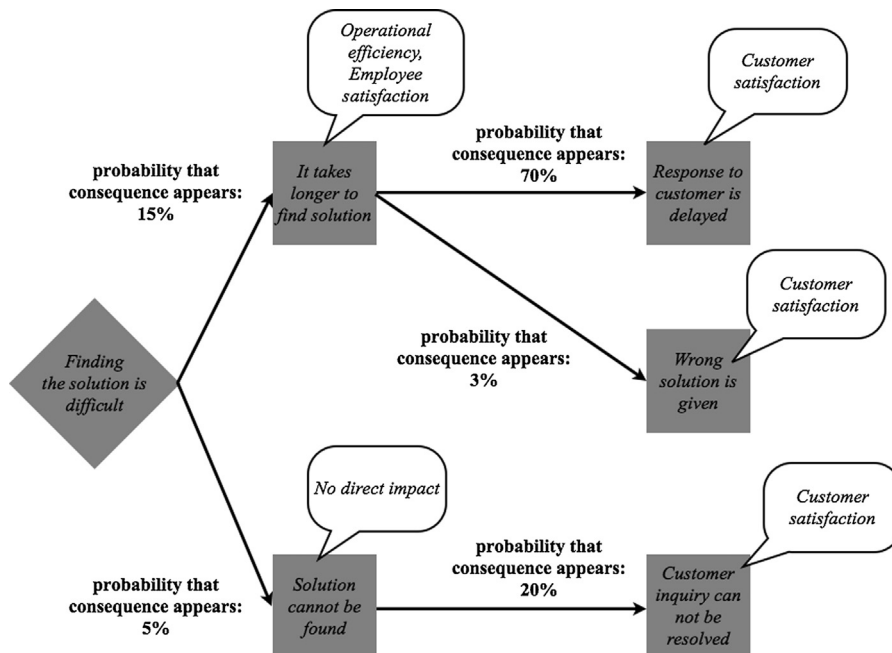


FIGURE 7.21

Example of adding the probability to each consequence.

B7.2: Estimate impact of each direct and intermediate consequence

Eventually, when a consequence has an impact on one or more business objectives, the impact has to be estimated in the measurement unit specified for the business objective. If a consequence does not have an impact, for example, on the business objective of health and safety, the value for the impact on this business objective would be zero. Moreover, if the consequence does not have any impact on any of the business objectives, all values in the vector would be zero per the definition.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

Figure 7.22 shows the extended example; here, the figures for the impact on business objectives have been added for each of the consequences. The direct consequence that it takes longer to find a solution causes a loss of \$20 each time, because the employee's time is wasted trying to find the right solution in the database. The direct consequence that a solution cannot be found has no direct impact on any business objectives. Moreover, the intermediate consequence

of a response to the customer is delayed has an impact of 0.1, the intermediate consequence of the wrong solution is given has an impact of 0.9, and the intermediate consequence that a customer inquiry cannot be resolved has an impact of 0.5 on the business objective of customer satisfaction. This is because a delay of the solution is not as bad as if a customer inquiry cannot be resolved, but it is even worse if an incorrect solution is given to the customer in our example.

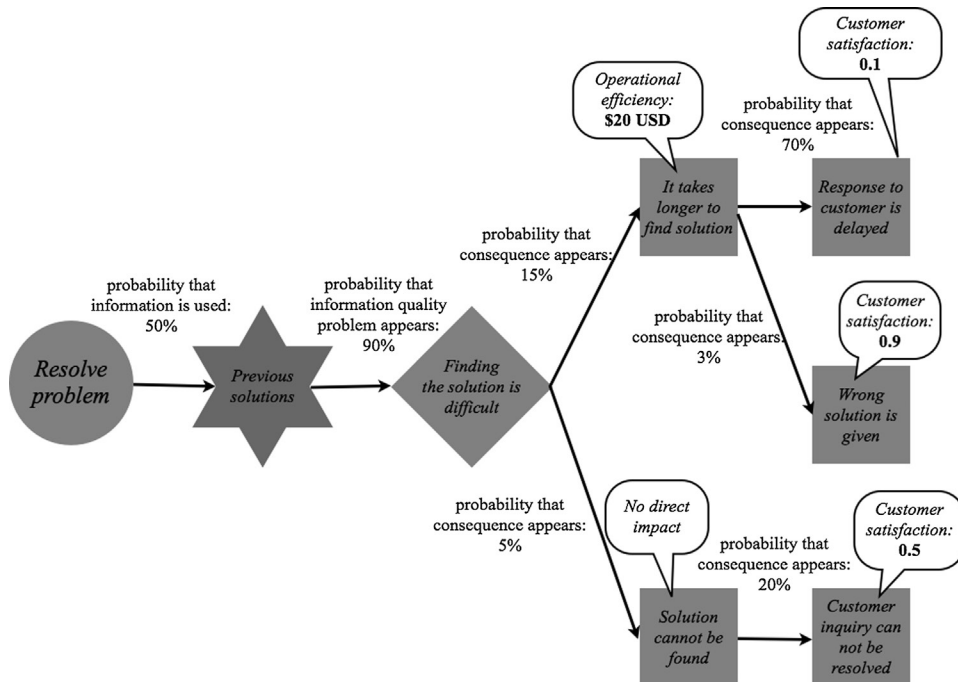


FIGURE 7.22

Example of adding the impact to each consequence.

STEP B8: REFINE NUMBERS AND VERIFY RESULTS

For each business process, further subject-matter experts should be chosen to refine the numbers and verify the results from the information risk analysis to reduce any bias in the input (Figure 7.23).

If possible, historical data should be used to improve the reliability of the data input. Sometimes, it is advisable to collect further data where feasible or execute enhanced data analysis to improve the numerical input.

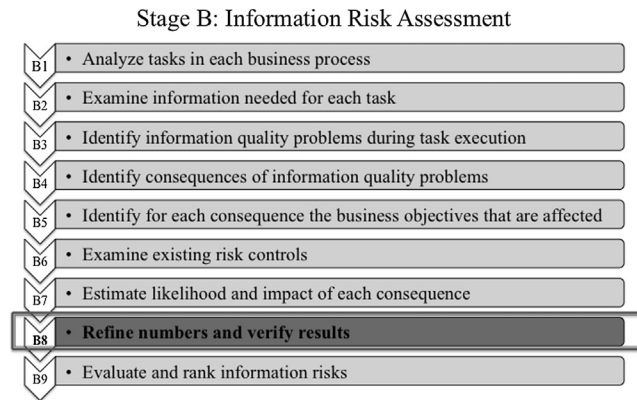


FIGURE 7.23

Step B8 in context.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

For step B8, the TIRM process facilitator identifies further subject-matter experts for each of the three business processes in the scope of the TIRM process within the call center, who get a chance to refine the outputs of steps B1 to B7. Some of the numbers are adjusted and some of the consequences are modeled in a slightly refined way. The changes are discussed with the business process representatives who originally provided the inputs.

The previous example is used once again to illustrate how this is done. The tools symbol shows where numbers have been refined in the resolve problem task. The likelihood that

the information quality problem of finding the solution is difficult occurs has been estimated too highly at the outset (90%) and is now reduced to 60% after having consulted with a number of call center agents. Moreover, the likelihood that when a solution cannot be found the customer inquiry cannot be resolved is much higher than originally anticipated at 50% rather than 20%. Also, it was discovered that the consequences of a solution cannot be found and the wrong solution is given both impact the business objective of operational efficiency, as they create follow-up costs for operations of \$150 and \$40 USD per instance. See Figure 7.24.

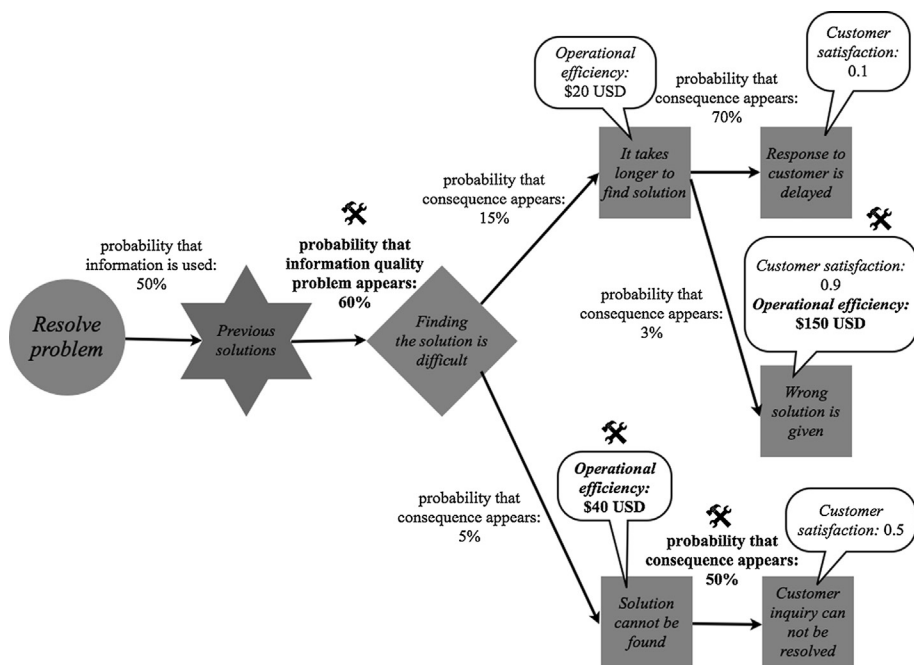


FIGURE 7.24

Refinement of numbers and results.

STEP B9: EVALUATE AND RANK INFORMATION RISKS

In this step (Figure 7.25), the expected overall impact of each information quality problem is calculated, evaluated, and, finally, information risks are ranked in a list. The activities of this step are shown in Figure 7.26.

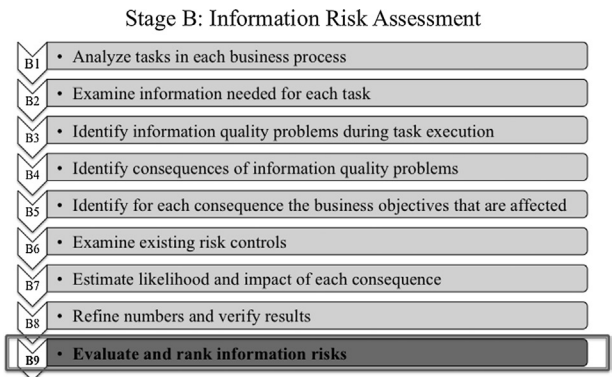


FIGURE 7.25

Step B9 in context.

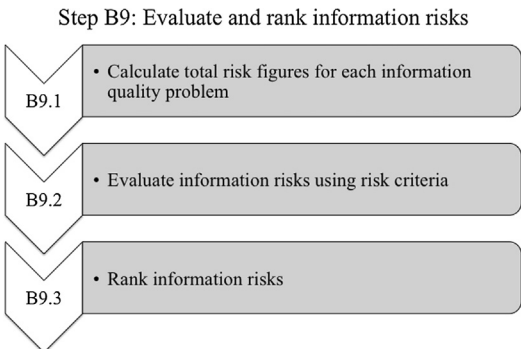


FIGURE 7.26

Activities in step B9.

B9.1: Calculate total risk figures for each information quality problem

This is a list of quantitative estimates that were collected as part of steps B1 to B8:

- B1: yearly frequencies of task execution
- B2: likelihood that data and information assets are needed for task
- B3: likelihood that the information quality problem appears when information is used for the task
- B7: likelihood that consequences appear and impact of each consequence on business objectives

This input can be now used to calculate the total risk caused by an information quality problem.

The expected total risk of an information quality problem can be calculated as the product of the following factors:

The yearly absolute frequency of the information quality problem $\times$ *the sum of* (the likelihood of the direct consequence $\times$ the overall impact of the direct consequence) *for all direct consequences*.

This calculation has to be done separately for each business objective, as each business objective is measured using a different metric. Moreover, it is useful to the decision maker to understand which business objective is affected by how much and by which particular information quality problem. The calculation can be done directly if estimates are in the form of a single number. If ranges or three parameters are given, you need to run a Monte Carlo simulation (see Chapter 11), which is best done with the assistance of an appropriate software tool, such as InfoRAS presented in Chapter 12.

While the likelihood of each direct consequence is available as input collected in step B7, the yearly frequency of the information quality problem must be calculated using equation (A) and the overall impact of a consequence has to be calculated using equation (B).

(A) *The yearly absolute frequency of the information quality problem* is the product of the following factors:

- The yearly frequency of task execution (collected in step B1) $\times$
- The likelihood that a data and information asset is needed (collected in step B2) $\times$
- The likelihood that the information quality problem appears in a task when information is needed (collected in step B3).

(B) A consequence c causes $1..N$ further consequences. The overall impact of a consequence c is hence the direct impact of the consequence c on business objectives (collected in step B7) multiplied by the sum for each further consequence $n=1..N$ of the following products:

- The likelihood that the further consequence n is caused by consequence c (collected in step B7) multiplied by
- The overall impact of the further consequence n (which needs to be calculated recursively using this equation).

Therefore, it is a recursive calculation, because for calculating the overall impact of a consequence, you need to calculate the overall impact of each of the consequences that are caused by this consequence.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM process manager now wants to know what the total information risk figures in each of the business processes are. We will use the example of the resolve problem task in the customer inquiry response process to demonstrate how these calculations are made. Figure 7.27 shows the final version of the example model created using the TIRM process.

So, the goal is to calculate the total risk of the information quality problem of finding the solution is difficult. There are two business objectives that can be affected in this example: operational efficiency and customer satisfaction. The total risk is a vector of values for these two business objectives.

First, we calculate *the yearly absolute frequency of the information quality problem* as the product of the following factors:

- The yearly frequency of executing the task resolve problem (see step B1): 430,000.
- The likelihood that the data and information asset of previous solutions is needed for this task (see step B2): 50%.
- The likelihood that the information quality problem of finding the solution is difficult appears when the data and information asset is needed for the task (see step B3): 60%.

Therefore, the yearly absolute frequency of the information quality problem is:

$$430,000 \text{ times per year} \times 50\% \times 60\% = 129,000 \text{ times per year}$$

Next, we need to calculate the overall impact of each of the direct consequences, for which we need to first know the *overall impact of each intermediary consequence*. The overall impact of the intermediary consequence that the response to a customer is delayed is (\$0, 0.1), as only the business objective of customer satisfaction is affected by this consequence. There are no further consequences caused by this consequence, therefore, the overall impact of this consequence equals its direct impact. Similarly, the overall impact of the wrong solution is given is (\$150, 0.9) and of the customer inquiry cannot be resolved is (\$0, 0.5).

Using the overall impact of the intermediate consequences, the *overall impact of each direct consequence* can be now

calculated. The overall impact of the direct consequence that it takes longer to find a solution can be calculated as the product of the direct impact of this consequence multiplied by the likelihood of each consequence multiplied by its overall impact:

$$(\$20, 0) + 70\% \times (\$0, 0.1) + 3\% \times (\$150, 0.9) = (\$20, 0) + (\$0, 0.07) + (\$4.5, 0.027) = (\$24.5, 0.097)$$

This means that each time the consequence that it takes longer to find a solution occurs, the expected impact on operational efficiency is \$24.5 USD and that 0.097 customers are dissatisfied (this is, of course, a theoretical value, as there can be either one or zero customers dissatisfied—it only gets meaningful once we aggregate it).

Similarly, the overall impact of the direct consequence that the solution cannot be found is calculated as:

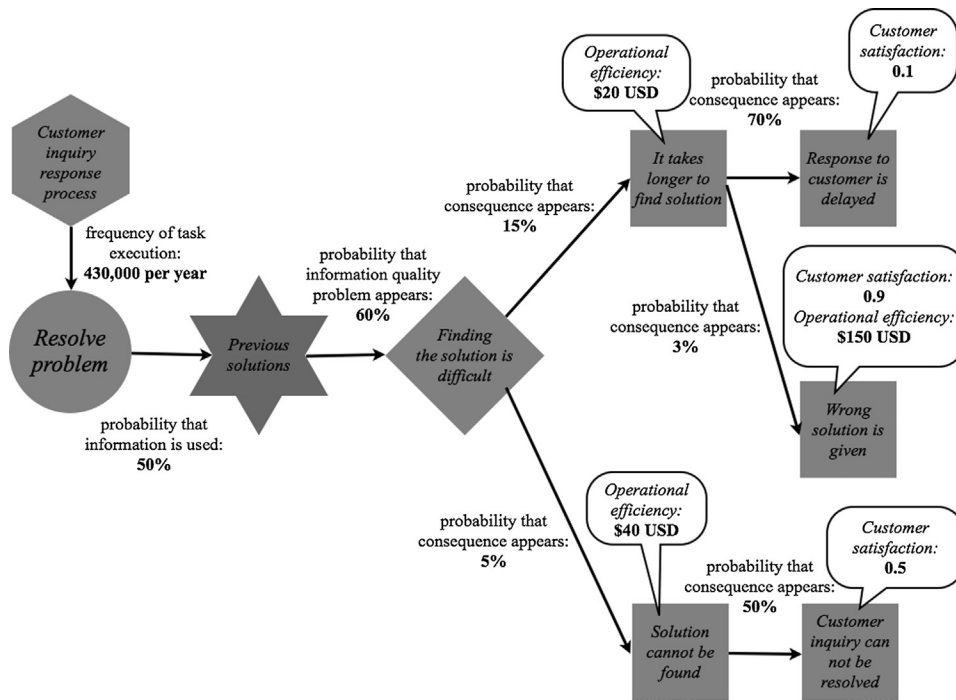
$$(\$40, 0) + 50\% \times (\$0, 0.5) = (\$40, 0) + (\$0, 0.25) = (\$40, 0.25)$$

Now, we can calculate the total expected risk of the information quality problem of finding the solution is difficult in resolve problem task, which is:

The yearly absolute frequency of the information quality problem $\times$ *the sum of* (the likelihood of the direct consequence $\times$ the overall impact of the direct consequence) *for all direct consequences*.

$$\begin{aligned} &129,000 \text{ times per year} \times (15\% \times \text{total impact of direct consequence that it takes longer to find a solution} + 5\% \times \text{total impact of direct consequence that the solution cannot be found}) \\ &= 129,000 \text{ times per year} \times (15\% \times (\$24.5, 0.097) + 5\% \times (\$40, 0.25)) \\ &= 129,000 \text{ times per year} \times ((\$3.675, 0.01455) + (\$2, 0.0125)) \\ &= 129,000 \text{ times per year} \times (\$5.675, 0.02705) \\ &= (\$732,075, 3489.45) \text{ per year expected total information risk caused by the information quality problem of finding the solution is difficult} \end{aligned}$$

Therefore, the expected yearly impact of the information quality problem of finding the solution is difficult on cost efficiency is roughly \$732,000 USD and around 3490 callers who are dissatisfied.

**FIGURE 7.27**

Final version of example model.

B9.2: Evaluate information risks using risk criteria

Once the annualized cost for the information quality problem has been calculated, the analyzed information risks (an information quality problem that has an impact that corresponds to an information risk) are compared to the risk criteria from substep A4.3.

This is used to evaluate the information risk on a five-level qualitative scale of very low, low, medium, high, or very high. The level of risk is also used to decide if the information risks are tolerable or if they require treatment.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

To evaluate information risks, the TIRM process manager compares the expected impact with the risk criteria. As a reminder, these are the risk criteria that were set in substep A4.3.

The following are the risk criteria for the business objective of operational efficiency measured in yearly lost revenue in USD and yearly higher operational costs in USD.

Very low	\$0	—	\$50,000	
Low	\$50,001	—	\$250,000	
Medium	\$250,001	—	\$500,000	
High	\$500,001	—	\$1,000,000	Not tolerable
Very high	\$1,000,001	—	Unlimited	Not tolerable

The following are the risk criteria for the business objective of customer satisfaction measured in the number of dissatisfied callers.

Very low	0	—	1000	
Low	1001	—	2000	
Medium	2001	—	3000	
High	3001	—	5000	Not tolerable
Very high	5001	—	Unlimited	Not tolerable

The expected yearly impact of the information quality problem of finding the solution is difficult on cost efficiency is around \$732,000 USD and 3490 callers who are dissatisfied. This means that the information risk is evaluated as high regarding both business objectives of operational efficiency and customer satisfaction and therefore the information risks are not tolerable and require treatment.

B9.3: Rank information risks

Information risks can then be ranked, giving due consideration to the total expected risks for each business objective and taking into account the organization’s current priorities. The ranking determines the priorities for the information risk treatment stage.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

Once all the other steps have been completed for the three business processes in the scope of the TIRM process at the call center, the TIRM manager creates a ranked list of information risks (Table 7.3). For the call center, customer satisfaction is a slightly higher priority than operational efficiency, since the call center is in a premium segment in which service quality plays a very important role (compare with outputs in steps A2 and A3).

The ranked list of information risks sets the priorities for treating information risks in stage C. Having assessed the information risks in the call center successfully, the TIRM process manager and process sponsor decide that it is now time to move on to the information risk treatment stage of the TIRM process.

Table 7.3 Ranked List of Information Risks at Call Center

Rank	Information Risk Title	Impact on Operational Efficiency	Impact on Customer Satisfaction
1	Customer data is incomplete and incorrect	\$518,000 (High)	6000 dissatisfied callers (Very high)
2	Finding the solution is difficult	\$732,000 (High)	3490 dissatisfied callers (High)
3	Experts are not available	\$285,000 (Medium)	3100 dissatisfied callers (High)
4	Customer feedback information is difficult to interpret	\$150,000 (Low)	2450 dissatisfied callers (Medium)

SUMMARY

This chapter has provided you with step-by-step guidance on how to identify, analyze, and evaluate information risks. The output of stage B is a ranked list of information risks in all business processes in the scope of the TIRM process, with quantitative values for the expected impact for each of the defined business objectives. The output of stage B will guide the treatment of information risks in stage C, which is explained in Chapter 8.

TIRM Process Stage C: Information Risk Treatment

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to identify causes of information risks
- How to find appropriate treatments for information risk
- How to determine the costs, benefits, and risks of information risk treatments
- How to evaluate, select, and communicate information risk treatments to stakeholders
- How to implement information risk treatments and verify their effectiveness

INTRODUCTION

Motivation and goals for stage C

Assessing information risks does not create much benefit if those assessments are not used later to mitigate the information risks. Information risk treatment is therefore the action phase; here, changes to working practices and procedures are made, enabling an organization to be better able to control information risks. These changes can be made in business processes, hardware, software, policies, and organizational structure. The changes can be either incremental or disruptive. ISO 31000 describes risk treatment as “selecting one or more options for modifying risks, and implementing those options” (ISO, 2009, p. 18).

Overview of stage C

Information risk treatment is carried out by following eight steps (Figure 8.1). First, the causes of information quality problems that lead to the major information risks are analyzed in step C1. Based on the actual causes of information risks, appropriate information risk treatments are identified in step C2, for which the costs, benefits, and implementation risks are estimated in step C3. The potential information risk treatments are evaluated and the best treatments are selected in step C4. The list of information risks and selected information risk treatment are then communicated to all key stakeholders in step C5 to obtain their feedback and buy-in for the implementation stage. In step C6, information risk treatment plans are developed, which are implemented in step C7. Finally, the effectiveness of the information risk treatments is verified in step C8. Information risk treatment is a cycle that only ends when an information risk becomes tolerable or reaches a level that is satisfying.

Stage C: Information Risk Treatment

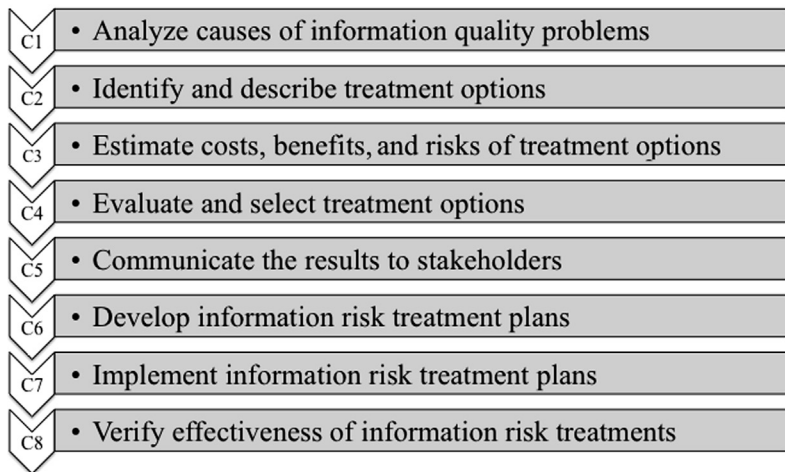


FIGURE 8.1

Eight steps to treating information risk.

Three types of workshops can be organized for stage C. The first workshop is information risk treatment identification, the purpose of which is to analyze the causes of information quality problems in step C1 and identify and analyze potential information risk treatments in step C2. This is usually a one-day workshop, but it could also take much longer if the scope of the TIRM process is particularly wide-ranging. It should involve the process manager, process facilitator, one or two business process representatives, and one or two IT representatives.

The second workshop is information risk treatment selection, the purpose of which is to identify the costs, benefits, and risks of each information treatment option in step C3; participants in this workshop should be the same people as in the previous workshop with the addition of the process sponsor. The second workshop also normally takes one day, but, again, it depends on the scope of the TIRM process. An evaluation, of which treatment options should be recommended to the decision makers in the organization, should be undertaken as part of this workshop; the decision makers will have the final say as to which information risk treatment options are to be implemented.

The third workshop is for step C6 and its purpose is information risk treatment plan development, which, as the name says, is to develop information risk treatment plans for the information risk treatments that were selected. The duration of the workshop and its participants should mirror those of the first workshop.

Output of this stage

The outputs of stage C are:

- An analysis of the causes of each information quality problem.
- A preselection of appropriate information risk treatment options.
- A cost, benefit, and risk analysis of the treatment options.
- A ranked list and evaluation of information risk treatment options.

- An implementation plan for each selected information risk treatment option.
- An implementation report for each selected information risk treatment option.

STEP C1: ANALYZE CAUSES OF INFORMATION QUALITY PROBLEMS

The information risk assessment stage has created a ranked list of information risks that require treatment. In this step ([Figure 8.2](#)), the causes of the information quality problems that lead to these risks are analyzed. In many information quality methodologies, this step is also called *root cause analysis*. David Loshin describes it as “an iterative process of analyzing a problem to determine the actual cause” ([Loshin, 2001](#), p. 382).

Information quality problems are caused by a variety of reasons. The causes can be technological, organizational, or human. An example of a technological cause is that software is poorly implemented or not available. An organizational cause can be that a business process to update customer data is not clearly defined. An example of a human cause could be that employees are not sufficiently motivated to collect data of high quality or they make errors during data entry. So, you can classify the causes and categorize them on the basis of whether they are technological, organizational, or human.

In this step, the causes of information quality problems are identified and then ranked on the basis of their importance ([Figure 8.3](#)).

C1.1: Identify causes of information quality problems

First, the causes of information quality problems need to be identified. This can be done in a number of different ways.

A simple method suggested by Danette McGilvray is to ask five “why” questions to get to the source of the problem ([McGilvray, 2008](#)). The questions do not have to actually start with the word “why,”

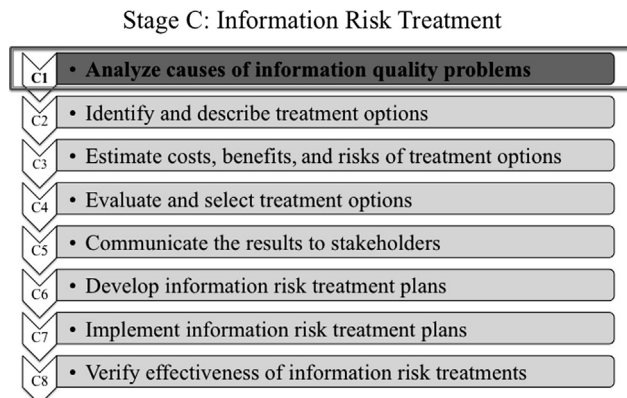


FIGURE 8.2

Step C1 in context.

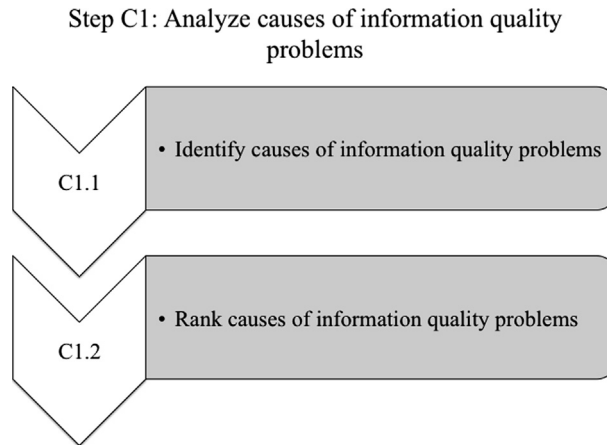


FIGURE 8.3
Activities in step C1.

but each question should lead closer to the actual cause of the information quality problem. For example:

- Why is the customer data incorrect? Because it is out of date.
- So, why is the customer data out of date? Because nobody updates the customer data.
- So, why does nobody update the customer data? Because there are no formalized processes and requirements to update the customer data.
- So, why are there no formalized processes and requirements? Because there is no entity in the organization responsible for governing data.

Information quality problems are caused at some point during the information life cycle. The information life cycle can be divided into a number of different stages—for example, when information is created and collected, processed and stored, accessed and used, maintained and updated, and disposed of. It is reasonable to identify causes of information quality problems along the information life cycle. Using the information flow maps created in substep A5.2 as a basis does this.

Another method that is used in information quality (IQ) management and risk management to model the causes of problems is the Fishbone diagram (McGilvray, 2008; see also Chapter 11), which “is structured by separating causes into major categories (represented by the lines of the fish backbone) with branches and sub-branches that describe more specific causes in those categories” (ISO, 2009, p. 57). The position of the cause in the information life cycle and the technology, organization, and people (TOP) classification can be used as the categories in the fishbone diagram. An example is shown in Figure 8.4.

C1.2: Rank causes of information quality problems

The identified IQ causes should be prioritized based on the severity of the resulting information risks and the degree to which each cause can be modified. As several IQ problems can have the same causes, one information risk treatment might mitigate a number of different information risks. A ranked list should be created that will help prioritize information risk treatment options.

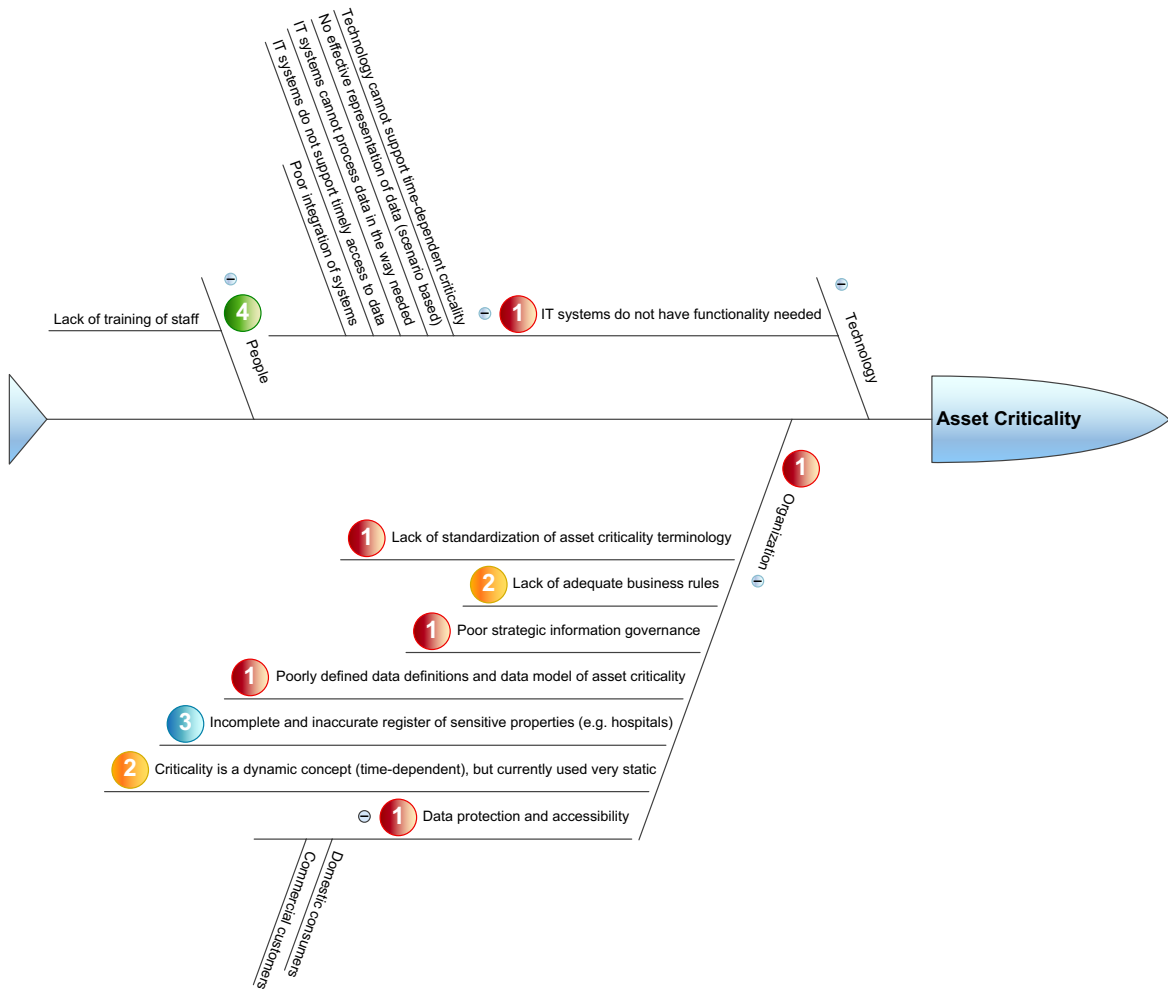


FIGURE 8.4

Illustration of a fishbone diagram for information quality root-cause analysis.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

In stage B of the TIRM process, four information quality problems were identified that cause information risks in the three business processes. These are in the scope of the TIRM process initiative at the call center. As a reminder, the ranked table of information risks is shown in [Table 8.1](#).

The TIRM process manager wants to now identify the causes of each of the information quality problems.

Together with the TIRM process facilitator and the IT system and database representatives, he first investigates where, in the information processing chain, the causes of the information quality problem could be generated. Looking at the information flow map created in substep A.5.2 does this ([Figure 8.5](#)), and finds the spots along the information life cycle where the causes might lie.

Continued



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER—cont'd

We will illustrate it for the information quality problem that customer data is incomplete and incorrect. One example for an issue at the beginning of the information life cycle is that call center agents input data fields with default or invalid values, make spelling errors, or leave fields empty during information creation. During the information maintenance life-cycle stage, data decays over time when it is not maintained properly by the call center agents and the client company.

As a next step, for the information quality problem that customer data is incomplete and incorrect, the team identifies the root causes of the issues that appear during the information life cycle and classifies them into technological, organizational, or people factors using a Fishbone diagram, as shown in [Figure 8.6](#).

Finally, the TIRM team ranks the root causes in a table based on how important the causes are for the mitigation of the information risks ([Table 8.2](#)).

Table 8.1 Ranked List of Information Risks at Call Center

Rank	Information Risk	Impact on Operational Efficiency	Impact on Customer Satisfaction
1	Customer data is incomplete and incorrect	\$518,000 (High)	6000 dissatisfied callers (Very high)
2	Finding the solution is difficult	\$732,000 (High)	3490 dissatisfied callers (High)
3	Experts are not available	\$285,000 (Medium)	3100 dissatisfied callers (High)
4	Customer feedback information is difficult to interpret	\$150,000 (Low)	2450 dissatisfied callers (Medium)

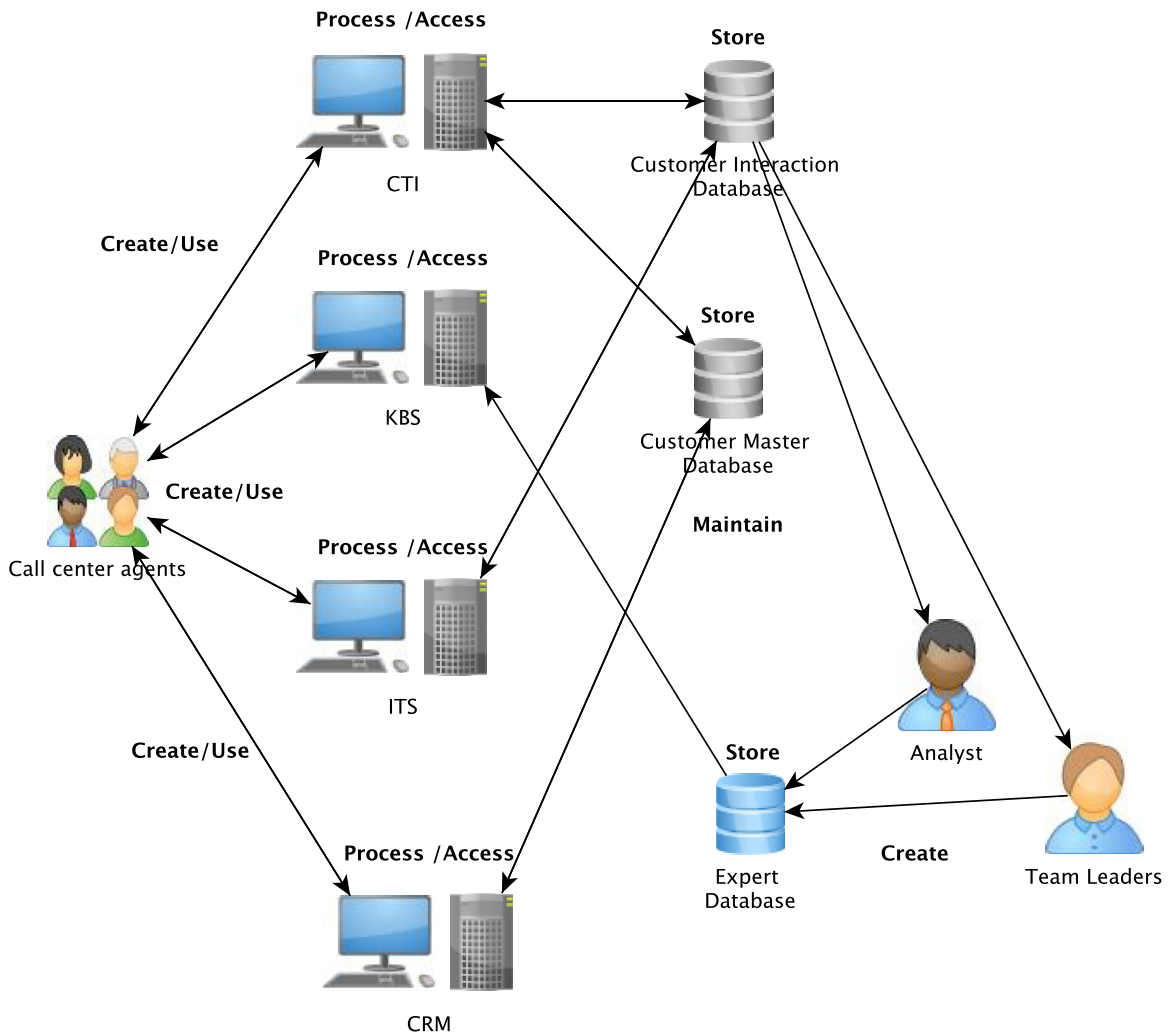
STEP C2: IDENTIFY AND DESCRIBE TREATMENT OPTIONS

After having the causes of the information quality problems identified, the next step ([Figure 8.7](#)) is to find possible actions that can be taken to mitigate the information risks. This can be done in two substeps, as shown in [Figure 8.8](#).

C2.1: Identify information risk treatment options

For each information risk selected in step B9, potential information risk treatments should be identified, with due consideration being given to the causes of the underlying information quality problem. Information risk treatments can often result in projects for information quality improvement. Projects that do not improve information quality only deal with the symptoms and not with the causes of the problems. However, treatment of symptoms should be considered if the treatment of the root causes is not feasible or too costly.

So, how can appropriate information risk treatments be identified? Examining how the causes and/or consequences of the information quality problems can be modified to decrease the information risk can do this. A straightforward way to brainstorm for information quality improvement is, therefore, to go through each cause of an information quality problem that leads to the risk, and look for options as to how the causes can be delimited. Depending on whether a cause of an information

**FIGURE 8.5**

Example of an information flow diagram.

quality problem lies in technology, organization, or human behavior, the appropriate information risk treatment will often be found to be in the same category as the cause. Moreover, as explained in step C1, causes are located at distinct points along the information life cycle, and often, suitable information risk treatments can be found at a similar point of the information life cycle. But, you should also look for solutions that are outside the box, which means that they can be in a different information life cycle or in a different category. Redesigning the business processes could, for example, potentially solve a problem that arises through people behavior, therefore a human cause would be treated with an organizational change.

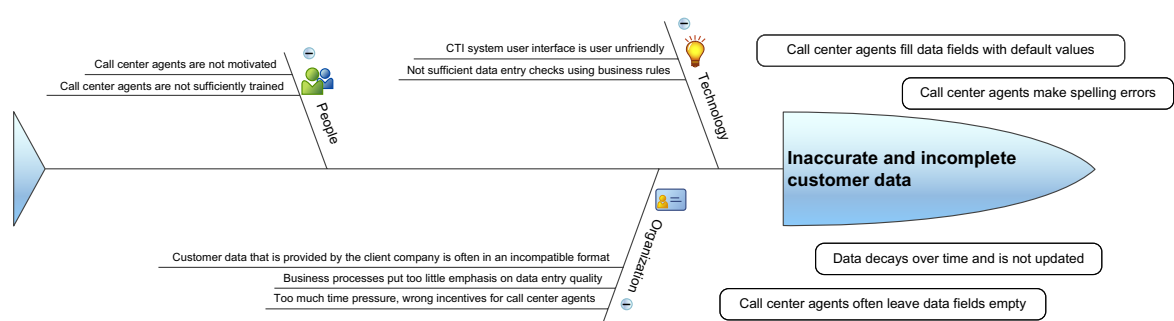


FIGURE 8.6

Illustration of a fishbone diagram used for IQ root-cause analysis at the call center.

Table 8.2 Ranked List of Root Causes for the IQ Problem That Customer Data Is Incomplete and Incorrect

Rank	Short Description	Category
1	Too much time pressure, wrong incentives for call center agents	Organization
2	Business processes put too little emphasis on data entry quality	Organization
3	CTI system user interface is user unfriendly	Technology
4	Insufficient data entry checks using business rules	Technology
5	Call center agents are not motivated	People
6	Call center agents are not sufficiently trained	People
7	Customer data that is provided by the client company is often in an incompatible format	Organization/Technology
8	Team leaders do not emphasize importance of data	Organization

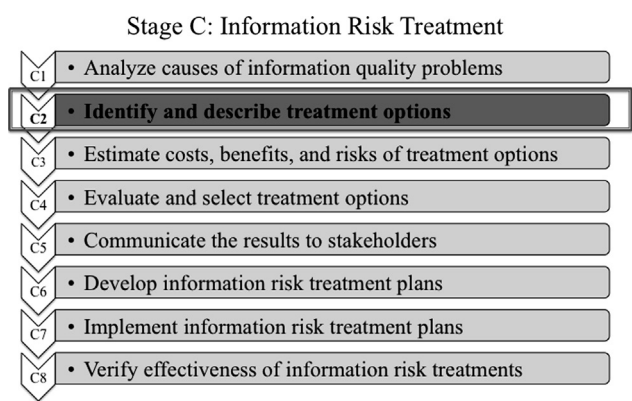


FIGURE 8.7

Step C2 in context.

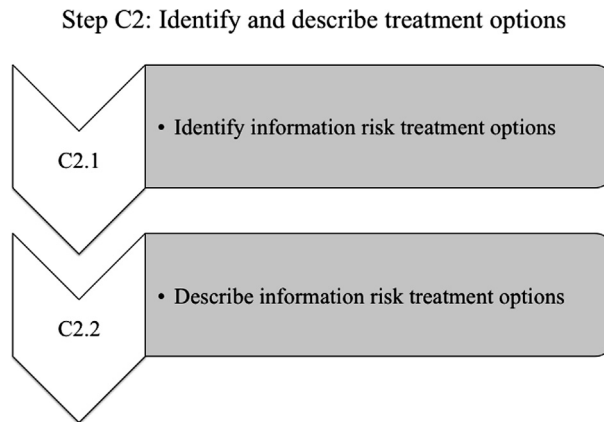


FIGURE 8.8
Activities in step C2.

Information Life Cycle	Create	Process	Access	Use	Dispose
Potential technology treatment	Modify ERP system so that data users can give feedback if collected information is sufficient and check the correctness already during the data collection stage	—	—	—	—
Potential organization treatment	Head of production and head of sales have to make it a requirement for sales staff to fill out the complete checklist with information that is as accurate as possible	—	—	When information is used, the sales department should be called to obtain additional clarifying information	—
Potential people treatment	Special training for sales staff that shows how they can interpret the customer requirements and capture the data better	—	—	—	—
Internal or external	Internal creation by sales staff	—	—	Internal usage by technical staff	—

Table 8.3 offers a template that can be used to brainstorm for appropriate information risk treatments using the information life cycle and the TOP categorization. The example shown in the table is taken from a case study with a manufacturing company.

For each information quality problem, a list of information risk treatment options is iteratively generated. If there are several information risk treatment options for one information risk treatment,

it should be examined if they can be implemented in parallel or if they are exclusive alternatives that cannot be implemented at the same time.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

For each root cause, potential information risk treatment options are identified at the call center by

the TIRM team, which are shown in [Table 8.4](#).

Table 8.4 Potential Information Risk Treatments

Root Cause	Category	Potential Information Risk Treatment
Too much time pressure, wrong incentives for call center agents	Organization	Change incentive system for call center agents and team leaders so that performance measurement also incorporates the quality of the data entered and updated
Business processes put too little emphasis on data entry quality	Organization	Formalize data entry and update requirements in business processes
CTI system user interface is user unfriendly	Technology	Optimize user friendliness of CTI system for simplified data entry
Not sufficient data entry checks using business rules	Technology	Create business rules that are checked during and after data entry and update
Call center agents are not motivated	People	Change incentive system for call center agents and team leaders so that performance measurement also incorporates the quality of the data entered and updated
Call center agents are not sufficiently trained	People	Organize data entry and update training for call center agents
Customer data that is provided by the client company is often in an incompatible format	Organization/ technology	Work with companies to improve the compatibility of the systems to handle data that has different formats
Team leaders do not emphasize importance of data	Organization	Change incentive system for call center agents and team leaders so that performance measurement also incorporates the quality of the data entered and updated

C2.2: Describe information risk treatment options

Each information risk treatment option identified in substep C2.1 should be described further:

- What is the title of the information risk treatment?
- What, exactly, needs to be done?
- How are information risks expected to be modified by the information risk treatment?
- With which other information risk treatments would this treatment be compatible or not compatible?
- Which technological, organizational, and/or human-related changes would be required?
- What would be the timescale of the change?



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM team further describes each of the identified information risk treatment options per the following example description.

Title of Information Risk Treatment: Change the Incentive System for Call Center Agents and Team Leaders. Change the incentive system for call center agents and team leaders so that performance measurement also incorporates the quality of the data entered and updated; this proposed change requires:

- Preapproval of the board of directors
- Redesign of the incentive system to include data entry and update quality as factors
- Development of appropriate measurement metrics
- Drafting of required policy, business process, and technology changes

- Final approval by the board of directors
- Implementation of the new incentive system

Two information quality problems will be mitigated by the information risk treatment, namely, the customer data is incomplete and incorrect and that finding the solution is difficult. This is because both information quality problems are directly related to the root causes that are modified by the information risk treatment:

1. Too much time pressure, inappropriate incentives for call center agents
2. Call center agents are not motivated
3. Team leaders do not emphasize the importance of data

The TIRM sponsor decides that the changes preferably should be implemented within one calendar year after the preapproval of the board of directors.

STEP C3: ESTIMATE COSTS, BENEFITS, AND RISKS OF TREATMENT OPTIONS

The ISO 31000 standard for risk management states that “selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived” (ISO, 2009, p. 19). In this step (Figure 8.9), expected costs and benefits of information risk treatments are identified (Figure 8.10). There are always things that may not proceed as expected during the implementation of an information risk treatment. These implementation risks should be considered during the evaluation of the information risk treatments.

Stage C: Information Risk Treatment

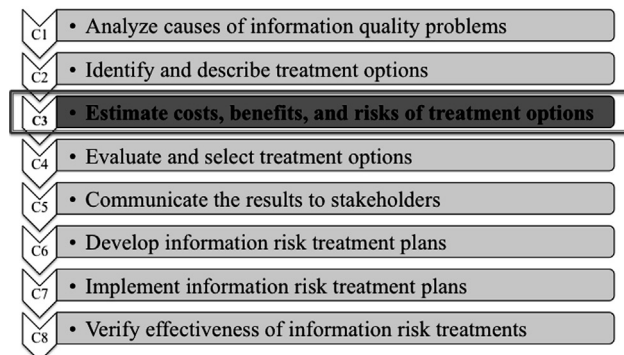


FIGURE 8.9

Step C3 in context.

C3.1: Estimate costs of information risk treatment options

First, expected costs for the options need to be estimated, which could include, for example, personnel costs, training costs, hardware costs, software costs, and external service provider costs. The costs should be split up into one-time costs and recurring costs.

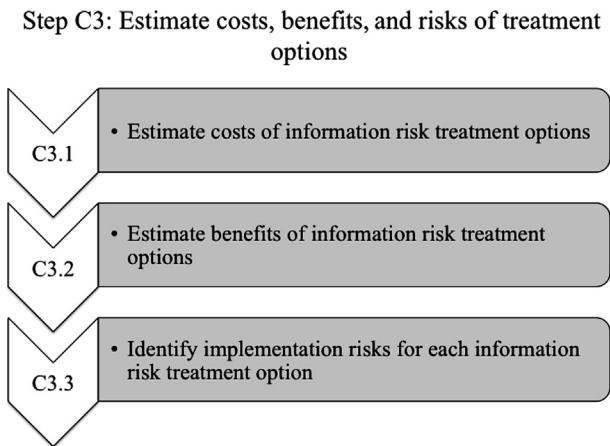


FIGURE 8.10
Activities in step C3.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The management team at the call center decides to look at a three-year time horizon when evaluating information risk treatment investments. The TIRM team determines the

costs for each information risk treatment. An example of the information risk treatment to change the incentive system for call center agents and team leaders is shown in [Table 8.5](#).

Table 8.5 Costs for Information Risk Treatment to Change the Incentive System for Call Center Agents and Team Leaders

Cost Category	Description	One-time Costs (Year 0)	Reoccurring Costs (Years 1–3)
Software	System changes to support changes in incentive system and measurement of new metrics	\$120,000	\$25,000
Hardware	No additional hardware required	0	0
External services	Data quality consultant for setting up data quality metrics (50 days, \$2000 per day)	\$100,000	0
Human resource requirements	Time of internal staff, 2.5 FTE (full-time equivalent) in a one-year project, \$60,000 yearly per FTE, afterwards 0.5 FTE yearly	\$180,000	\$30,000
Total Costs	\$565,000 over three years	\$400,000	\$55,000

C3.2: estimate benefits of information risk treatment options

Second, the benefits of each information risk treatment option are estimated. Before this calculation can be done, the workshop participants have to estimate the new expected likelihood of the occurrence of information quality problems, after the information risk treatment has been successfully implemented, for each task that is affected by the risk treatment. Then, to determine the expected benefits of a potential information risk treatment, the level of information risk is compared before and after the treatment option has been implemented.

However, the benefits of an information risk treatment might only become visible gradually, which should be explicitly considered in the modeling. For instance, in the first two years after treatment implementation, there are no benefits yet; in years two to five, only 50% of the benefits can be achieved; and from year five onward, 100% of the benefits are achieved. Moreover, to improve the reliability of the results, expected costs and benefits can be estimated in three scenarios—that is, a worst-case, average, and best-case scenario. An examination should also be undertaken of which other benefits that go beyond the scope of the process might accrue from the information risk treatment option.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM team at the call center estimated the benefits for each information risk treatment. For instance, it is estimated that the information risk treatment to change the incentive system for call center agents and team leaders can reduce the likelihood of the occurrence of the information quality

problems that customer data is incomplete and incorrect by 40% and that finding the solution is difficult by 35%. Half of the benefits, so it is expected, will start from the second year and will be fully realized in the third year. The benefits over three years are shown in [Table 8.6](#).

Table 8.6 Benefits of Information Risk Treatment to Change the Incentive System for Call Center Agents and Team Leaders					
Year	0	1	2	3	Sum
Decreased costs in US Dollars (Operational efficiency)	0	0	\$231,700	\$463,400	\$695,100
Decreased number of dissatisfied customers (Customer satisfaction)	0	0	1810	3621	5432

C3.3: Identify implementation risks for each information risk treatment option

Third, there might be implementation risks associated with the risk treatment option—for example, the costs might be higher than expected, the benefits might not be fully realized, or other aspects of the organization might be negatively affected. Potential implementation risks should be identified and documented for each information risk treatment option.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

The TIRM team at the call center organizes a brainstorming session to identify potential implementation risks for each information risk treatment. Implementation risks of the information risk treatment to change the

incentive system for call center agents and team leaders are presented in [Table 8.7](#), and are evaluated overall as high for this information risk treatment.

Table 8.7 Implementation Risks of Information Risk Treatment to Change the Incentive System for Call Center Agents and Team Leaders

Implementation Risk	Likelihood	Consequence
No final approval is given by board of directors	Very low	Investment is completely wasted
Final approval by board of directors is delayed	Medium	Slightly increased costs and benefits will take longer to be realized
Design of new incentive system takes longer	High	Increased costs and benefits will take longer to be realized
Implementation of new incentive system takes longer	Medium	Increased costs and benefits will take longer to be realized
Software changes do not work and need redesign	Low	Significantly increased costs and benefits will take longer to be realized; quality of service might be affected
Problems in user adoption	Medium	Benefits will not be fully realized
Measurement metric do not drive the right behavior	Low	Benefits will not be realized

STEP C4: EVALUATE AND SELECT TREATMENT OPTIONS

In this step (Figure 8.11), information risk treatment options are evaluated, with due consideration being given to the costs, benefits, and risks of the option. Risk treatment options are selected, taking this evaluation and the overall organizational priorities and culture into account. Moreover, a five-step scale from very low, low, medium, high, to very high can be used to evaluate the priority of the risk treatment option.

Note that sometimes when the risk is not tolerable, it can be decided to treat a risk although it is not justifiable on economic grounds as suggested by the ISO 31000 standard (ISO, 2009).

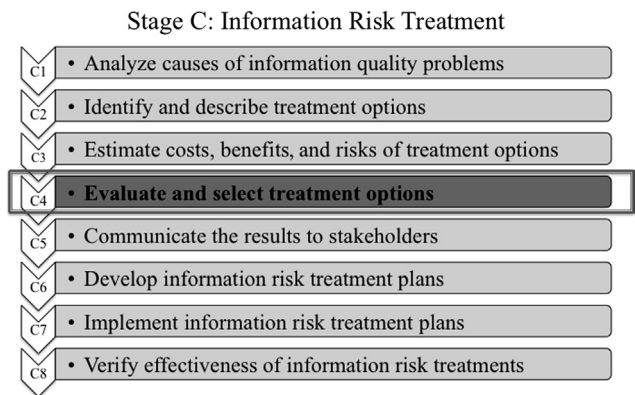


FIGURE 8.11

Step C4 in context.

The selected information risk treatment options should be ranked in a list, taking their overall evaluation and priority evaluation into account. A recommendation should be forwarded to the senior decision makers who will have the final say as to which information risk treatment options are approved for implementation.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

To prepare the evaluation for the board of directors, the TIRM process manager brings the benefits and costs for each information risk treatment into a single table and calculates the accumulated cash flow and net present value (NPV) over three years (Table 8.8). He discusses with the TIRM process sponsor which recommendations should be given to the board of directors. For those information

risk treatments that should be proposed to the board, a business case is created that describes the information risk treatments and presents the hard numbers.

The TIRM process sponsor presents the business cases to the board of directors who make the final decision as to which information risk treatments should now be implemented (Table 8.9).

Table 8.8 Investment Analysis of the Information Risk Treatment to Change the Incentive System for Call Center Agents and Team Leaders

Year	0	1	2	3	Sum
Costs	\$400,000	\$55,000	\$55,000	\$55,000	\$565,000
Benefits operational efficiency	0	0	\$231,700	\$463,400	\$695,100
Benefits customer satisfaction	0		\$1810	\$3621	\$5432
Cash flow	-\$400,000	-\$55,000	\$176,700	\$408,400	
Accumulated cash flow	-\$400,000	-\$455,000	-\$278,300	\$130,100	
NPV		\$17,647			

Table 8.9 Investment Evaluation of Potential Information Risk Treatments

Potential Information Risk Treatment	Increased Number of Satisfied Customers	NPV	Implementation Risks	Overall Evaluation	Decision of Board of Directors
Change incentive system for call center agents and team leaders so that performance measurement also incorporates the quality of the data entered and updated	5432	\$17,647	High	High	Implement with medium priority
Formalize data entry and update requirements in business processes	2040	\$52,592	Medium	High	Implement with high priority

Continued

Table 8.9 Investment Evaluation of Potential Information Risk Treatments—cont’d

Potential Information Risk Treatment	Increased Number of Satisfied Customers	NPV	Implementation Risks	Overall Evaluation	Decision of Board of Directors
Optimize user friendliness of CTI system for simplified data entry	987	–\$12,123	High	Low	Do not implement
Create business rules that are checked during and after data entry and update	2629	\$36,145	Medium	High	Implement with high priority
Organize data entry and update training for call center agents	450	\$1545	Low	Medium	Implement with low priority
Work with companies to improve the capability of the systems to handle data that has different formats	3459	\$7363	Very high	Very high	Implement with medium priority

STEP C5: COMMUNICATE THE RESULTS TO STAKEHOLDERS

The support of stakeholders is paramount to manage the successful implementation of selected information risk treatments (Figure 8.12). Communicating the results is therefore an important part of both risk management and information quality management practices. Therefore, the list of information risks and selected information risk treatments should be communicated in this step to all relevant stakeholders. This can be done in many different ways, such as in the form of a written report or in a meeting in which the results are presented. The stakeholders should be encouraged to give feedback, which should be carefully considered since in response to such feedback, it might mean that changes or modifications are required to previously made decisions.

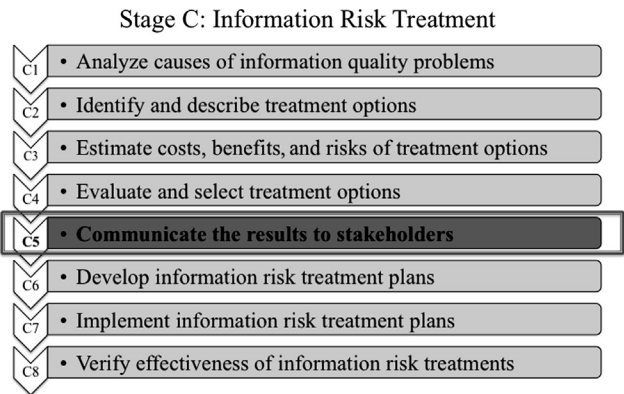


FIGURE 8.12

Step C5 in context.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

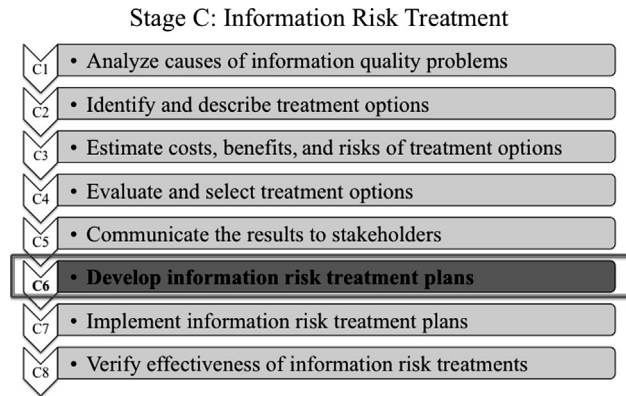
The TIRM team develops a communication plan, which is presented in [Table 8.10](#). A number of events are organized separately for each of the stakeholder groups to communicate the messages. A discussion

session that involves team leaders and members of the IT department is also organized to set the foundation for good cooperation and collaboration during the implementation of the information risk treatment.

Stakeholder Group	Why are They Important?	Which Message Should be Sent Out?
Board members	Approval absolutely essential at many stages during implementation.	Implementing the information risk treatment measures will improve customer satisfaction and decrease operational costs.
Team leaders	Their support is necessary to change the behaviors of call center agents.	Fewer information quality problems mean fewer business problems and daily incidents that the team leaders need to deal with.
Call center agents	A number of causes of information quality problems are directly related to the call center agents' behaviors.	Higher-quality data will make it easier for call center agents to better serve customers. There will be less frustration in the daily job and less effort will be needed to deliver good job performance.
IT department	The IT department needs to be encouraged to work out solutions that will work in practice. They need to be motivated to cooperate effectively with other parts of the business.	Only through close cooperation with the business side will the implementation of information risk treatments be successful. It will enable the IT department to perform the data management activities to higher standards. Improved data quality will open new opportunities for data analytics.
Client companies	There might be service disruptions when changes are executed. Informing clients about plans will help them to understand that the information risk treatments are in their interests.	Information risk treatments are implemented to improve customer satisfaction levels even further. The disruptions during implementation will be reduced to a minimum. The benefits will accrue quickly.

STEP C6: DEVELOP INFORMATION RISK TREATMENT PLANS

Once the most important stakeholders agree to the proposed treatments, the best way to implement the treatment has to be investigated. In this step ([Figure 8.13](#)), for each information risk treatment selected for implementation, an information risk treatment plan is developed. There are usually many different ways to implement an information risk treatment. The most effective way to implement the option is determined after considering the prevailing culture and the lessons learned in the organization, because this will give you a steer toward the most effective route.

**FIGURE 8.13**

Step C6 in context.

As part of the preparation of an information risk treatment plan, the following things should be documented, according to the ISO 31000 standard (ISO, 2009, p. 20):

- The reasons for selection of treatment options, including expected benefits to be gained
- Those who are accountable for approving the plan and those responsible for implementing the plan
- Proposed actions
- Resource requirements including contingencies
- Performance measures and constraints
- Reporting and monitoring requirements
- Timing and schedule

Moreover, a project team needs to be chosen and sometimes selection of software required has to be made (see Chapter 12). Advice from external consultants who have experience of the type of information risk treatment should also be considered if this level of expertise does not currently exist in the organization.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

For each information risk treatment, the TIRM team, in coordination with the board of directors, chooses a project manager and an implementation plan is developed by the

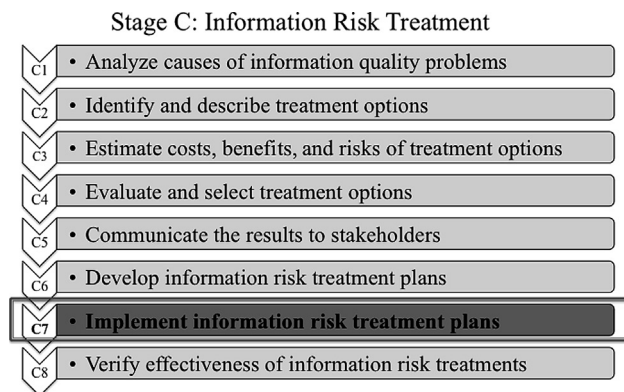
TIRM process manager. An example is given in Table 8.11 for the information risk treatment to change the incentive system for call center agents and team leaders.

Table 8.11 Implementation Plan for the Information Risk Treatment to Change the Incentive System for Call Center Agents and Team Leaders

Task ID	Description	Due By	Responsible for Implementation
1	Preapproval of the board of directors	8/20/13	TIRM process sponsor
2	Redesign of incentive system to include data entry and update quality as factor	10/11/13	Project manager
3	Establishment of appropriate measurement metrics	11/30/13	Project manager
4	Draft required policy, business process, and technology changes	2/24/14	Project manager
5	Final approval of board of directors	3/1/14	Project manager
6	Implementation of new incentive system	8/20/14	Project manager

STEP C7: IMPLEMENT INFORMATION RISK TREATMENT PLANS

In this step (Figure 8.14), each selected information risk treatment is implemented according to the approved information risk treatment plan developed in step C6. The implementation should be fully documented. General best-practice principles in project management apply during implementation. You can use any project management methodology that is accepted in your organization; select the one you consider is most appropriate for the type and scale of the implementation project. If suitable, the implementation can initially be done on a small scale, as this will enable you to check if the addressed information risks can be treated successfully. You can then expand the treatment to the full scope.

**FIGURE 8.14**

Step C7 in context.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

During the course of the year, implementation of each of the selected information risk treatments commences using the priorities set out in step C4. Each project manager documents the progress of the implementation using the template

shown in Table 8.12. If additional actions are required, when, for example, problems arise during implementation, then the project manager of an information risk treatment can escalate the issues, if required, to the TIRM process manager.

Table 8.12 Project Status Report for Information Risk Treatment to Change the Incentive System for Call Center Agents and Team Leaders

ID	Task Description	Status	Status Description	Required Actions
1	Preapproval of the board of directors	Completed	Approval has been given	None
2	Redesign of incentive system to include data entry and update quality as factor	Delayed	The redesign is more difficult than originally assumed; there is disagreement between different parties	Consider involving external performance management consultant
3	Establishment of appropriate measurement metrics	In progress	Measurement metrics are currently developed by special task team	None
4	Draft required policy, business process, and technology changes	Not started	—	—
5	Final approval of board of directors	Not started	—	—
6	Implementation of new incentive system	Not started	—	—

STEP C8: VERIFY EFFECTIVENESS OF INFORMATION RISK TREATMENTS

The effectiveness of the implemented information risk treatment is verified in this step (Figure 8.15). The costs and benefits are checked and compared with the planned expected costs and benefits. Lessons learned should be documented to improve information risk treatments in the future.

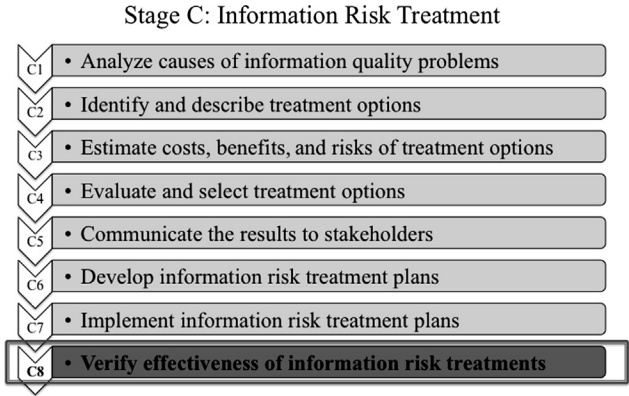


FIGURE 8.15
Step C8 in context.



EXAMPLE: TIRM PROCESS APPLIED AT A CALL CENTER

After all five information risk treatments have been fully implemented and three years have passed, it is time for the TIRM team at the call center to verify the benefits and summarize the learnings. The TIRM process manager realizes that it is difficult to measure the benefits that have accrued from each individual information risk treatment because the information risk treatments are interdependent. He, therefore, decides to look at the overall benefits of all five implemented information risk treatments. In fact, a clear increase in satisfied customers and decrease in operational costs could be measured, as shown in [Table 8.13](#). Taken as a whole, the investment has been worthwhile, although the NPV is much lower than expected, as the actual implementation costs exceeded the planned costs and some

of the benefits were not realized. The good news is that the NPV is still positive and that the increase in the number of satisfied customers has been higher than anticipated.

To learn from the implementation of these information risk treatments, the TIRM process manager organizes sessions with each of the project managers to summarize the key learnings, which are presented in [Table 8.14](#).

While some aspects did not work out as well as anticipated, the TIRM process sponsor and the board of directors are, overall, very pleased with the outcomes. Consequently, they decide to run the TIRM process on an annual basis to further optimize data and information assets at the call center. The lessons learned are considered in the next cycle of the TIRM process.

Table 8.13 Comparison of Planned versus Realized Benefits				
	Total Increased Number of Satisfied Customers Planned	Total Increased Number of Satisfied Customers Achieved	Total NPV Planned	Total NPV Achieved
Total for all five information risk treatments implemented over three years	14,010	20,000	\$115,292	\$40,647

Table 8.14 Summary of Lessons Learned During Information Risk Implementation

Information Risk Treatment	Lessons Learned
Change incentive system for call center agents and team leaders.	Redesign of incentive systems is a huge effort on its own. Measurement metrics need to be objective and fair and have to be sufficiently tested. This requires more effort than anticipated.
Formalize data entry and update requirements in business processes.	Formalization of requirements makes it clearer to employees what is required. Stronger focus should be placed on enforcement of the requirements.
Create business rules that are checked during and after data entry and update.	Business rules started only to be effective after they have been combined with incentives and formalization of requirements.
Organize data entry and update training courses for call center agents.	Training was more effective than originally expected. Call center agents are more motivated in data entry when they understand why it is important.
Work with companies to improve the capability of the systems to handle data that has different formats.	Establishing good relationships with the client companies is key to get a better understanding of the customer data that is handed over. Capability to handle different formats was vastly improved through this information risk treatment.

SUMMARY

This chapter presented stage C of the TIRM process, which is an eight-step approach to identify, evaluate, and implement suitable treatments for the information risks acknowledged in stage B. Information risk treatment first identifies and ranks the root causes of the information risks after which potential information risk treatments are identified. To evaluate and select the right information risk treatment options, the costs, benefits, and expected implementation risks have to be estimated. The benefits are, therefore, calculated using the risk figures from stage B. Communicating effectively to the most important stakeholders increases their support during implementation. Information risk treatment plans are developed then implemented, and the effectiveness of the information risk treatments are verified at the end of stage C. Finally, lessons learned are summarized to improve the next cycle of the TIRM process, which starts back at stage A. The next cycle of the TIRM process does not require the same amount of effort, as a lot of information has already been collected and needs only to be updated. Additionally, your organization is already very familiar with the way in which the TIRM process is run.

In the next chapter, we discuss strategies to better integrate the TIRM process within the organization.

REFERENCES

International Organization for Standardization (ISO). (2009). *ISO 31000:2009 Risk Management—Principles and Guidelines on Implementation*. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.

International Organization for Standardization (ISO). (2009). *ISO/IEC 31010:2009 - Risk Management—Risk Assessment Techniques*. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.

Loshin, D. (2001). *Enterprise Knowledge Management: The Data Quality Approach* San Francisco: Morgan Kaufmann.

McGilvray, D. (2008). *Executing Data Quality Projects: Ten Steps to Quality Data and Trusted Information™*. Burlington, MA: Morgan Kaufmann.

Integrating the TIRM Process within the Organization

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to integrate the TIRM process within your organization
- The roles and responsibilities that can be set up for the TIRM process
- Guiding principles to ensure successful implementation of the TIRM process

INTRODUCTION

In the last few chapters, the most important elements of TIRM were introduced in detail. In this chapter, we give recommendations on the integration of TIRM within the organization. We consider where responsibility for TIRM should lie, how those responsibilities might be assumed, and also explore the role that organizational culture has to play. TIRM is essentially a process to steer Enterprise Information Management (EIM) in a way that promises to create the best business value for information. We will, therefore, also clarify the relationship between EIM and TIRM in this chapter. Additionally, we cover how TIRM should be integrated with the enterprise risk management (ERM) function in the organization.

ROLES AND RESPONSIBILITIES FOR TIRM

Who is responsible for TIRM? The correct answer to this question is “everybody in the organization.” At a time when information is driving the economy as never before, it is important to have a well-implemented TIRM program where everyone has responsibility for ensuring that information is managed effectively. From IT to finance to human resources to marketing, from the CEO to staff working in the field, it should be incumbent upon everyone to regard TIRM as an integral element of day-to-day business. This may be achieved by, for example, encoding TIRM into business processes, performance measures, etc., and communicating it in ways that are relevant to individual employees and their role within the organization.

The view that the management of risk is a collective responsibility is supported by ISO 31000, which states: “Risk management is not a standalone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and part

**ATTENTION**

TIRM is not the specific responsibility of IT. It is the collective responsibility of the whole organization to manage information risks.

of all organizational processes, including strategic planning and all project and change management processes” (ISO, 2009).

While the board of directors has overall responsibility and accountability for the strategic direction of the organization and for delivering performance (and profitability), the responsibility for TIRM may in many instances be placed firmly at the feet of the chief risk officer (CRO) or chief compliance officer (CCO). While this is understandable, it means that there is the potential danger of everyone else in the organization thinking that they have neither responsibility nor accountability for TIRM, and that is not a good situation for an organization to be in. Therefore, representatives from all corners of the organization should be involved in the TIRM program. In particular, we suggest the specific roles and committees to manage the transition to an organization that effectively manages information risks; these are discussed in the following sections.

Specific roles

TIRM should be a collective responsibility with each manager being accountable for managing information risk within his or her sphere of responsibility. Yet, it is important in the early days of implementation to give responsibility for the implementation of activities to a few key individuals, supported by a team if appropriate, in the longer term. There are a number of roles that should be allocated to kick off a successful TIRM program:

1. TIRM process sponsor
2. TIRM process manager
3. TIRM process facilitator(s)
4. Business process representatives
5. IT system and database representatives

If similar roles already exist as part of the enterprise information governance program, it would be appropriate to align TIRM with information governance roles and responsibilities. TIRM is integral to EIM. The roles do not require a full-time position to be created, but rather should be executed in addition to current job activities by capable employees. Depending on the scale of your organization and the scope of the TIRM process, the number of people needed can increase when the size of the TIRM program is big. In very large organizations you might even consider creating full-time positions for some of the roles. Each role is discussed in the following.

**IMPORTANT**

Specific roles give structure to the TIRM program; ensure that all the key parts of the business are represented in the TIRM committees (under consideration of the scope of the TIRM process).

TIRM process sponsor

The TIRM process sponsor plays the most important role. This individual should be a senior executive who has the authority to start and maintain a TIRM program within the organization. He or she should understand the importance of managing information risks.



IMPORTANT

The TIRM process sponsor should be a senior executive with enough organizational power to convince other business divisions to implement TIRM. The job title of a potential TIRM process sponsor usually starts with C (e.g., CEO, COO, CFO, CIO). Alternatively, it might be a president, vice president, or director.

The TIRM process sponsor is the advocate for implementing TIRM within the organization and provides the necessary resources and establishes the political support. The TIRM process sponsor heads the TIRM steering council, the role of which will be described later.

TIRM process manager

Whereas the TIRM process sponsor makes resources available, the TIRM process manager manages these resources to ensure the effective implementation of the TIRM process. This individual should be familiar with all concepts of TIRM and also have experience in information governance and management, and should ideally have worked in the business side of the organization. He or she should be familiar with and knowledgeable about all key business divisions in the organization. He or she is responsible for ensuring that TIRM policies are implemented and sustained, and therefore heads up the TIRM managing committee and leads the team of TIRM process facilitators to achieve this. Moreover, the TIRM process manager communicates with business process and IT system and database representatives to coordinate their efforts. The TIRM process manager has to report to the TIRM steering council.

TIRM process facilitators

The TIRM process facilitators are dedicated personnel trained in TIRM concepts and methods and support the implementation of the TIRM program with their expertise. These individuals prepare, facilitate, and analyze the results of workshops and process the insights gleaned from workshops into a format that is easy to understand by decision makers. They work directly with the TIRM workgroups as well as with business process and IT system and database representatives.

Business process representatives

Each important business process in the scope of the TIRM program should have at least one business



ACTION TIP

TIRM process facilitators should bring expertise in data management and be familiar with the business, how it operates, and what targets and goals the organization as a whole is striving to achieve. The TIRM process facilitators are strongly advised to read this book from cover to cover, as it will help them develop a good understanding and expertise of the necessary background, the TIRM process and the available techniques.

process representative. If a business process involves several business functions, a representative from each relevant function should be chosen. One of the business process representatives should be selected as the spokesman and coordinator, and represent the business process through membership of the TIRM managing committee.

IT system and database representatives

An IT system and database representative should be chosen for each major IT system and database. This should be someone who is knowledgeable about the data within the system and is able to use data quality software tools, such as data profiling (see Chapter 12). Information technology can both cause and prevent information risks and therefore plays an important role in TIRM. An IT system and database representative should be knowledgeable about the IT system or database he or she represents and assist in analyzing where IT hardware and software applications can create failure, security problems, and information risks. The representative also provides support when the analysis of the causes of information risks is undertaken. Additionally, he or she provides support when the identification and implementation of information risk treatment options that involve information technology are being considered. An IT system and database representatives can be, for example, a data steward or information quality manager, but could also be somebody from the IT function who is responsible for data rather than application management.

Responsible committees

In general, there can be three levels of responsibilities that are carried out by three different committees:

1. TIRM steering council
2. TIRM managing committee
3. TIRM workgroups

The optimal number and structure of responsible committees will obviously differ from organization to organization. Some larger organizations might need more levels of responsibility, whereas for smaller organizations, it might suffice to have just one committee. Also, if you implement the TIRM process in a relatively small scope, fewer structures and resources will naturally be required. Each of the three proposed levels is described in more detail in the following subsections.

Program leadership: TIRM steering council

A steering council should be formed of senior executives from preferably each business division that operates at a very strategic level. The head of this council should be the TIRM process sponsor. The steering council decides the goals and scope of information risk management and sets the policies. It also decides which information risk treatment options should be implemented based on the recommendations of the TIRM managing committee. It gives authority to the TIRM program. The TIRM manager should report regularly to the steering council and should therefore be a permanent nonvoting member of this council.

Program management: TIRM managing committee

A TIRM managing committee should be established that operates at a tactical level. The TIRM process manager should head up the managing committee. The committee consists of the TIRM process

facilitators and of selected business process and IT and database representatives. The committee manages and coordinates the TIRM activities within the workgroups. It also decides what needs to be reported to the TIRM steering council and prepares decisions that need to be made by them. The committee monitors whether or not the information risk management policies are being complied with and verifies the effectiveness of the implementation of the (chosen) information risk treatments.

Program implementation: TIRM workgroups

A TIRM workgroup operationally leads the implementation of a specific part of the TIRM program. For example, a workgroup can be responsible for overseeing and coordinating information risk assessments. Other workgroups can focus on the implementation of more complex types of information risk treatments. Therefore, there will be a number of workgroups operating simultaneously. A workgroup should consist of business process and IT system and database representatives and a TIRM facilitator—each one selected on the basis of their suitability and expertise in the type of task that the workgroup is responsible for. Each workgroup reports to the TIRM managing committee.

Advice for small- and medium-size organizations

If you are working for a small- or medium-size organization, you are rightly thinking that it is going to be too costly to implement the TIRM process in your organization. The good news is that due to the smaller size of your organization, it will take less effort to implement a successful TIRM program. Therefore, fewer roles and committees need to be created to implement the TIRM process.

Advice for large organizations

Very large organizations need much more structure to ensure that the TIRM program is delivered with success. We recommend following the advice in this section. If the TIRM process is initially implemented in a smaller scope, fewer resources are required and it can be sufficient to proceed with a much-reduced number of roles and committees. Deciding to merge the roles, responsibilities, and committees with other related councils and roles (e.g., for enterprise information management, data governance, and ERM) to reduce the overhead costs would be a prudent move. The relationship to these functions is discussed next.



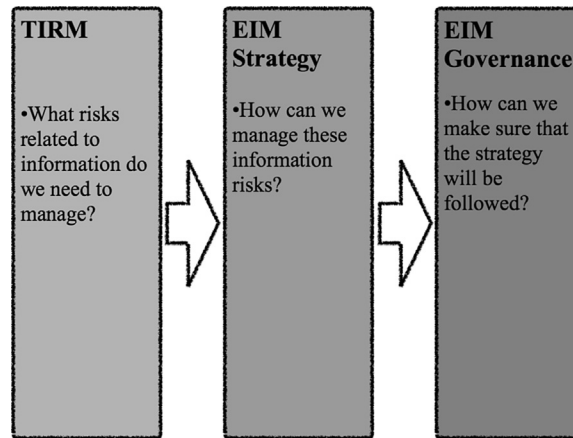
ACTION TIP

In smaller organizations, the roles can be reduced to a minimum. For example, in an organization that has 20 to 30 employees, one person could take on the roles and responsibilities of the TIRM process sponsor, process manager, and expert. Also, instead of having three levels of committees, one TIRM managing committee would suffice.

THE RELATIONSHIP BETWEEN TIRM AND EIM

Relationship of TIRM to EIM strategy and governance

The role of TIRM is to focus the EIM efforts on the things that matter most for the business. EIM is steered by the information strategy and governance. The strategy is the set of goals and objectives for EIM that should be followed; these should be aligned with the business strategy and goals. Information governance sets and monitors the rules, standards, and policies for EIM to ensure that the

**FIGURE 9.1**

TIRM influences EIM strategy and governance.

information strategy is actually followed. If your organization has not started an information governance program, we highly recommend John [Ladley's book \(2012\)](#), which discusses all of the important fundamentals of information governance. Information governance requires the definition of roles and responsibilities, principles, policies, functions, metrics, technology, and tools. Note that the roles and committees in information governance can overlap with the ones in TIRM, which is not a problem, but is encouraged since it reduces communication problems. The relationship between the TIRM program and information strategy and information governance is shown in [Figure 9.1](#).

The TIRM process allows organizations to understand where poor information hurts the business most and where better information could open up the biggest business opportunities—that is, which risks related to information need to be managed. The information strategy formulates the approach to manage these risks and information governance and then ensures the execution of the information strategy. Information governance is essential to make sure that the information strategy is delivered and enables the successful implementation of projects to treat information risk. The TIRM process then allows for regular monitoring of any changes in information strategy and governance, and whether these have led to the expected results by reducing the negative risks and increasing opportunities for the effective management of risks.

Sometimes, there is a perception that information governance could be a straitjacket that prevents the organization from pursuing its broader goals; however, nothing could be further from the truth. While it is apparent that many organizations have started to take the management of information risk seriously only as a consequence of having to comply with legislative and regulatory frameworks, there is an increasing recognition that wider information risk management can become a core competence, which if developed effectively, enhances processes and procedures.

Information policy and implementation strategy

Information policy is an overarching statement setting out *why* information management is mission-critical to the organization and how it sits within a wider organizational expression of (organizational) objectives. Implementation strategy articulates *how* the policy is going to be operationalized.

Organizations adept at managing information risk recognize the importance of formulating and implementing robust policies and strategies for its management. Without this, employees might improvise and manage information risk in disparate ways that could lead to inefficiency, duplication, poor decision making, security breaches, compliance failure, and ultimately in the severest cases put the organization out of business (Webb, 2008).

TIRM should be a component of the information policy and its implementation strategy, as well as risk assessment procedures. Any strategic plan should be a tangible expression of measurable outcomes—remember the adage “what gets measured, gets managed.” While information policy and implementation strategy can be formulated without TIRM, they may be better if information risk is considered.

Relationship between information governance and corporate governance

As discussed, TIRM informs information governance. Moreover, the TIRM program will fall within the auspice of the wider information governance program, and information governance will fall within the broader corporate governance program. Corporate governance is very firmly in the spotlight since the impact of economic liberalization and deregulation of business (through globalization) has brought a demand for transparency and compliance with regulatory and legal frameworks. Organizations are constantly being pressured to be more transparent and accountable to their stakeholders. Pressure from government, consumer groups, and nongovernmental organizations, as well as shareholder activism, is “forcing” organizations to be more open about their operations.

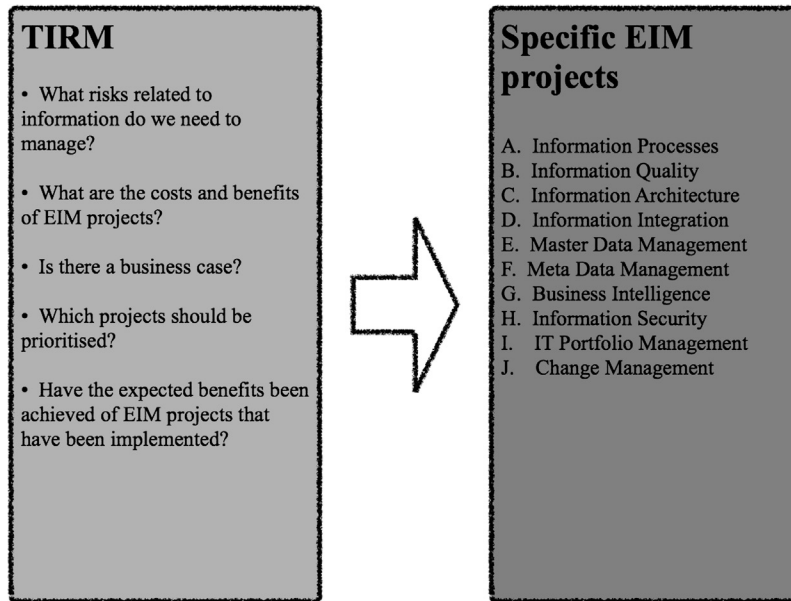
Investors, particularly institutional investors (e.g., pension funds, insurance companies), are increasingly willing to pay a premium to invest in organizations that have good governance procedures in place. These institutional investors are, of course, interested in seeing continuing profitability, but these days are also concerned about how profits are made, how internal governance is carried out, and the organization’s relationship with other stakeholder groups. Good governance leads to better management of risk; better management of risk leads to good performance and higher returns for investors. Many companies now provide commentary in their annual reports about their governance procedures.

Governance codes have been developed in different countries and are issued by a variety of entities, such as stock exchanges, trade bodies, professional associations, institutional investors, governments, and international organizations (e.g., International Monetary Fund). Generally speaking, law does not mandate compliance with such codes and principles, but there may be some legal requirements for some organizations. Each organization should be fully cognizant of what their regulatory and legal obligations are and ensure that they are compliant with them.

According to Crowther and Seifi (2010) there are four principles of corporate governance:

1. *Transparency*—it needs to be apparent to all what the governance procedures are.
2. *Accountability*—reporting structures must be clear.
3. *Responsibility*—someone must be accountable for all parts of the effect and a clear chain of actions is required.
4. *Fairness*—systems must operate impartially and without prejudice.

Corporate governance currently focuses on how an organization conducts itself in relation to all its stakeholders.

**FIGURE 9.2**

TIRM process related to specific EIM projects.

Specific EIM projects

TIRM can also support specific EIM projects. It can help make decisions about which EIM projects should be implemented based on their impact on information risk. EIM can calculate the benefits of the projects and compare them to the costs and risks. TIRM can help to select and guide which projects should be implemented and also help prioritize the projects by providing a reasoned grounding in the business impact of poor information that could be improved by the EIM project. The relationship between TIRM and specific EIM projects is visualized in [Figure 9.2](#).

Understanding which risks are created by poor information and quantifying those risks by, for example, expressing them as an annual financial impact, can be used to build business cases for the specific EIM projects and improve the effectiveness of EIM as a whole.



EXAMPLE

A company considers buying a master data management (MDM) software tool and alongside that the purchase of consulting services to successfully implement the changes in the business processes that are deemed necessary. Such a project can be very costly. By analyzing which information

risks are treated if the project is implemented, the benefits of the project can be calculated with the help of TIRM. TIRM can also help the organization to make better-informed decisions about which EIM projects actually make sense, both from a financial perspective and a nonfinancial perspective.

TIRM INTEGRATED WITH ERM

ERM is the enterprise-wide framework for dealing with uncertainty in the organization. Hopkin (2010) defines five principles for ERM:

1. Risk management activities must be proportionate to the risk level faced by an organization.
2. Risk management activities need to be aligned with the other activities in the organization.
3. Risk management must be comprehensive.
4. Risk management activities must be embedded within the organization.
5. Risk management activities must be dynamic and responsive to emerging and changing risks.

According to Hopkin, ERM requires a set of risk management–specific policies, strategy, and architecture, and protocols and guidelines. Moreover, organizational culture is an important element for risk management. The organization’s risk appetite needs to be defined and ERM should be integrated with corporate governance activities. Risk management activities should be documented, and responsibilities for risk management need to be assigned. The CRO, if existent in the organization, plays a key role for TIRM and is a potential candidate for the TIRM process sponsor role besides the CIO. The CRO should at least be a member of the TIRM steering council.

What is the relationship between TIRM and ERM?

Protecting the value of core business assets and ensuring that harmful risks are minimized applies to information just as much as it does to the protection of other types of organizational assets. TIRM manages the risks that arise from information and reports them to the ERM function. By improving the information quality in the organization, the overall effectiveness of ERM can also be improved. ERM often concentrates on the extreme uncertainties in an enterprise such as stock market crashes, economic recessions, shifts in technology and markets, earthquakes, and fires. Many information risks would therefore not be significant enough to be managed under the ERM umbrella, but are often still very important for the competitiveness and success of an organization. Therefore, they should be reported to the ERM function, but often they need to be handled separately and in a different level of granularity. To summarize, TIRM is on the crossroad of ERM and EIM, with both functions playing an important role, but, as emphasized at the beginning of this chapter, the responsibility for managing information risks should lie in everyone’s hands across all business functions.

SUMMARY

This chapter discussed how, at a high level, an organization can implement the TIRM program. In particular, roles and committees have been proposed that can be adapted to give structure to the TIRM program. We have also shown how TIRM interrelates with EIM and ERM in an organization.

REFERENCES

- Crowther, D., & Seifi, S. (2010). Corporate Governance and Risk Management. Available at, www.bookboon.com.
- Hopkin, P. (2010). *Fundamentals of Risk Management: Understanding Evaluating and Implementing Effective Risk Management*. London: Kogan Page, p. 47.

- International Organization for Standardization (ISO). (2009). ISO 31000:2009 Risk Management—Principles and Guidelines on Implementation. Available at, http://www.iso.org/iso/catalogue_detail?csnumber=43170.
- Ladley, J. (2012). *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program* (1st ed.). San Francisco: Morgan Kaufmann.
- Webb, J. (2008). *Strategic Information Management: A Practitioner's Guide*. Oxford: Chandos Publishing Ltd.

TIRM Process Application Example

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Learn from a fictitious case study of LightBulbEnergy Inc.
- An electricity utility company uses the TIRM process to assess information risks and evaluate an information technology investment

INTRODUCTION

In this chapter, we present a full case study of how the TIRM process can be applied in the energy industry. It is a story about LightBulbEnergy Inc., an energy utility company that applies the TIRM process to understand the risks that arise from poor information quality and evaluate an IT investment that aims to mitigate the information risks. Note that this case study and the company are fictitious. Nevertheless, the case study represents a realistic example that draws on our experiences of applying the TIRM process in a number of different companies.

STAGE A: ESTABLISH THE CONTEXT

Step A1: Set the motivation, goals, scope, responsibilities, and context of the TIRM process

A.1.1: Formulating the motivation for the TIRM process

LightBulbEnergy Inc. manages a vast amount of distributed physical assets as part of the electricity network. It requires huge investments on a regular basis to ensure that the electricity network runs smoothly. For optimal asset management, high-quality asset information is absolutely essential. A large proportion of the asset information is not reliable and suffers from many different data defects. For several years, LightBulbEnergy Inc. has observed the advances in information technologies in the areas of mobile geographic information systems (GISs), which can potentially improve the quality of asset information. While these new technologies promise many benefits, the implementation of them is a substantial commitment, financially and organizationally. Although being a national leader in the energy market, LightBulbEnergy Inc. is hesitant in adopting new technologies too quickly. A few years ago, the company decided to wait until the technologies had sufficiently advanced, being anxious to avoid investing prematurely. Today, the head of engineering believes that the time to invest in some modernizing technologies has come. In his opinion, the technologies together with the

worldwide product identification standards have sufficiently matured to make an investment worthwhile. He feels that missing out on the chance of investing now would be a strategic error. The CFO of the company, however, remains very skeptical. He would only be convinced if he can see sufficient evidence that the benefits will exceed the costs and implementation risks of the investment. Listening to the debate between the CFO and the head of engineering, the CIO suggests applying the TIRM process to establish the impact of the (potentially) improved asset information quality of the planned investment. She believes that the executive board can make a better-informed management decision by understanding what the impact of not having availability to the new technology-driven information could be. The head of engineering and the CFO are both happy to proceed with the idea suggested by the CIO.

A.1.2: Defining the goals of the TIRM Process

The CIO also convinces the other members of the executive board who agree to implement the TIRM process to evaluate the planned investment in more detail. Moreover, the CIO is curious as to whether there might be any other information treatments that could help the company cope with existing information risks. The goals of the TIRM process are summarized by trying to address two particular questions:

1. Should the company invest in a mobile GIS?
2. What other information risk treatments could be of high value to the organization?

A.1.3: Defining the scope of the TIRM process

It is decided that the scope of the TIRM process should be limited to the power distribution part of the organization. From the very beginning, it was clear that the TIRM process should focus on risks that arise from poor asset information. As there are only a limited amount of resources available for implementing the TIRM process, it is decided that the process should focus only on business processes that are expected to be most substantially affected by the planned changes in GIS technology. It is recommended that TIRM process facilitators should determine the most affected business processes by interviewing managers from different divisions in the organization. Moreover, they should find out which information resources and information quality dimensions could potentially be affected by the change in technologies. These activities are planned as part of investigating the information environment.

A.1.4: Defining the responsibilities for the TIRM process

The head of engineering offers to become the sponsor of the TIRM program, as he is the executive who is most keen to see the investment being realized. He suggests that the CIO and CFO join him in the TIRM steering council, and it is agreed that the head of engineering takes on the leadership of this council. Both the CFO and the CIO are happy to participate, but have different reasons for doing so: the CFO because he would like to ensure, with his presence, that the analysis is done objectively, and the CIO, because she thinks that the results from the TIRM program will provide a great opportunity for the IT department to engage with the rest of the business and to generate tangible business results for the entire enterprise. Moreover, she hopes that applying the TIRM process will generate valuable insights about the business for IT and might help to push the new GIS initiative through, which would be a major project for the IT function.

Two weeks later the steering council convenes for a kickoff meeting to define the details of the TIRM program. Beforehand, the CIO was asked by the head of engineering to identify the most suitable manager from her IT department to lead the TIRM initiative operationally. The CIO therefore brings Bill Mighty to the meeting, who is an experienced IT project manager. He proposes that Bill becomes the TIRM process manager. After a quick introductory conversation, the three steering council members agree that Bill, who has experience in data governance, manufacturing IT, and risk management, is the appropriate person for the position of the TIRM process manager. They also agree that there should be three TIRM process facilitators to assist Bill in implementing the TIRM process, and that one should be chosen by each member of the TIRM steering council. It is decided that the TIRM managing committee that is responsible for the implementation of the process should consist of the three TIRM process facilitators and be led by the TIRM process manager. Moreover, two employees from the IT department are chosen to act as the IT system and database representatives.

A.1.5: Defining the context of the TIRM process

The third issue that is discussed in the kickoff meeting of the steering council is how the TIRM process should be integrated within the organization. As the primary reason for implementing the TIRM process is to evaluate an IT investment, the CFO suggests that the TIRM process should be run under the organizational umbrella of an investment evaluation project. The steering council members suggest that the most important information risks should be reported to the enterprise risk officer. In the event that the TIRM process would be further used, independent of any particular investment project, after project completion, it would be evaluated to extend the TIRM process to an independent enterprise-wide program.

Step A2: Establish the external environment

LightBulbEnergy Inc. competes in an energy utility market that is fully privatized. The regulation in the market determines the prices that are allowed to be charged to the consumers and the quality of service that has to be delivered. It also sets high requirements regarding environmental protection and health and safety. Usually, one energy company dominates a particular regional market and is a less dominant player in other regions. Expansion often occurs through mergers and acquisitions.

Step A3: Analyze the organization

A.3.1: identify the business model

The business model of the company is fairly simple: producing electricity and distributing it to end consumers and business consumers.

A.3.2: Identify business processes

The project manager invites the business process modeling group leader to the first TIRM managing committee meeting to help identify which business processes could benefit most from the mobile GIS technologies. Together, they identify the following three most affected business processes:

1. Incident management
2. New connections
3. Capital asset replacement/refurbishment

A.3.3: Identify the organizational structure

There are three main business units: energy production, energy distribution, and general IT and management services.

A.3.4: Identify the organizational culture

LightBulbEnergy Inc. is proud of its engineering tradition, having been able to provide its clients with reliable energy for over six decades. It places an emphasis on cutting-edge energy generation technologies and owns numerous patents created by its employees. The different departments have very different cultures and therefore they often build silos and do not exchange enough information. There is often mistrust by the engineering staff at different local sites of the managers who are based in the headquarters several hundred miles away from other offices; they often impose changes that are not reasonable from the perspective of the technical personnel. The culture at LightBulbEnergy Inc. is very much engineering oriented, but information management is not a popular topic in the company, as it is often associated with staff being made redundant through automation. The approach to information management is therefore quite ad-hoc. Moreover, some staff are suspicious of new information technologies, fearing that they might not be able to cope with the new technologies or that their job roles will be replaced by technology.

Step A4: Identify business objectives, measurement units, and risk criteria

By analyzing the corporate mission and interviewing senior leadership, the TIRM process facilitators identify three core business objectives that the organization aims to achieve and propose them to the TIRM steering council. Together with the TIRM steering council, the following business objectives, measurement units, and risk criteria were chosen:

1. Operate the Business in a Cost-effective Manner

Short name: Cost effectiveness
Measurement unit: Lost USD yearly
Risk criteria:

Very high	Above \$5 million
High	Above \$1 million and up to \$5 million
Medium	Above \$0.5 million and up to \$1 million
Low	Above \$0.1 million and up to \$0.5 million
Very low	Below or equal to \$0.1 million

2. Provide Reliable Services to the Customer

Short name: Service reliability
Measurement unit: Number of hours of service disruptions per client and per year
Risk criteria:

Very high	Above 2 million hours
High	Above 500,000 and up to 2 million hours
Medium	Above 100,000 and up to 500,000 hours
Low	Above 10,000 and up to 100,000 hours
Very low	Below or equal to 10,000 hours

3. Always Operate Safely and Take Care of the Environment

Short name: Safety and environment

Measurement unit: Custom scale measuring the damage in points:

>10,000 points: Very high impact. A number of employees get seriously injured or die in work accidents. There is a major fire or another type of major public accident in which members of the public get seriously injured or killed, or a large number of properties get damaged. A hospital or another critical building has no electricity supply. A major pollution or damage to the natural environment.

1000–9999 points: High impact. One or more employees get seriously injured or die in a work-related accident. There is a fire or another type of major public accident in which members of the public get injured, or a number of properties get damaged. Major inconvenience for the public (e.g., causing a large traffic jam). A significant pollution or damage to the natural environment.

100–999 points: Medium impact. One or more employees get injured or nearly injured in a work-related accident. A public accident is caused in which members of the public could have gotten potentially injured, or a number of properties could have gotten potentially damaged. Medium inconvenience for the public. A medium pollution or damage to the natural environment or a medium noncompliance to natural protection laws.

1–99 points: Low impact. Smaller noncompliance with health and safety. Minor inconvenience for the public. Minor noncompliance to natural protection laws.

0–0.9 points: Very low impact, nonsignificant.

Risk criteria:

Very high	Above 10,000 points
High	Between 3000 and 9999 points
Medium	Between 1000 and 2999 points
Low	Between 100 and 999 points
Very low	Below 99 points

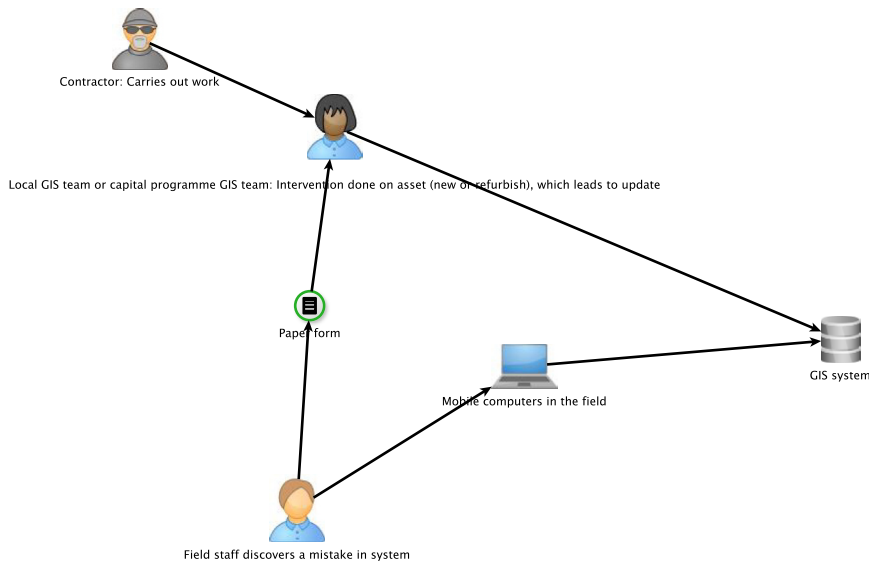
Step A5: Understand information environment

As part of this step, the TIRM process facilitators analyze a map of the IT systems landscape at LightBulbEnergy Inc. and identify for each business process whether or not an IT system is used. Moreover, they preliminarily identify information quality problems from the perspective of the IT department. To understand the information environment, the TIRM process facilitators organize meetings with the two IT system and database representatives of LightBulbEnergy Inc. The results from this investigation are summarized in the following subsections.

A.5.1: Understand relevant IT systems and databases

Four key IT systems in the scope of the process application were identified and analyzed with the IT system and database representatives:

- Geographical information system (GIS)
- Maintenance planning (MP) system
- Customer relationship management (CRM) system
- Enterprise resource planning (ERP) system

**FIGURE 10.1**

Information flow diagram example.

Each IT system runs on a separate database. The TIRM process facilitators collect information flow diagrams that were created by the IT department. An example is shown in [Figure 10.1](#).

Existing models of the enterprise architecture do exist, but they show the interrelationship between IT systems and business processes only at a very high level. The TIRM management committee thinks that an improved modeling of the enterprise architecture, although reasonable in the future, would exceed the planned budget for the TIRM process. The high-level model is used as an orientation point without going into further detail.

A.5.2: Understand relevant information management processes

Currently, a large proportion of infrastructure asset data in the company is captured and updated manually. As part of step A5, the company has organized an information quality management maturity assessment by interviewing IT and data managers and information users, using a questionnaire that evaluates the level of maturity in 13 process areas, as shown in [Figure 10.2](#). The results indicate that the company fulfills the criteria for maturity level 2, but only partially fulfills for maturity level 3 or higher. LightBulbEnergy Inc. has well-defined basic management processes (e.g., for information needs analysis, information storage management, and access control management), but when it comes to managing information quality itself, it does not have formalized business processes.

A.5.3: Investigate potential information management and information quality issues

A preliminary list of information quality issues has been created by the TIRM process manager by interviewing IT and database representatives and based on existing data profiling results ([Table 10.1](#)).

Level	Process Area (13)	Results
5	Information Quality Firewall	0%
5	Information Quality Management Performance Monitoring	0%
4	Continuous Information Quality Improvement	0%
4	Enterprise Information Architecture Management	0%
4	IQM Governance	25%
3	Information Quality Management Roles and Responsibilities	25%
3	Information Quality Assessment	0%
3	Information Quality Needs Analysis	67%
3	Information Product Management	80%
2	Information Security Management	67%
2	Access Control Management	67%
2	Information Storage Management	75%
2	Information Needs Analysis	100%

FIGURE 10.2

Information quality management maturity.

Table 10.1 Preliminary List of Information Management Issues	
Issue No.	Known Information Quality Issue
1	Asset missing in GIS
2	Asset location inaccurate
3	Asset location inconsistent
4	Asset location difficult to interpret
5	Wrong classification of asset type on GIS
6	Asset size is incorrect or missing
7	Asset age is incorrect or missing
8	Missing information on past rehabilitation
9	Condition assessment is out of date or missing
10	Performance is not using the right factors or is out of date or missing
11	Inaccurate or missing material information

STAGE B: INFORMATION RISK ASSESSMENT

After having established the context, the TIRM steering council decides to move on to the information risk assessment stage. The TIRM process manager organizes a one-day workshop for each business process with the TIRM process facilitators and the previously chosen business process representatives for steps B1 to B8. The results of each workshop are described in the following commentary, for each of the business processes separately. The output of the workshops is then used for information risk evaluation in step B9, which is done during only one workshop for all business processes.

Business process 1: Incident management

Step B1: Analyze tasks in each business process

The incident management process reacts to power outages, health and safety issues, and other failures in the electricity network that require immediate attention (Figure 10.3). Approximately 1000 times

per month on average, a customer reports an incident to the customer service center of LightBulbEnergy Inc. For each of the incident reports, a decision has to be made if further resources should be allocated to investigate and resolve it. In most cases, it is not a real incident or it is connected to an issue that is already known; the reported incident may not appear to have been recorded or many customers telephoning to report supply problems will be affected by incidents that have already been recorded. However, roughly 300 times per month on average, a reported incident requires further investigation or action.

Step B2: Examine information needed for each task

In this step, only information related to the GIS is considered, as decided in the scoping of the TIRM process in step A1. Half of the incidents that are reported to the customer service center are not actually related to the electricity network; an example would be a short circuit fault in a household. In such an instance, the customer is told that the responsibility does not lie with the company. However, each time the incident is related to the electricity network (approximately 50% of the reported incidents), further information is needed that is used to assess the situation and allocate resources, as shown in Figure 10.4. One piece of information is about current maintenance and repair activities that take place in the electricity network that prevents field staff being sent out twice. Often, LightBulbEnergy Inc. is already aware of the problems that are reported and help has already been scheduled. Moreover, information about known problems in the network is required to be able to inform the customer that the problem has already been taken care of and, usually, no further resources have to be allocated.

Once an incident has been assigned to the field engineers or a special task force, three pieces of information are always an essential input to resolve the issue, as illustrated in Figure 10.5. Information about ongoing repairs and maintenance activities in the network problems are important since

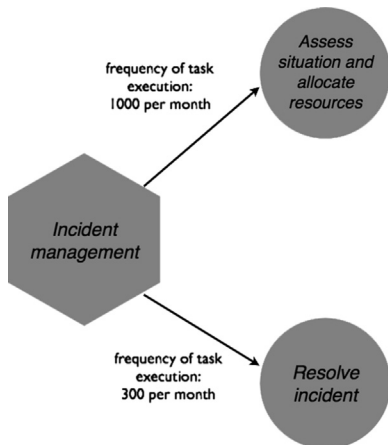


FIGURE 10.3

Incident management process.

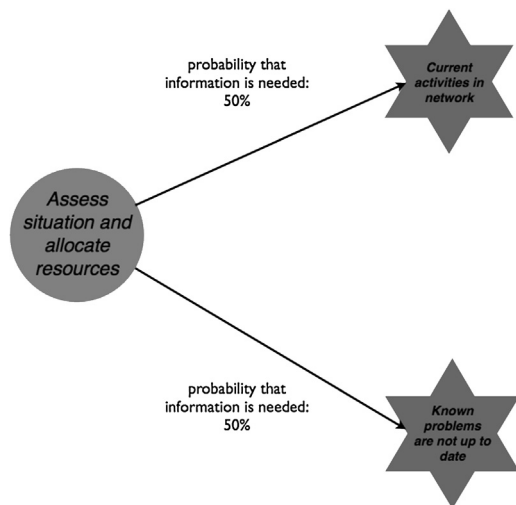
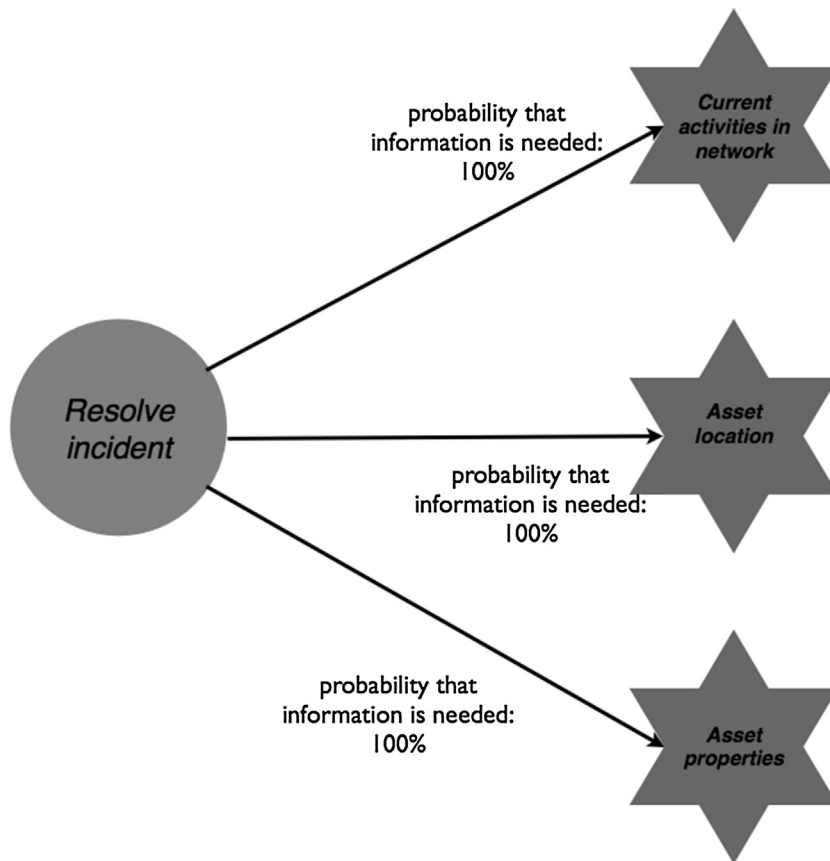


FIGURE 10.4

Information needs for incident management, part 1.

**FIGURE 10.5**

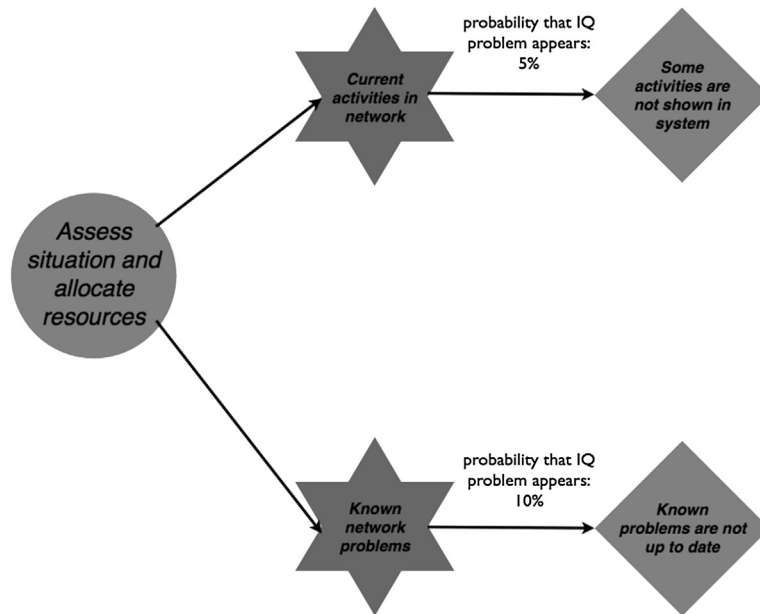
Information needs for incident management, part 2.

sometimes a repair has to wait until another activity is finished. Information about the asset location is needed as the faulty asset needs to be found to be fixed. Also, information about asset properties is key to make the right decision about asset replacement and repairs, and to take the necessary safety precautions.

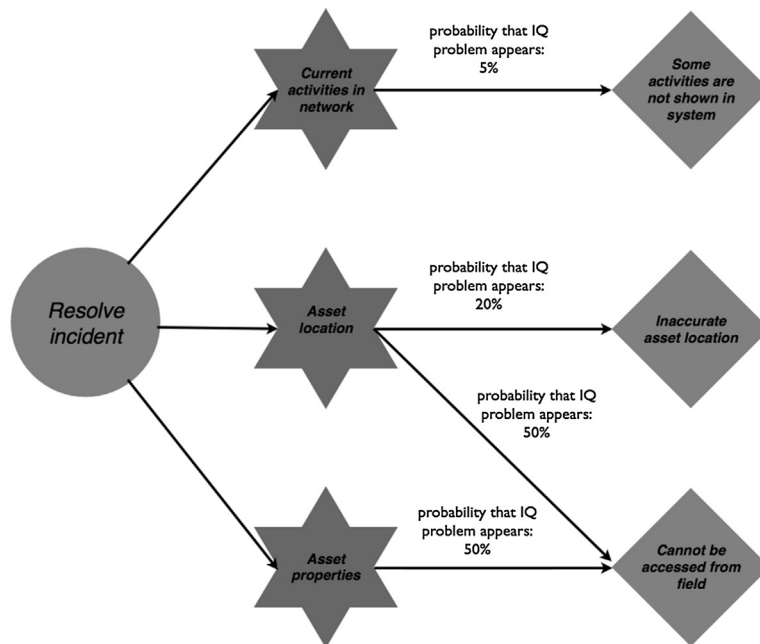
Step B3: Identify information quality problems during task execution

The business process representatives for incident management identify a number of information quality problems that appear in the business process, as shown in [Figure 10.6](#). Information about ongoing maintenance and repair activities in the electricity network are not always shared by the field engineers and, therefore, in 5% of cases is incomplete when used for one of the two tasks in the process. Also, one in ten problems that engineers are aware of are not kept up to date in the IT systems.

For resolving the incident ([Figure 10.7](#)), the same information quality problem occurs when it comes to current activities in the electricity network—that is, 5% of the activities are not displayed in the IT

**FIGURE 10.6**

Information quality problems in the incident management process, part 1.

**FIGURE 10.7**

Information quality problems in the incident management process, part 2.

system. Also, information about the asset location is often incorrect; in fact, this includes approximately 20% of the data. Moreover, in half of the cases, when the engineer needs the information about asset location and information about asset properties, it cannot be accessed, because the engineer is out in the field and does not have connection to the IT system.

Step B4: Identify consequences of information quality problems

Both information quality problems in the assess situation and allocate resources task can lead to the same direct consequence—that a poor decision is made to send out field resources, as shown in Figure 10.8. Because of the poor information on current activities in the network, the customer service center is not aware that there are already ongoing maintenance activities taking place or the problem is already known. The intermediate consequence is that several engineers might be working on the same issue and be unaware of each other, which can lead to time and materials that are wasted and even to potential health and safety issues.

When the customer service center is unaware that a reported problem is already known and that there might be plans in place to tackle the problem, again field resources are sent out unnecessarily. In some cases, a known problem might, for example, require special protective equipment and is therefore not addressed straight away because it takes time to obtain that special equipment. Being unaware of this, the customer service center might send out a field resource without the right equipment, which can lead to potential health and safety issues.

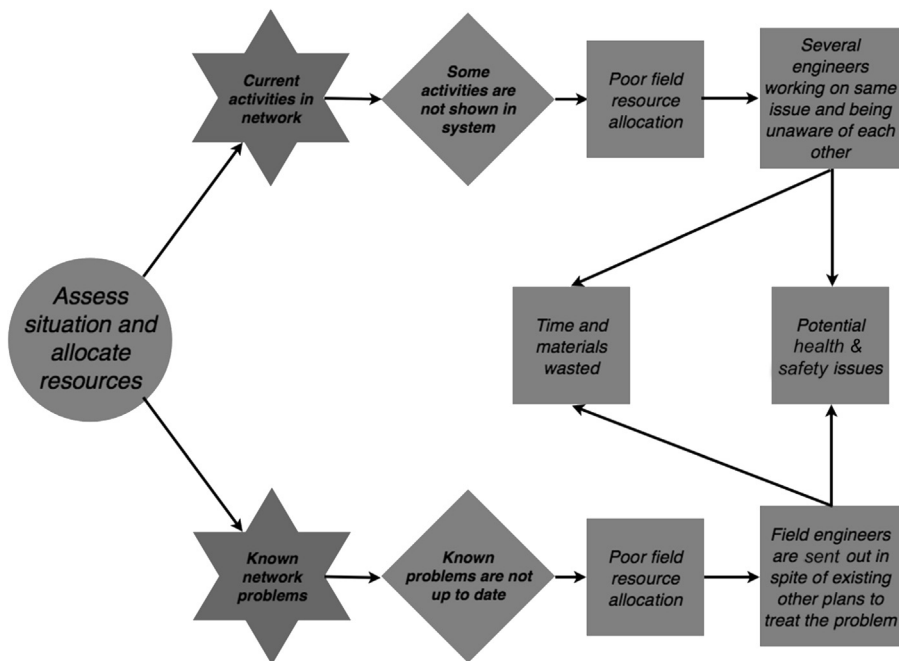
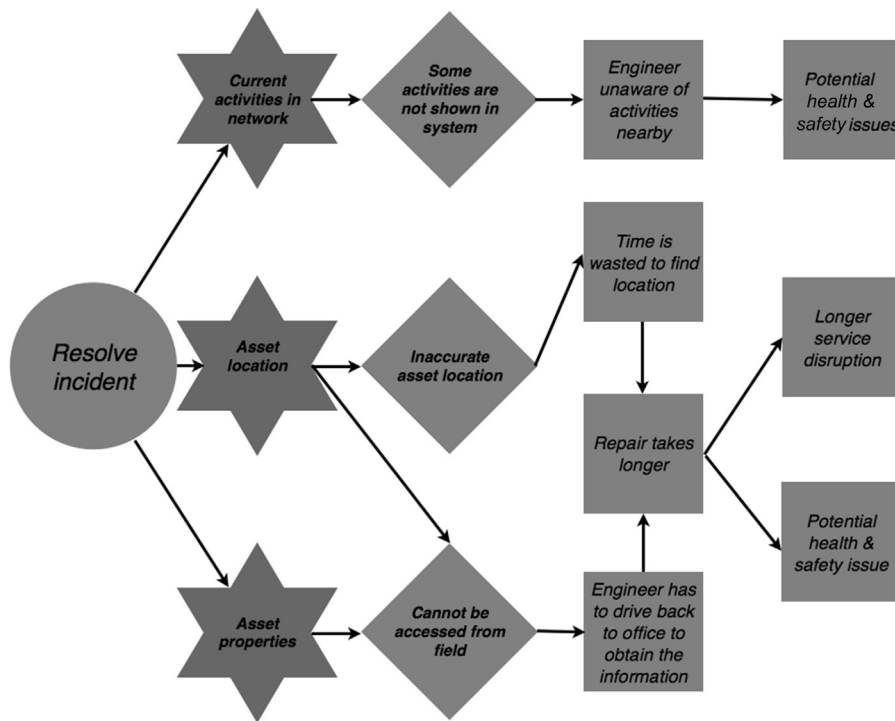


FIGURE 10.8

Consequences in the incident management process, part 1.

**FIGURE 10.9**

Consequences in the incident management process, part 2.

The second task to resolve the incident has three potential direct consequences of information quality problems, as shown in Figure 10.9. When a field engineer is not aware of ongoing activities in the electricity network that might affect his or her work, there might be problems regarding health and safety. Incorrect asset location information leads to time and resources being wasted to find the right location of the asset. When asset location or asset properties information is needed in the field, it cannot be accessed, and therefore, the engineer has to drive back to the office to print out the information. In both cases, the repair can take longer, which can lead to a lengthier disruption of service. Moreover, occasionally the incident might cause hazards for people and the environment, therefore a longer repair time creates a higher exposure to risk in terms of health and safety.

Step B5: Identify for each consequence the business objectives that are affected

In this step, the impact of each consequence on the business objectives identified in step A3 is identified. Figure 10.10 shows which business objectives are affected by poor information quality in the assess the situation and allocate resources task. The consequence of time and materials being wasted has an impact on the business objective of cost effectiveness, whereas the consequence of potential health and safety issues has an impact on the business objective of safety and environment.

Figure 10.11 shows which business objectives are affected by poor information quality in the resolve incident task.

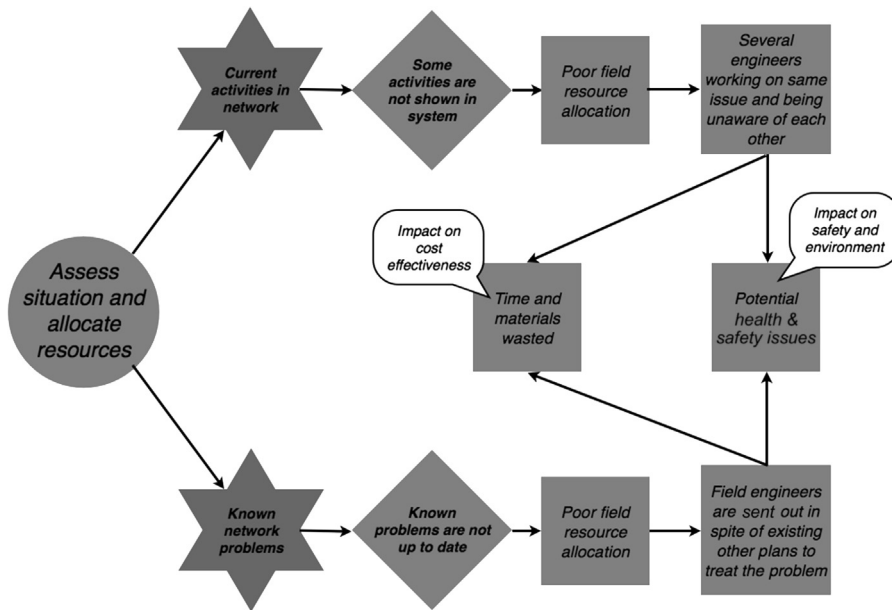


FIGURE 10.10

Affected business objectives in the incident management process, part 1.

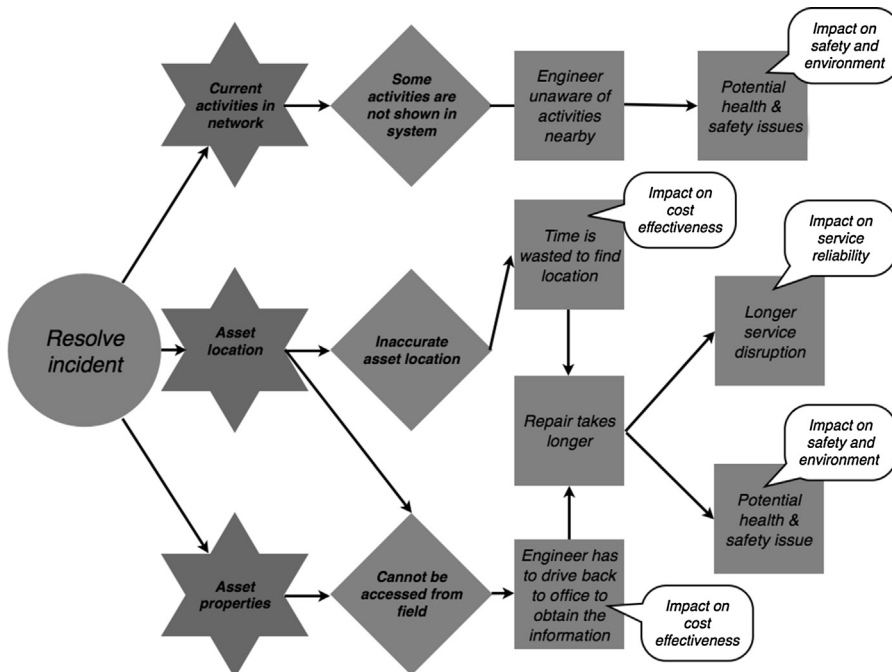
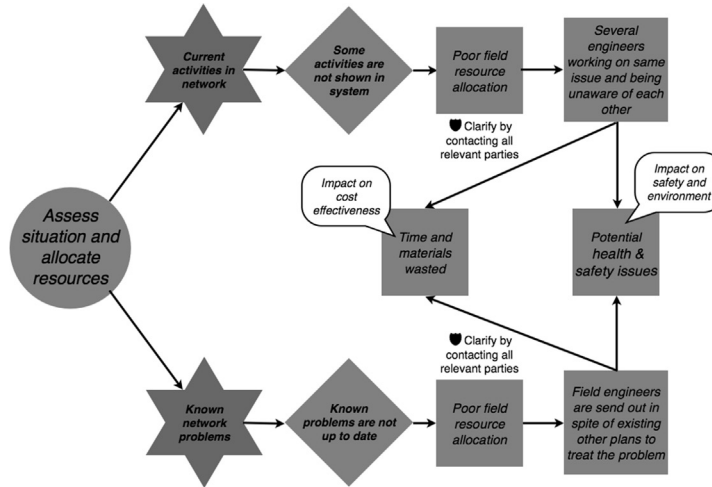


FIGURE 10.11

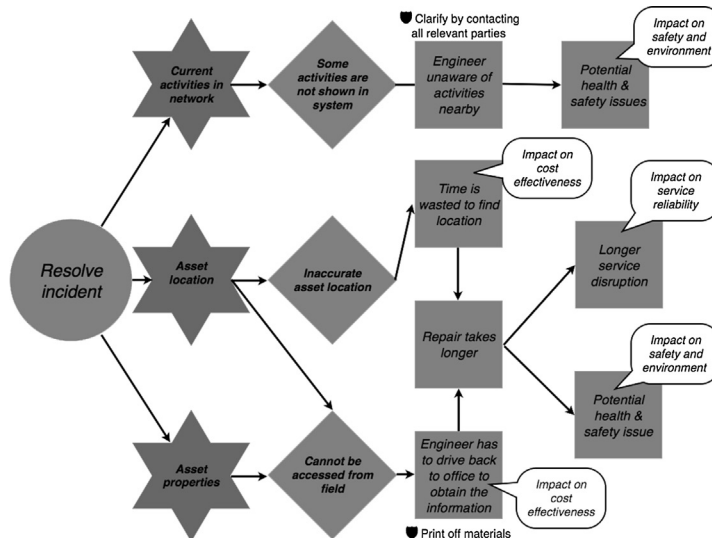
Affected business objectives in the incident management process, part 2.

Step B6: Examine existing risk controls

When assessing the situation and allocating resources, ongoing activities in the network and information about known problems are crucial to make the right resource allocations. To prevent poor information quality leading to a wrong allocation, in important cases managers from different departments are called to make sure that the information is complete and accurate (Figure 10.12). Engineers who resolve the incident to prevent safety risks, as shown in Figure 10.13, undertake the same actions. This

**FIGURE 10.12**

Risk controls in the incident investments process, part 1.

**FIGURE 10.13**

Risk controls in the incident investments process, part 2.

risk control is nevertheless quite time intensive and costs the company on average around \$20 USD because of the lost time. Still, this only partially prevents the consequences from ensuing, as issues regarding information quality are not being discovered.

When engineers plan to go offsite, they often print out data about asset properties and asset location, as they know that they cannot access the data from the field (Figure 10.13). However, this risk control only works in certain cases, because often engineers cannot foresee which data they will actually need. The printing costs each time are around \$5 USD on average.

Step B7: Estimate likelihood and impact of each consequence

Figure 10.14 shows the probabilities of consequences and the quantified impact on business objectives for the assess the situation and allocate resources task of the business process. For example, the consequence of poor field resource allocation follows with a 20% probability when information about current activities in the network is needed during task execution and some activities are not shown in the system. Moreover, this risk causes the consequence of several engineers working on the same issue and being unaware of each other with a probability of 10%, which results in potential health and safety issues having an impact of 100 on the scale defined in step A4 on the business objective of safety and environment with a likelihood of 50%. It always leads to time and material being wasted, which costs \$1000 per average incident.

Figure 10.15 shows the probabilities and the quantitative impact on business objectives of consequences for the resolve incident task of the incident management process.

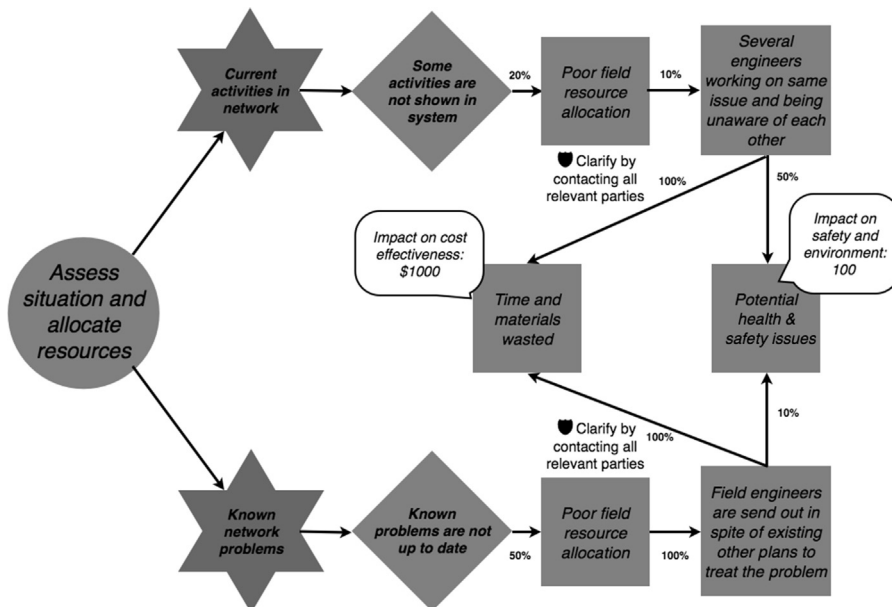


FIGURE 10.14

Probability and impact of each consequence in the incident investments process, part 1.

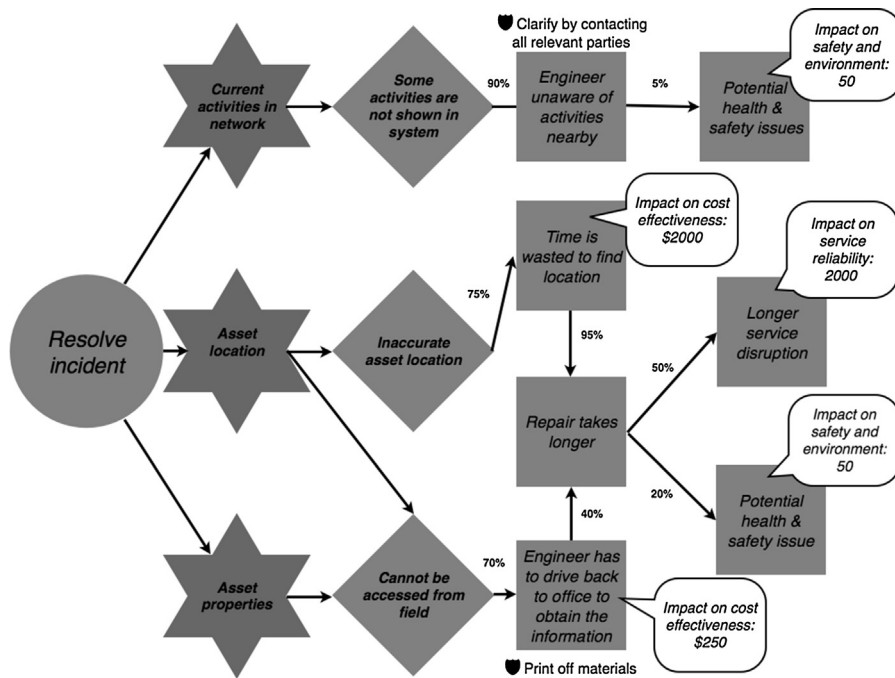


FIGURE 10.15

Probability and impact of each consequence in the incident investments process, part 2.

Step B8: Refine numbers and verify results

For each business process, the TIRM process manager who checked the modeling input and suggested changes identified at least one more subject-matter expert. In some cases, there was some larger disagreement and a meeting was organized to resolve the dispute. The finalized results are discussed here.

The refined and finalized model for the assess the situation and allocate resources task of the incident management process is shown in Figure 10.16. The changes are highlighted with a tools symbol. During the check of the numbers, it came up that poor field resource allocation follows the information quality problem of activities not shown in the system, with a probability of 30% rather than 20%. Also, when information about known network problems is not up to date and a poor field allocation happens, field engineers are not always sent out in vain, but rather in four out of five cases (80%, as highlighted in figure).

Figure 10.17 shows the adjusted model for resolving the incident. An average service disruption caused by a longer repair affects, on average, 1000 customers for one hour, and not 2000 customers as indicated during the initial analysis (highlighted in bold and underlined). Moreover, a potential health and safety issue happens in only 10% of cases, in contrast to 20%, when a repair takes longer (highlighted in gray box).

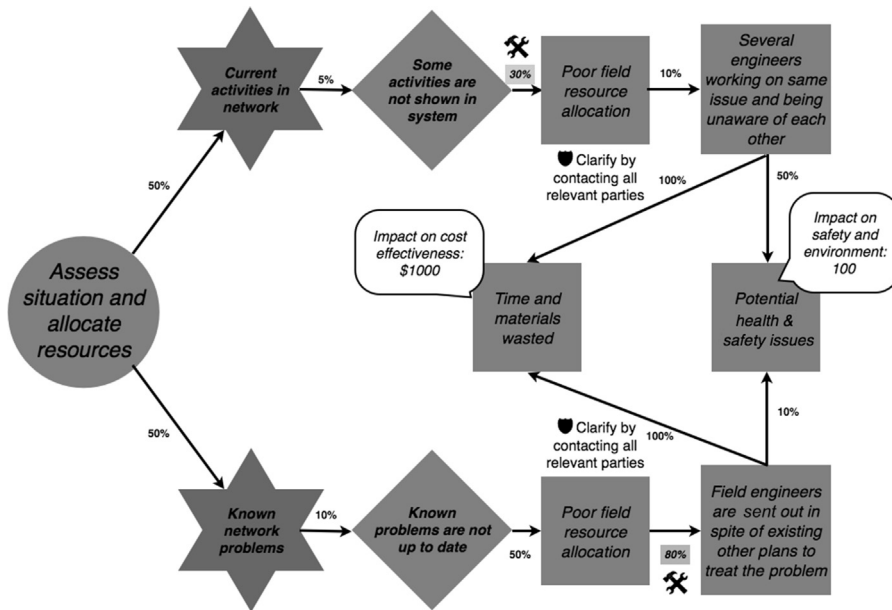


FIGURE 10.16

Finalized refined model of the assess the situation and allocate resources task in the incident investments process, part 1.

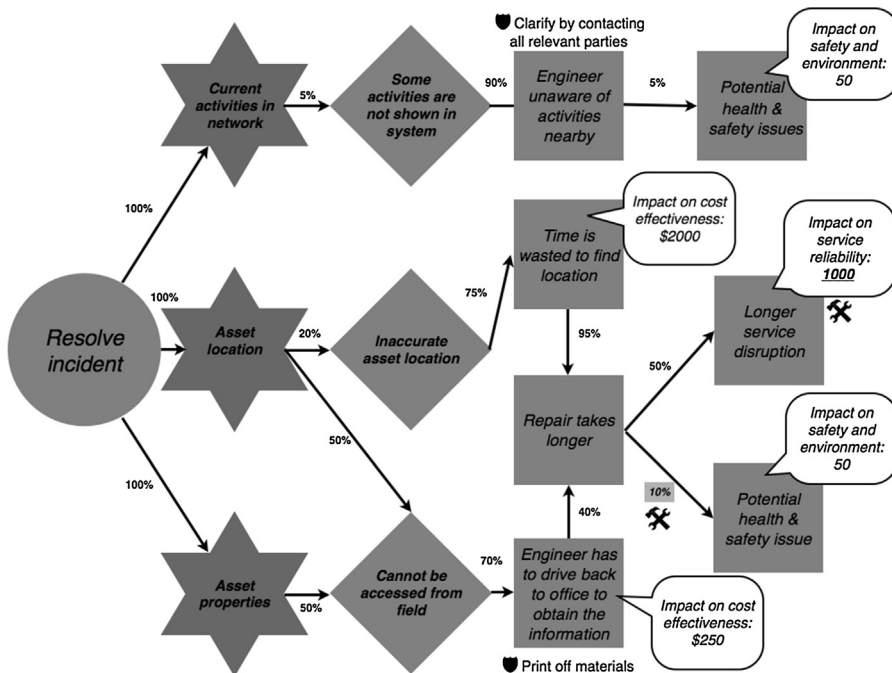


FIGURE 10.17

Finalized refined model of the resolve incident task in the incident investments process, part 2.

Business process 2: New connections

Step B1: Analyze tasks in each business process

The new connections process handles customer queries for new property developments that need to be connected to the electricity network (Figure 10.18). The requests come from private households as well as professional developers. Each request needs to be evaluated and a quote is given to the customer. There are roughly 200 requests per month, but not all of the requests actually lead to a new connection, for example, because the clients decide not to construct a new building after all. Around 120 times per month a new household or industrial property is actually connected to the electricity network.

Step B2: Examine information needed for each task

Two essential pieces of information that are always used for both tasks in the process are information about the asset location and information about the attributes of assets (Figures 10.19 and 10.20). Information about the location is needed during request evaluation to assess the costs of the new connection, which depends on the distance of the new property to the nearest electricity line. However, only certain electricity lines are usable for a new connection, so this is where asset attributes become important. Note that other pieces of information, such as information about the availability of materials and customer payments, are also essential for the new connections process, however, they are out of the scope of the TIRM process application as defined by the TIRM steering council.

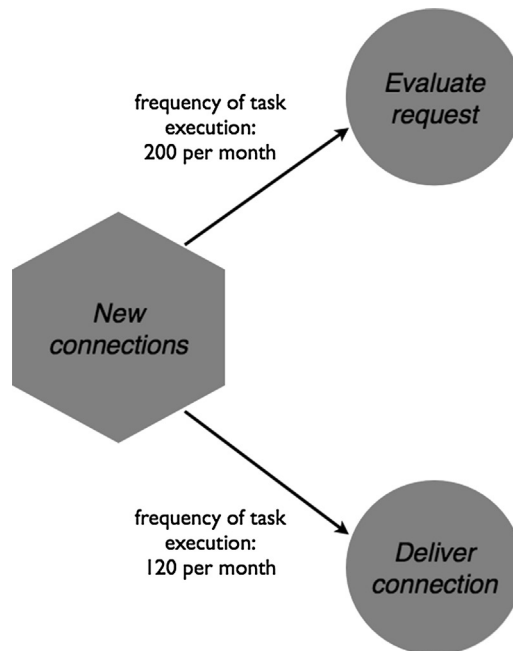


FIGURE 10.18

New connections process.

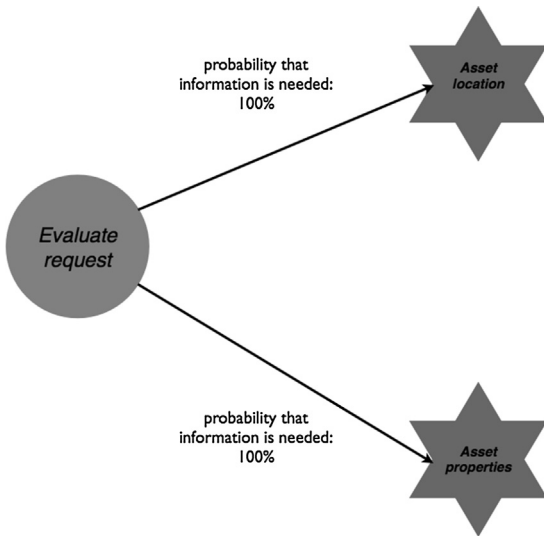


FIGURE 10.19

Information needs for new connections, part 1.

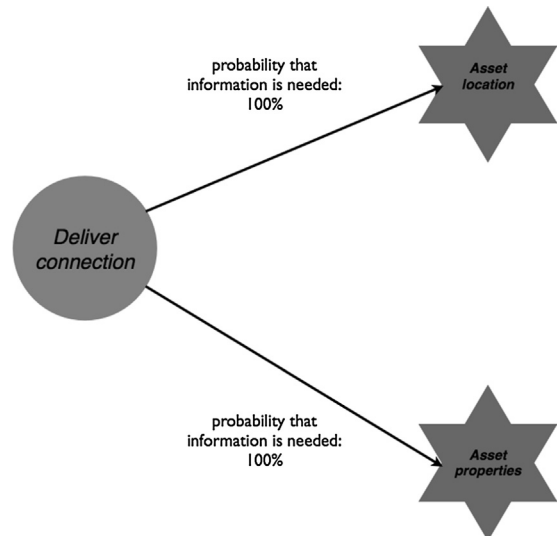


FIGURE 10.20

Information needs for new connections, part 2.

Step B3: Identify information quality problems during task execution

In the new connections process, both tasks suffer from the same information quality problems, as shown in Figures 10.21 and 10.22. In 20% of cases, asset location is not accurate and causes problems. In 10% of the evaluate request tasks and in 30% of the deliver connection tasks, when the engineer needs the information about asset location and asset properties, it cannot be accessed, because the engineer is out in the field and does not have connection to the IT system. Moreover, some information about asset properties that are needed for evaluating requests and delivering the connection are not available in 15% of times.

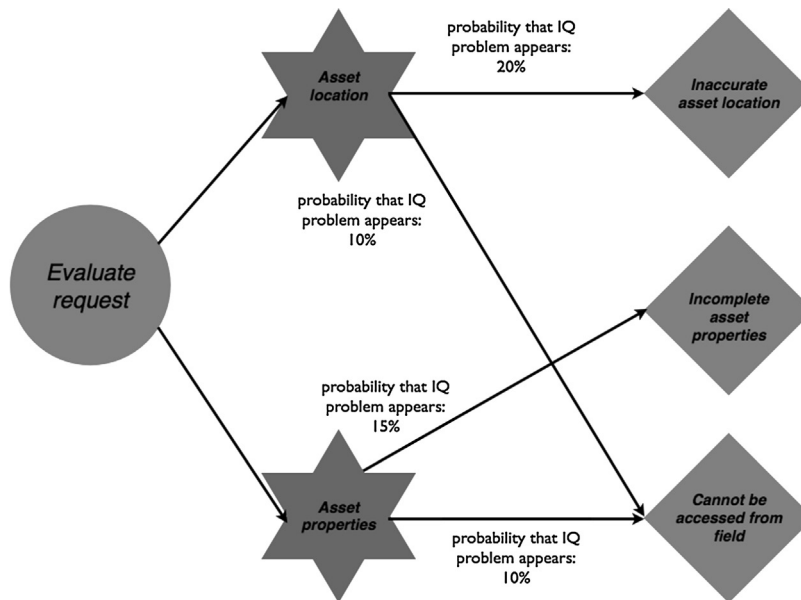
Step B4: Identify consequences of information quality problems

When a customer request for connecting a new property to the electricity network is being evaluated, inaccurate asset location and incomplete asset properties information can lead to an incorrect cost calculation (Figure 10.23).

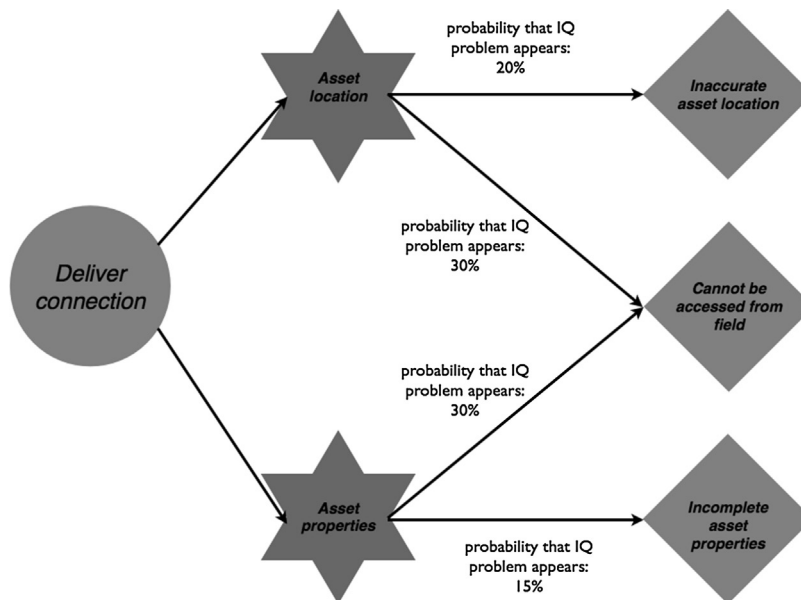
When the connection is supposed to be made (Figure 10.24), the same information quality problems can cause a delay of the installation, which is a disruption for the customer and increases the costs for LightBulbEnergy Inc. In both stages of new customer connections, during evaluation of the request and during delivery of the connection, engineers who need the information from the field have to drive back to the office to obtain the information, which is a waste of time and gas.

Step B5: Identify for each consequence the business objectives that are affected

The consequences of the wrong cost calculation and engineer has to drive back to the office to obtain the information clearly both impact the business objective of cost effectiveness, as illustrated in

**FIGURE 10.21**

Information quality problems in the new connections process, part 1.

**FIGURE 10.22**

Information quality problems in the new connections process, part 2.

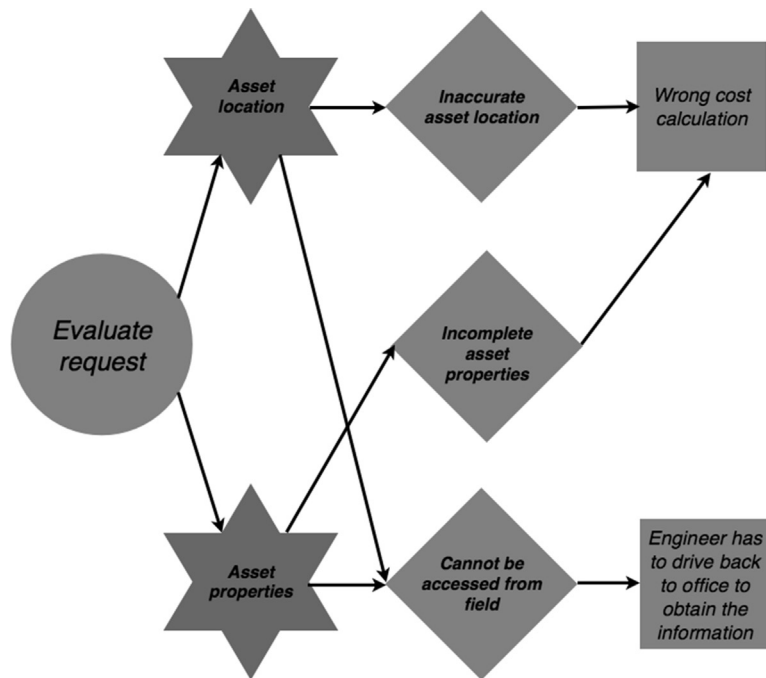


FIGURE 10.23

Consequences in the new connections process, part 1.

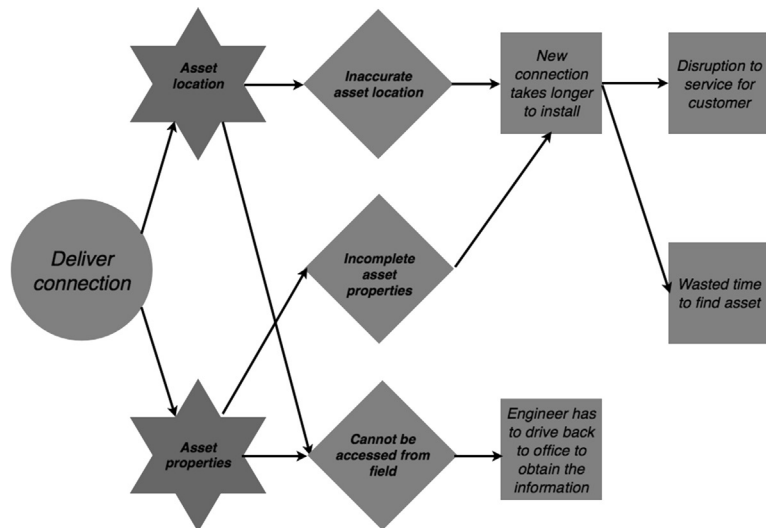


FIGURE 10.24

Consequences in the new connections process, part 2.

Figures 10.25 and 10.26. A disruption to the service of a customer has an impact on the business objective of service reliability.

Step B6: Examine existing risk controls

A risk control in the new connections process is to charge customers more to make up for additional costs when incorrect cost calculations are made during the request evaluation, as shown in Figure 10.27.

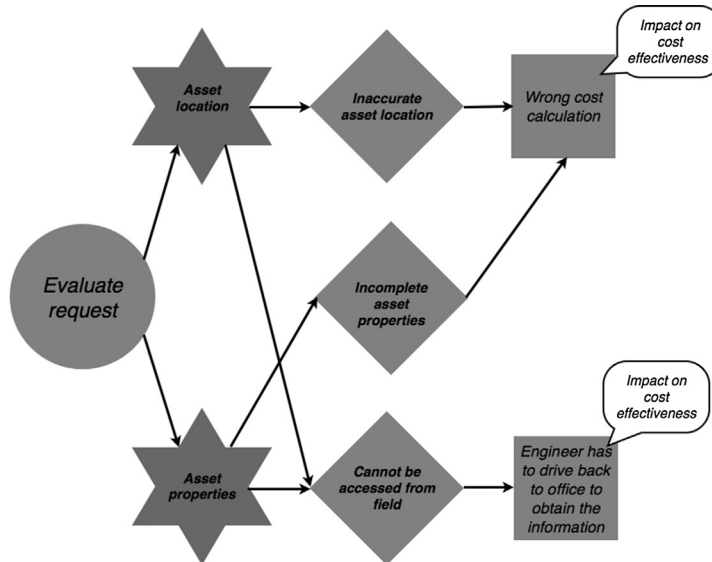


FIGURE 10.25

Affected business objectives in the new connections process, part 1.

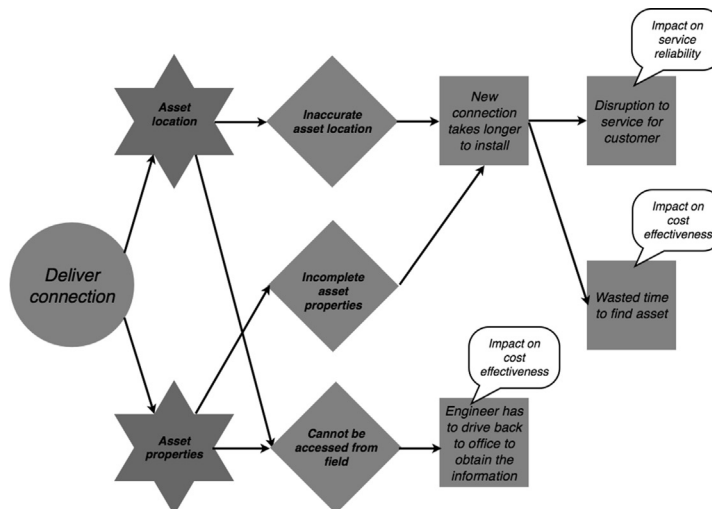


FIGURE 10.26

Affected business objectives the new connections process, part 2.

Moreover, when engineers plan to go offsite to evaluate the request or to deliver the connection, the data about asset properties and asset location is often printed out in paper form as they know that they cannot access the data while in the field (Figures 10.27 and 10.28).

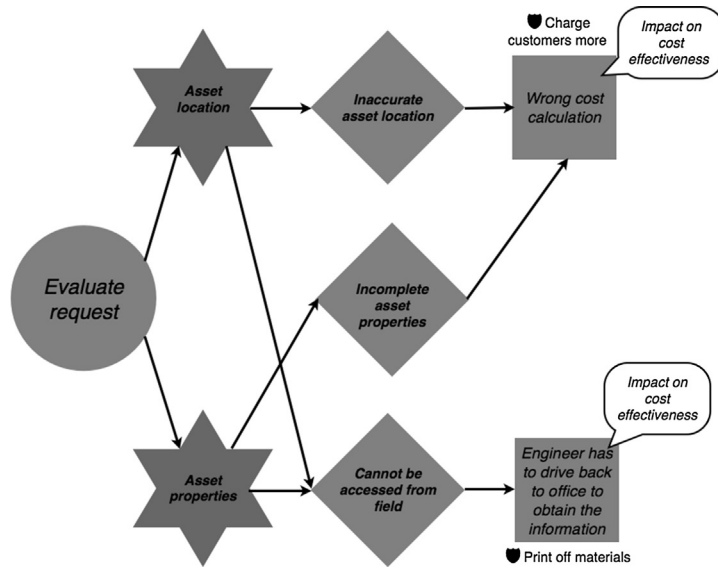


FIGURE 10.27

Risk controls in the new connections process, part 1.

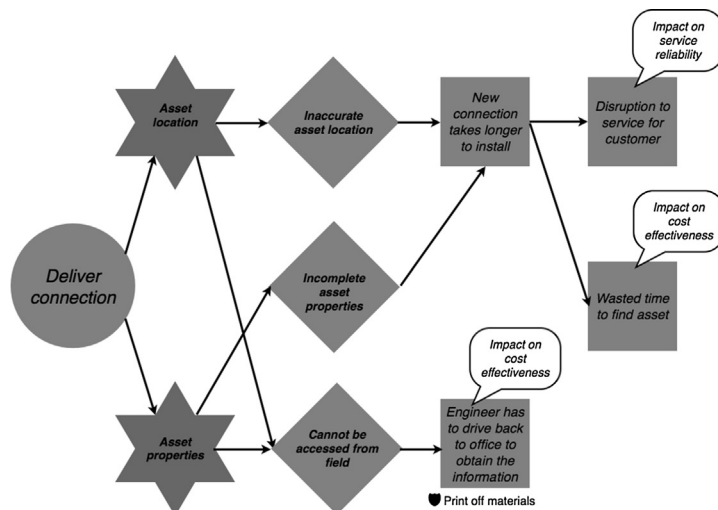


FIGURE 10.28

Risk controls in the new connections process, part 2.

Step B7: Estimate likelihood and impact of each consequence

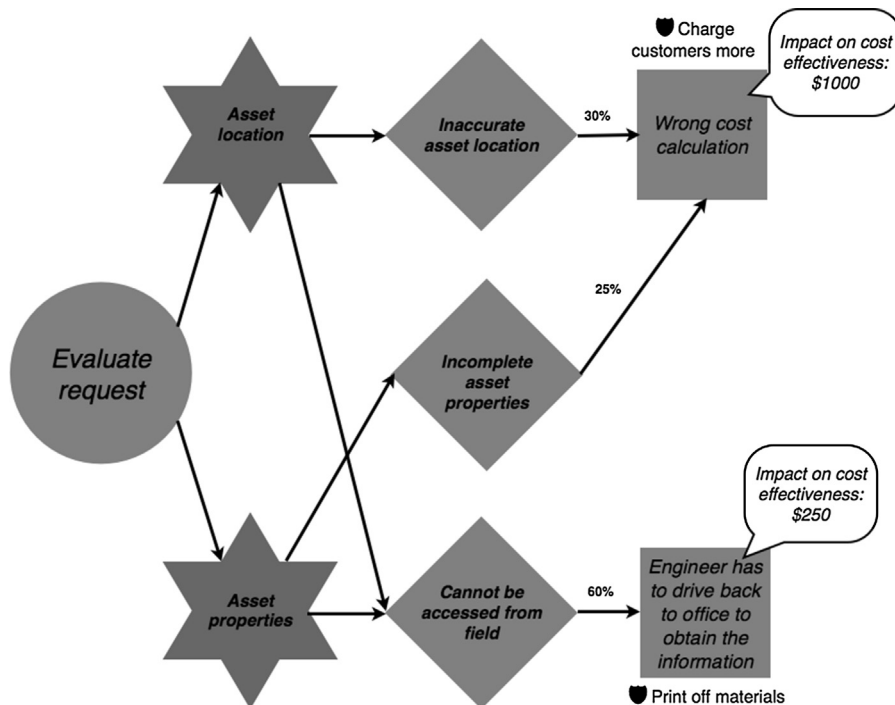
Figure 10.29 illustrates the probabilities and the quantitative impact on business objectives of consequences for the evaluate request task of the new connections process.

Figure 10.30 displays the probabilities and the impact of each consequence for the deliver connection task of the new connections process.

Step B8: Refine numbers and verify results

The verification of the risk analysis by an additional subject-matter expert, a new connections manager, revealed that the costs of a wrong cost calculation during request evaluation lie, on average, at around \$2000 rather than \$1000 as originally anticipated (highlighted in Figure 10.31 with the tools symbol).

Furthermore, Figure 10.32 displays the refinements made in the deliver connection task. The costs for wasted time to find an asset are, on average, a bit lower as modeled (\$2000 instead of \$3000). Also, an engineer has to drive back to obtain information around 60% (and not 40%) of the time when he or she cannot access the required data from the field.

**FIGURE 10.29**

Probability and impact of each consequence in the new connections process, part 1.

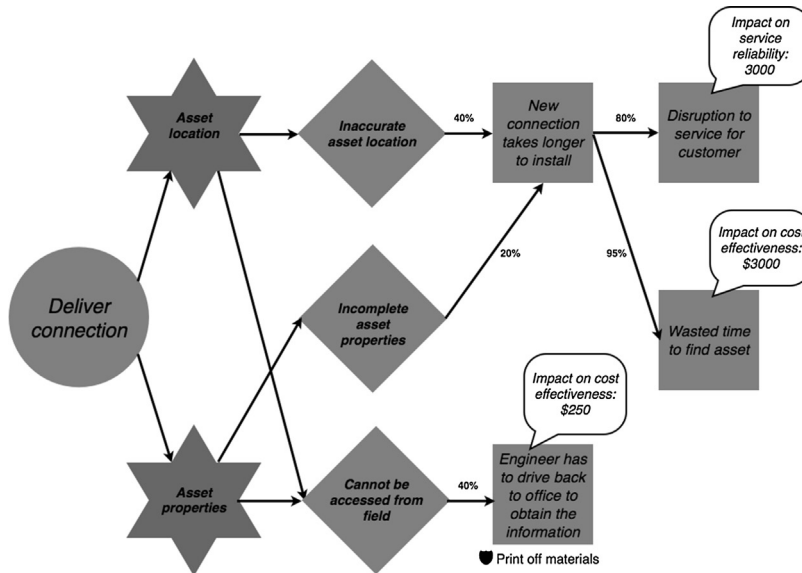


FIGURE 10.30

Probability and impact of each consequence in the new connections process, part 2.

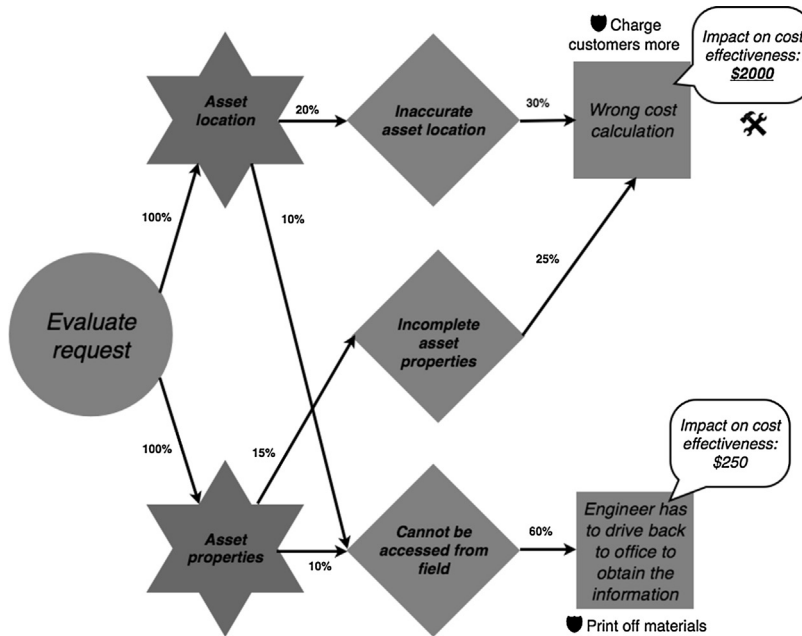


FIGURE 10.31

Finalized refined model of the evaluate request task in the new connections process, part 1.

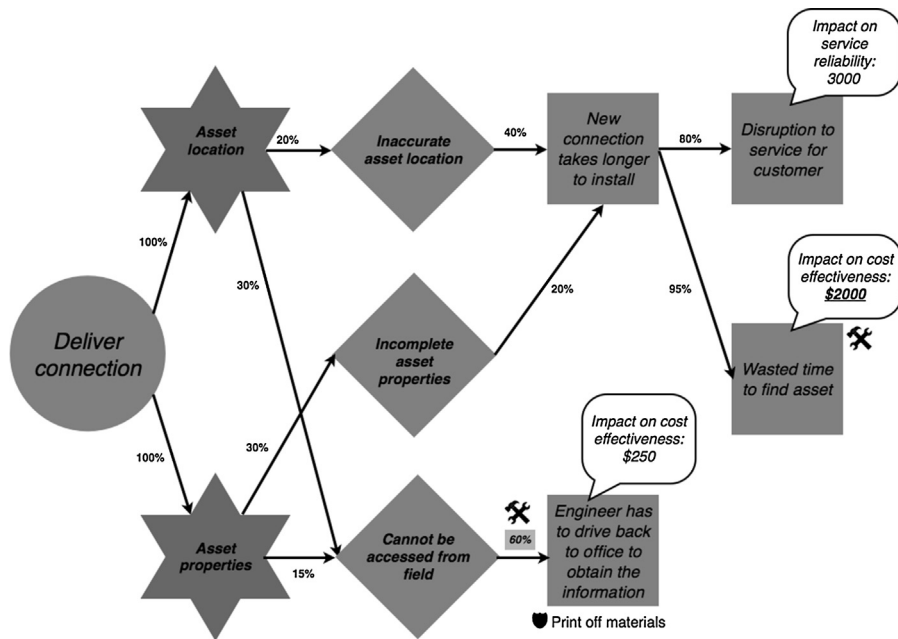


FIGURE 10.32

Finalized refined model of the deliver connection task in the new connections process, part 2.

Business process 3: Infrastructure investments

Step B1: Analyze tasks in each business process

The infrastructure investment process deals with investments in the electricity network, such as refurbishment, replacement, or building new electricity lines and substations (Figure 10.33). In particular, around 50 potential investments are identified per month, of which, on average, 35 per are actually implemented. The identify and select investments task involves the identification of investment needs and making the investment decision based on an evaluation of the costs, benefits, and risks of each investment. The selected investment projects are then planned and implemented (the plan and fulfill investments task).

Step B2: Examine information needed for each task

The last business process that deals with infrastructure investments also suffers from four information quality problems. For identifying and selecting investments, as shown in Figure 10.34, information about the asset condition is needed that gives a measure of the degree of the deterioration of the asset and remaining asset life. Moreover, information about faults occurring with the asset is also used.

For planning and executing the investment, shown in Figure 10.35, information about the location and properties of assets is key to understand in which geographical regions asset replacement and refurbishment is necessary and which type of treatment is required.

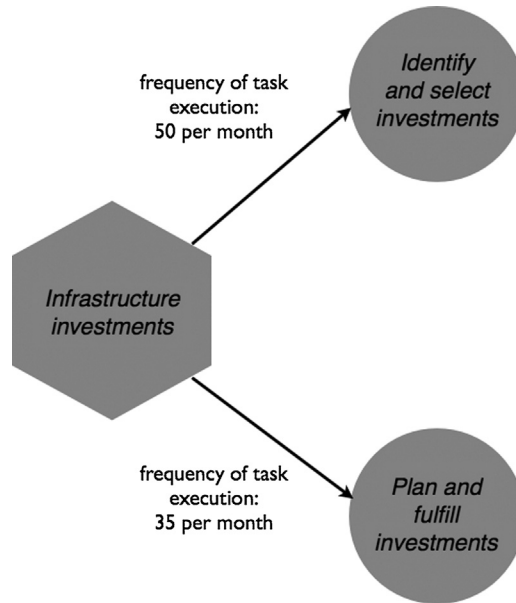


FIGURE 10.33

New connections process.

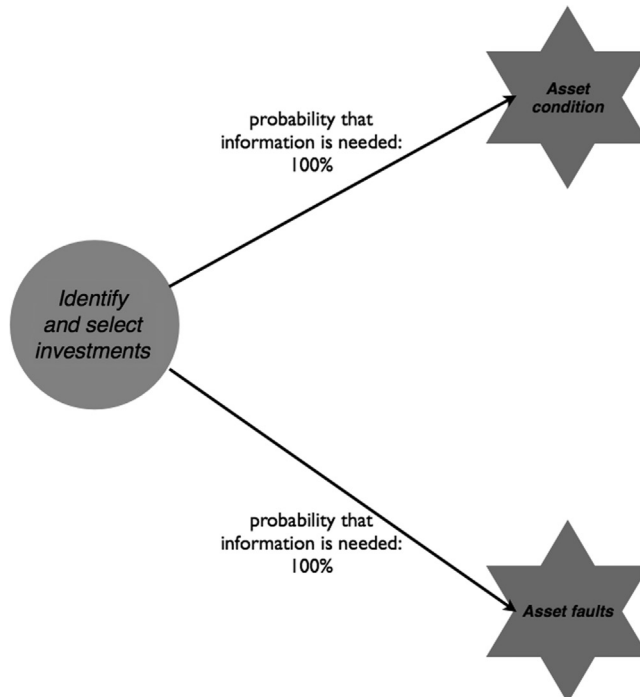
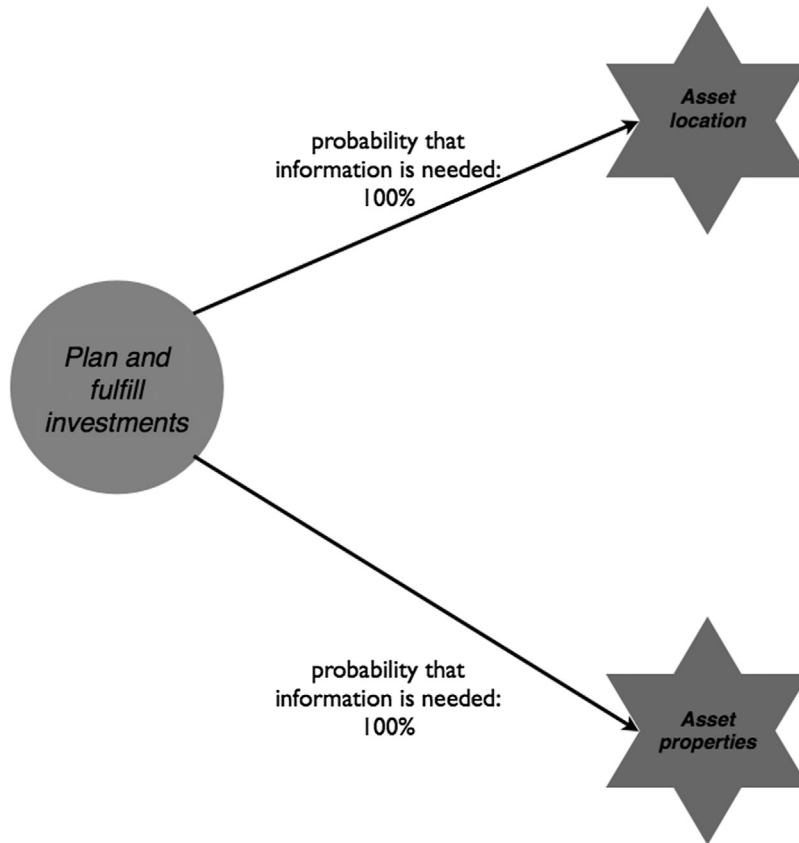


FIGURE 10.34

Information needs for infrastructure investments, part 1.

**FIGURE 10.35**

Information needs for infrastructure investments, part 2.

Step B3: Identify information quality problems during task execution

When investments are identified and selected, in 25% of cases when asset fault data is needed, there are some asset faults missing in the historical records that are used to determine the probability of failure (Figure 10.36). Furthermore, information about the condition of the asset is incorrect in 10% of cases.

During planning and fulfillment of the network investments, information quality problems appear that are similar to those seen when information about asset location and asset attributes was needed (Figure 10.37). The information about the location of the asset is incorrect in 20% of cases and information about key attributes of the asset is not available in 15% of cases. Before engineers go out in the field, the location of assets and their key attributes are printed out on paper. In 10% of cases, additional information is needed in the field that has not been anticipated, which then is not accessible. The problem comes up when additional information is required when the fulfillment engineers are already in the field.

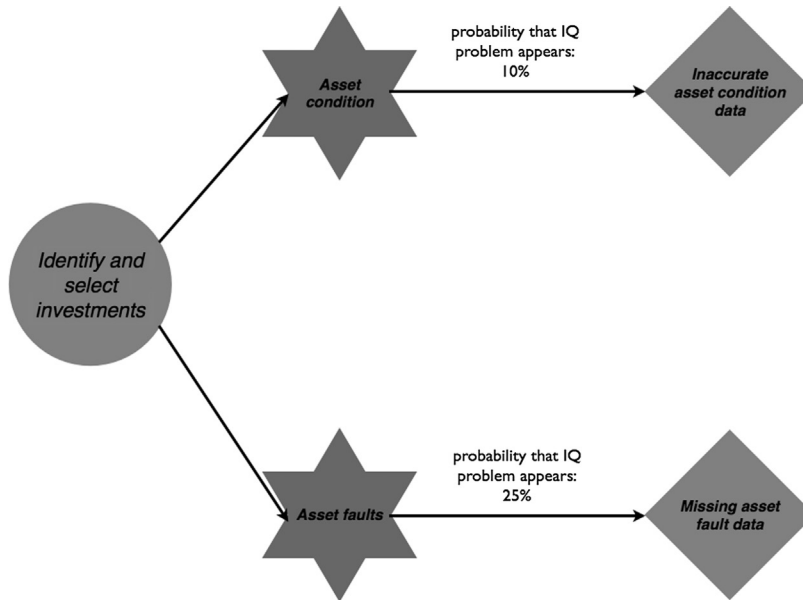


FIGURE 10.36

Information quality problems in the infrastructure investment process, part 1.

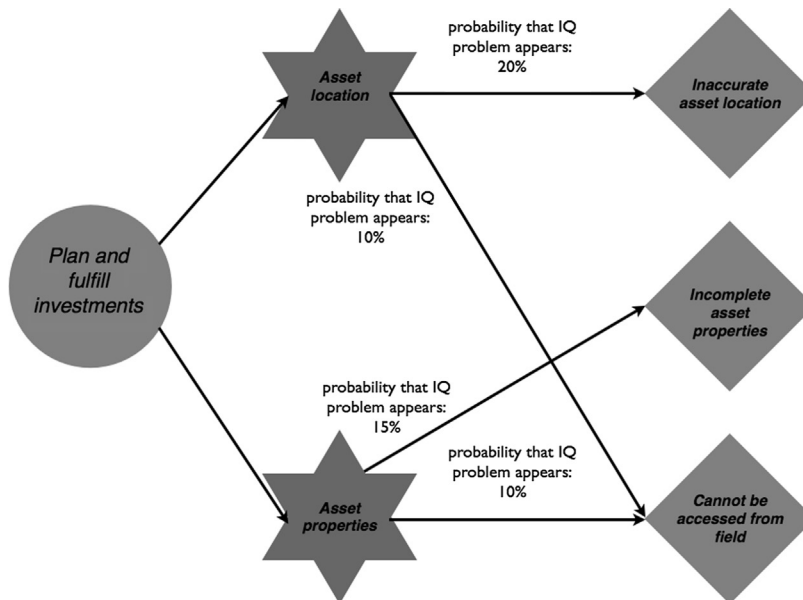


FIGURE 10.37

Information quality problems in the infrastructure investment process, part 2.

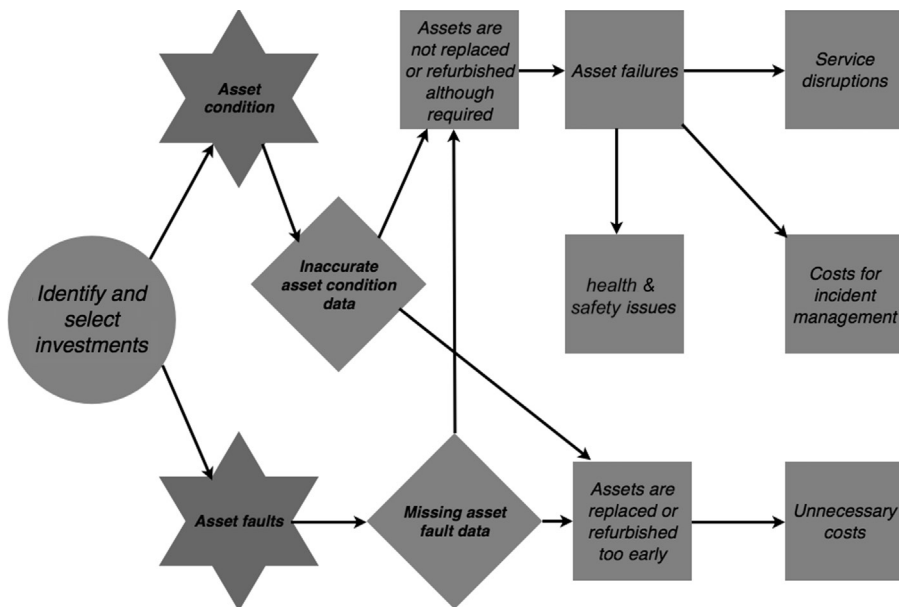
Step B4: Identify consequences of information quality problems

The identification and selection of infrastructure investments relies heavily on data about the condition of assets and previously experienced faults (Figure 10.38). The asset condition data is, however, sometimes incorrect and often information about asset faults is missing in the database or is recorded at a higher level because the failed asset could not be correctly identified when the fault was first recorded. Both information quality problems can potentially lead to very similar direct consequences, as they can cause a suboptimal investment decision. Simply speaking, either the assets are refurbished and/or they are replaced too early or too late. Doing it too early causes unnecessary costs, as the asset could have been used for a longer time. Not replacing or refurbishing assets when necessary can lead to asset failures in the electricity network. Asset failures can cause costs for incident management or might lead to disruptions in service to the customer (e.g., power outages). In extreme cases, asset failures can be dangerous for employees, the general population, and the environment.

During implementation of the investment, inaccurate asset location and incomplete asset properties can lead to higher implementation costs (Figure 10.39). Moreover, when engineers need the information while being on the construction site, they need to go back to their office to get the information.

Step B5: Identify for each consequence the business objectives that are affected

Information quality problems have an impact on all three different business objectives when infrastructure investments are evaluated and chosen (Figure 10.40). Service disruptions due to asset failure

**FIGURE 10.38**

Consequences in the infrastructure investments process, part 1.

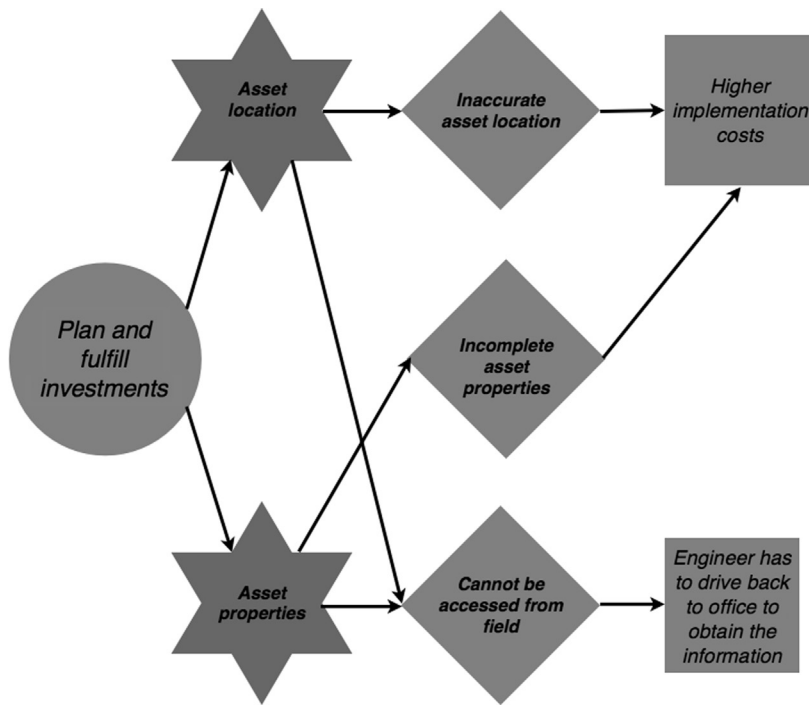


FIGURE 10.39

Consequences in the infrastructure investments process, part 2.

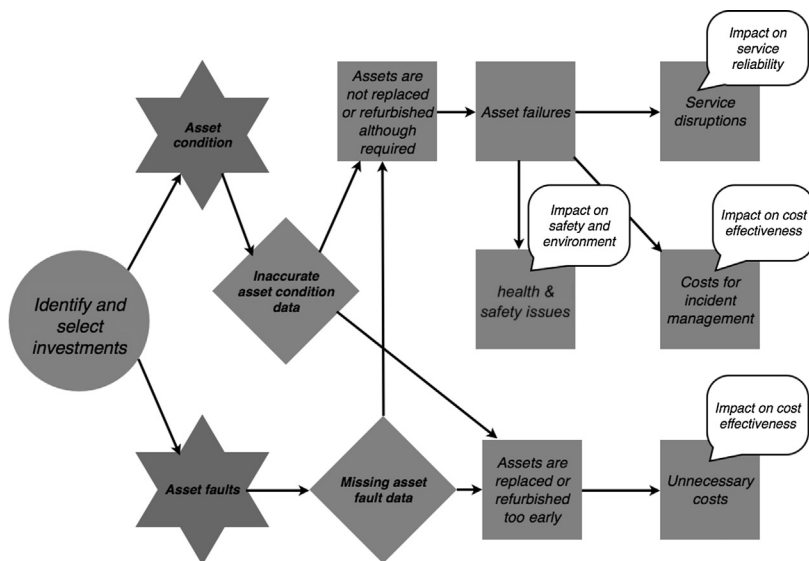


FIGURE 10.40

Affected business objectives in the infrastructure investments process, part 1.

have an impact on service reliability. Asset failures also increase the costs as the incident has to be managed, which impedes cost effectiveness and in some cases leads to health and safety problems that impact the business objective of safety and environment.

When the investment is planned and fulfilled, higher implementation costs and engineers having to return unnecessarily to the office to obtain data both affect the business objective of cost effectiveness, as illustrated in Figure 10.41.

Step B6: Examine existing risk controls

Infrastructure investments based on low-quality data can lead to assets not being replaced or not refurbished when needed. When in doubt, infrastructure investments like refurbishment and maintenance activities are ideally carried out earlier to prevent asset failures from occurring; this is one risk control taken, as illustrated in Figure 10.42. To prevent investments taking a suboptimal time (i.e., too early or too late), an additional risk control is that the assets are checked onsite.

As before, during planning and fulfillment, engineers print out data about asset properties and asset location, as they know that they cannot access the data from the field, (Figure 10.43).

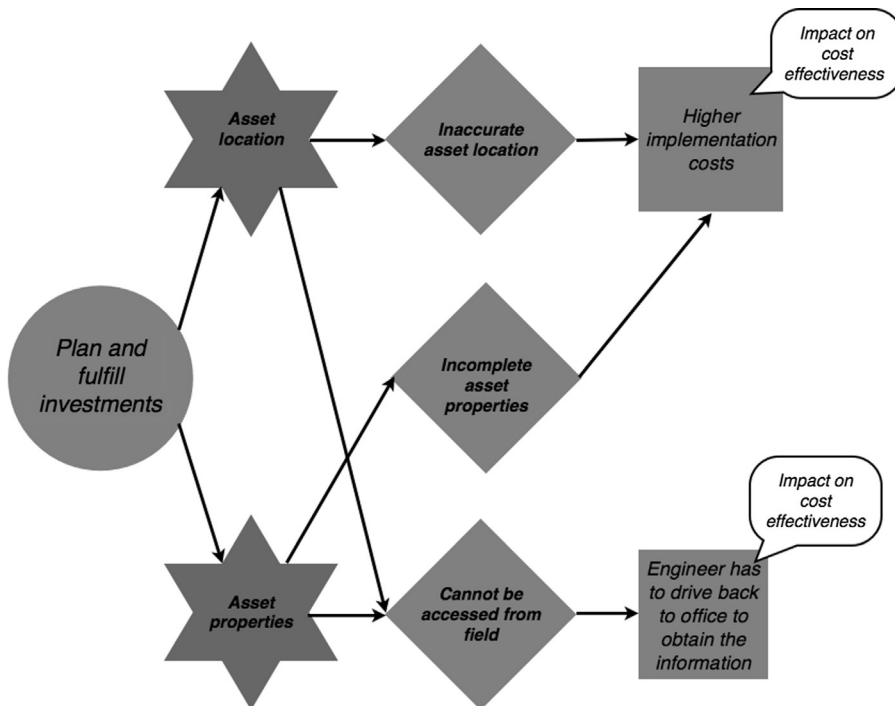


FIGURE 10.41

Affected business objectives in the infrastructure investments process, part 2.

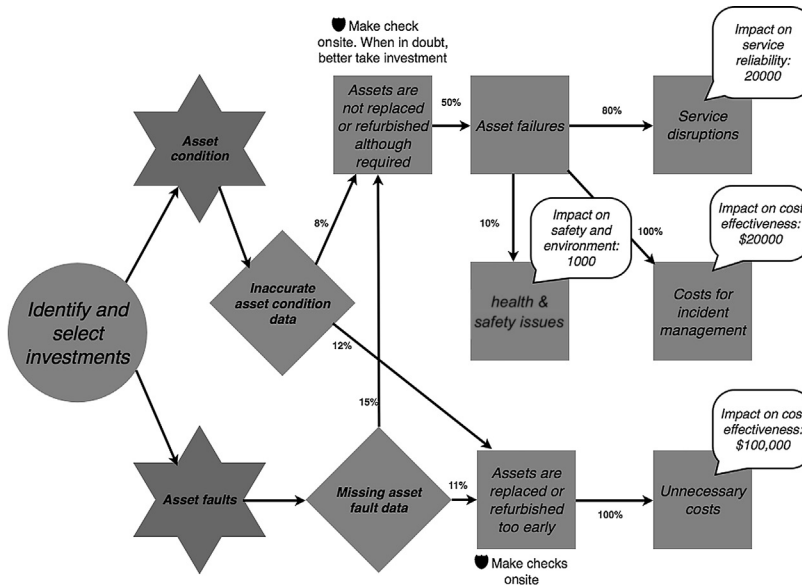


FIGURE 10.42

Risk controls in the infrastructure investments process, part 1.

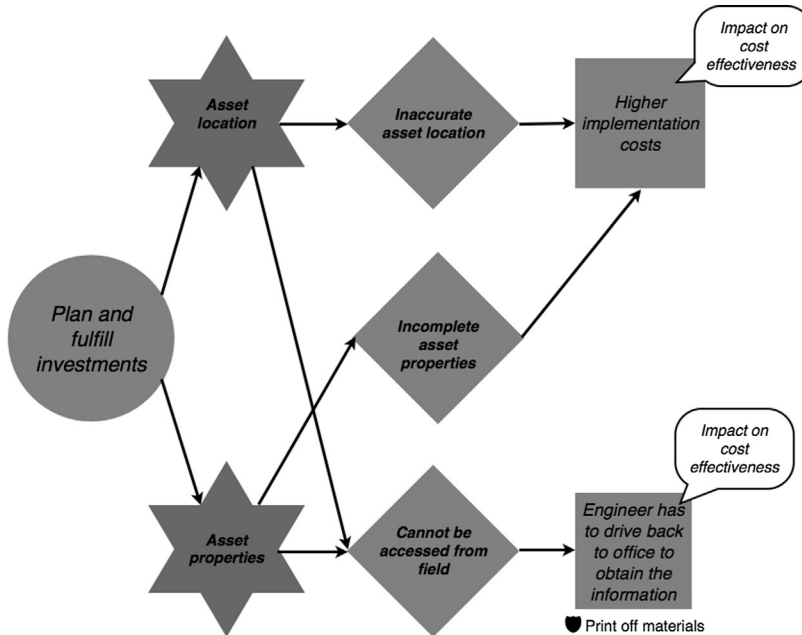


FIGURE 10.43

Risk controls in the infrastructure investments process, part 2.

Step B7: Estimate likelihood and impact of each consequence

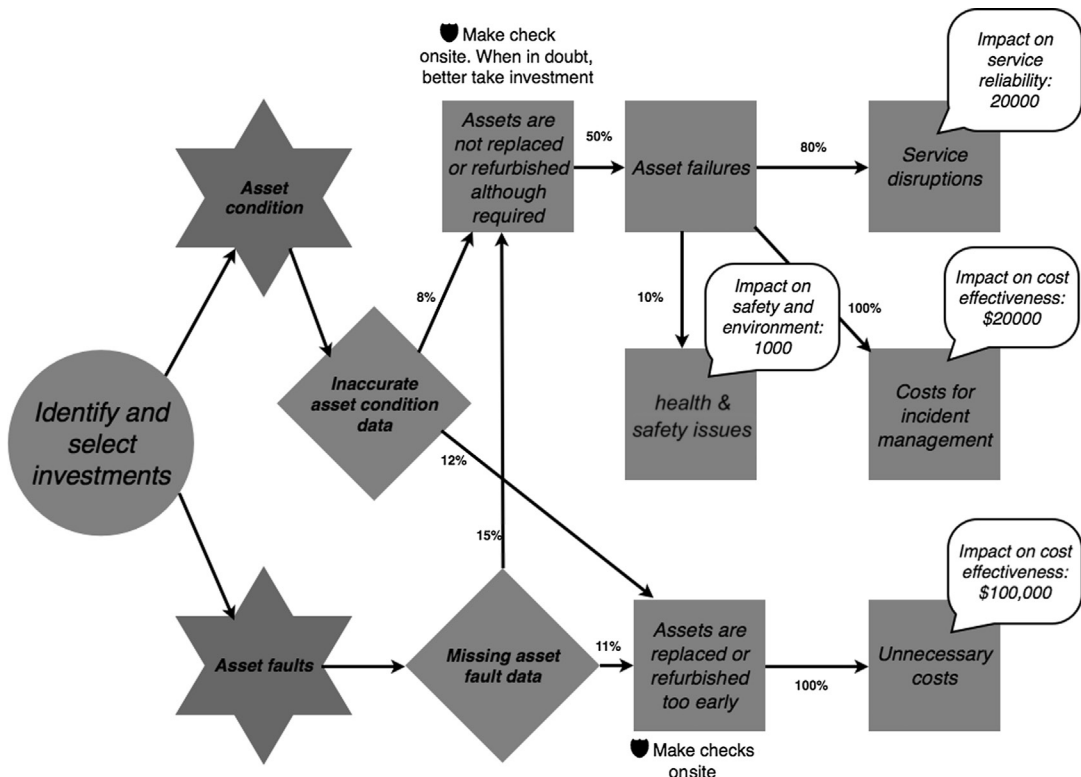
Figure 10.44 shows the probabilities and the quantitative impact on business objectives of consequences of information quality problems in the identify and select investments task of the infrastructure investments process.

Figure 10.45 shows the probability and the impact of each consequence of information quality problems in the plan and fulfill investments task of the infrastructure investments process.

Step B8: Refine numbers and verify results

Figures 10.46 and 10.47 show the refined model of the infrastructure investments process. The changes are again highlighted with a tools symbol. Further investigation revealed that during identification and selection of investments, missing asset fault data leads to the consequence that assets are not replaced or refurbished although required in 7% of cases, so significantly lower than the 11% originally anticipated.

Finally, as part of planning and fulfillment of an investment, historical data was found that shows that higher implementation costs, which are due to inaccurate asset location data or incomplete asset

**FIGURE 10.44**

Probability and impact of each consequence in the infrastructure investments process, part 1.

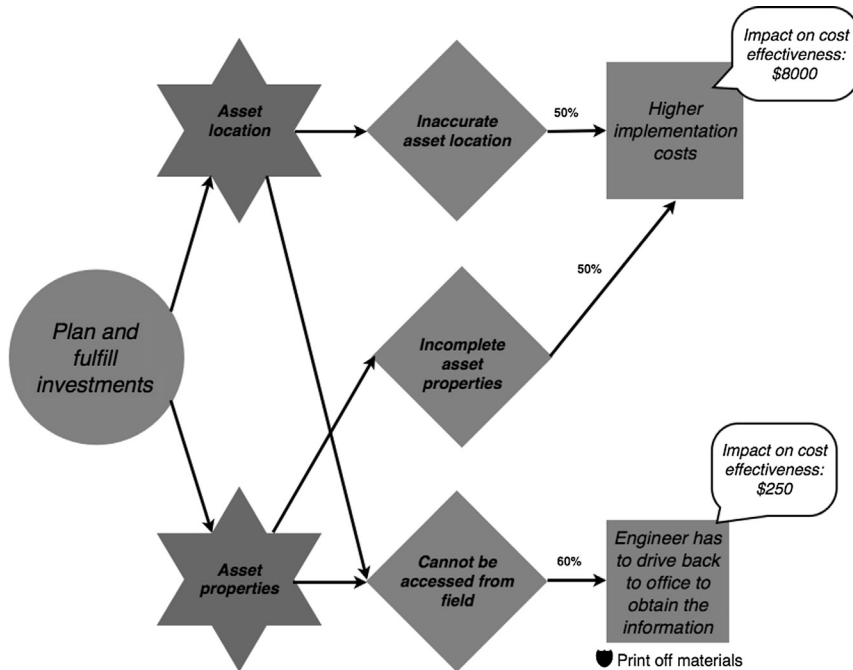


FIGURE 10.45

Probability and impact of each consequence in the infrastructure investments process, part 2.

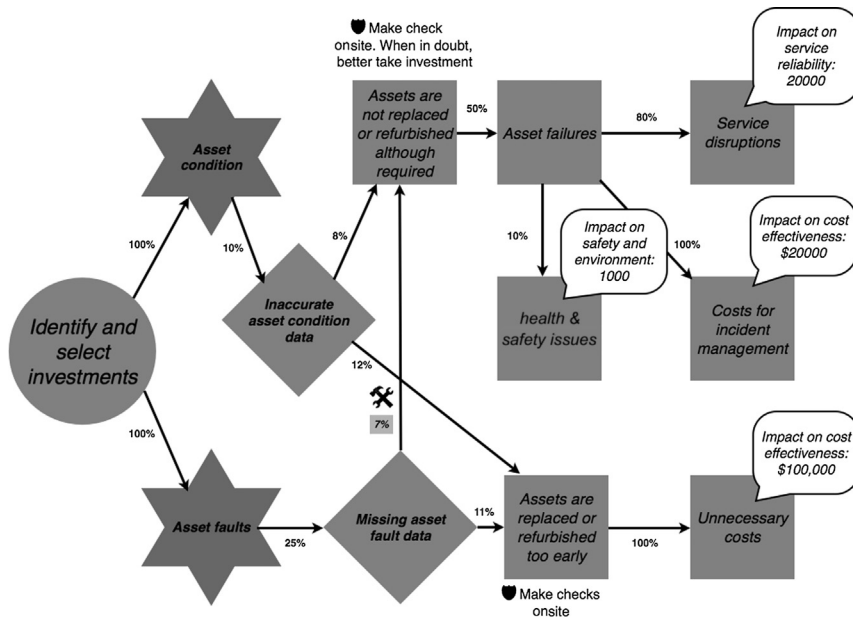


FIGURE 10.46

Finalized refined model of the identify and select investments task in the infrastructure investments process, part 1.

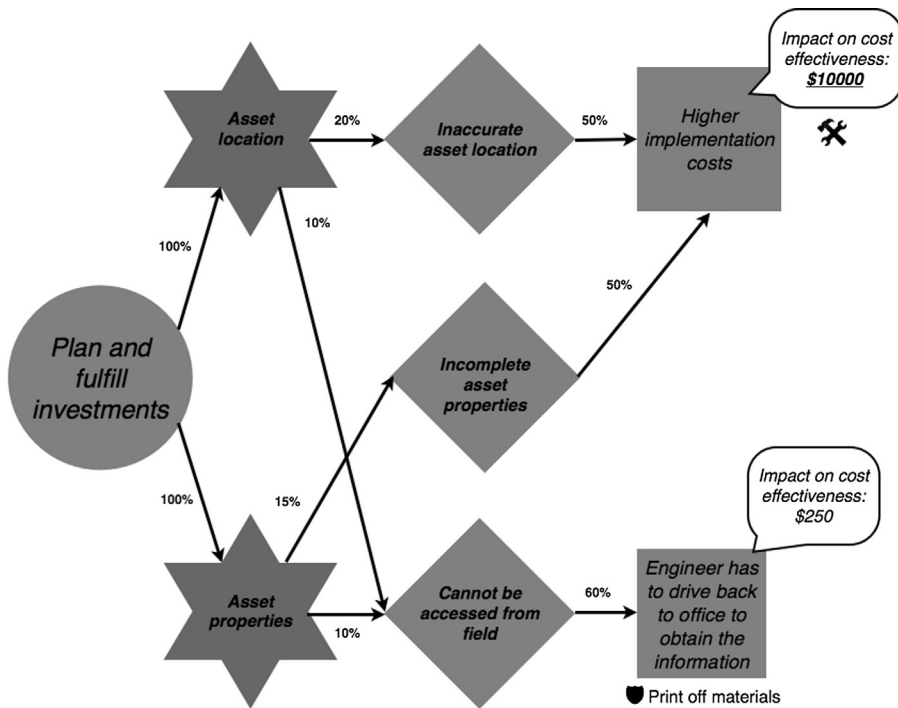


FIGURE 10.47

Finalized refined model of the plan and fulfill investments task in the infrastructure investments process, part 2.

properties data, lies at around \$10,000 on average and not \$8000 as assumed during the first round of analysis (underlined and bold in Figure 10.47).

Step B9: Evaluate and rank information risks

The total impact of each one of the information quality problems was calculated and the information risks were ranked in an information risk evaluation workshop. The results are summarized in Table 10.2.

Moreover, each information risk was compared to the risk criteria formulated in step A4 to evaluate it. The result of the evaluation is shown in Table 10.3. It was decided that the highest risk regarding the business objectives should be used as the overall evaluation. It was also determined that for all information risks that are evaluated as high or very high, information risk treatment is necessary.

After the information risk evaluation workshop was completed, the TIRM steering council decided that it was now time to move on to the information risk treatment stage.

Table 10.2 Ranked List of Information Risks (Time Horizon of One Year)

Rank	Information Quality Problem	Cost Effectiveness (Lost USD)	Service Reliability (Number of Hours without Service)	Safety and Environment (Custom Metric)
	Total	\$5,642,310	2,777,940 hours	11,625
1	Inaccurate asset location	\$1,650,720	1,339,380 hours	2565
2	Missing asset fault data	\$1,755,000	84,000 hours	525
3	Incomplete asset properties	\$392,040	812,160 hours	0
4	Asset location cannot be accessed from field	\$434,700	252,000 hours	2520
5	Asset properties cannot be accessed from field	\$392,850	252,000 hours	2520
6	Known problems are not up to date	\$240,000	0 hours	2400
7	Inaccurate asset condition data	\$768,000	38,400 hours	240
8	Some activities are not shown in system	\$9000	0 hours	855

Table 10.3 Information Risk Evaluation

Rank	Information Quality Problem	Cost Effectiveness	Service Reliability	Safety and Environment	Overall Evaluation
	Total	Very high	Very high	Very high	Very high
1	Inaccurate asset location	High	High	High	High, treatment required
2	Missing asset fault data	High	Low	Low	High, treatment required
3	Incomplete asset properties	Low	High	Very low	High, treatment required
4	Asset location cannot be accessed from field	Low	Medium	High	High, treatment required
5	Asset properties cannot be accessed from field	Low	Medium	High	High, treatment required
6	Known problems are not up to date	Low	Very low	High	High, treatment required
7	Inaccurate asset condition data	Medium	Low	Low	Medium
8	Some activities are not shown in system	Very low	Very low	Low	Low

STAGE C: INFORMATION RISK TREATMENT

The TIRM process manager organized a two-day workshop with the IT system and database representatives, TIRM process facilitators, and selected members of the TIRM steering council.

Step C1: Analyze causes of information quality problems

As a first step, they investigated the root causes of each of the information quality problems that require treatment. This was done by drawing a fishbone diagram and using the categories technology, organization, and people to categorize potential root causes. Figures 10.48 to 10.50 show the results of the root-cause analysis.

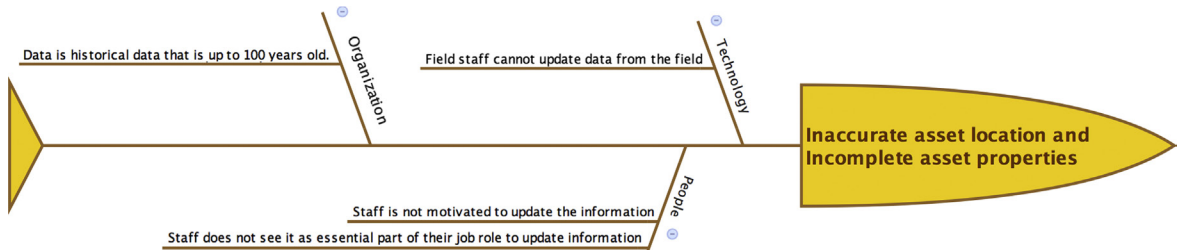


FIGURE 10.48

Root-cause analysis for information quality problems of inaccurate asset location and incomplete asset properties.

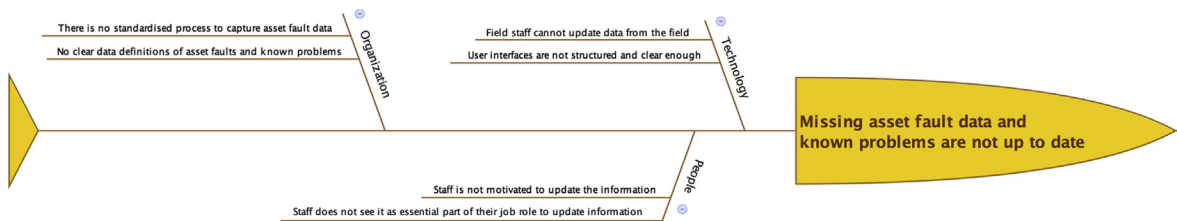


FIGURE 10.49

Root-cause analysis for information quality problems of missing asset fault data and known problems are not up to date.

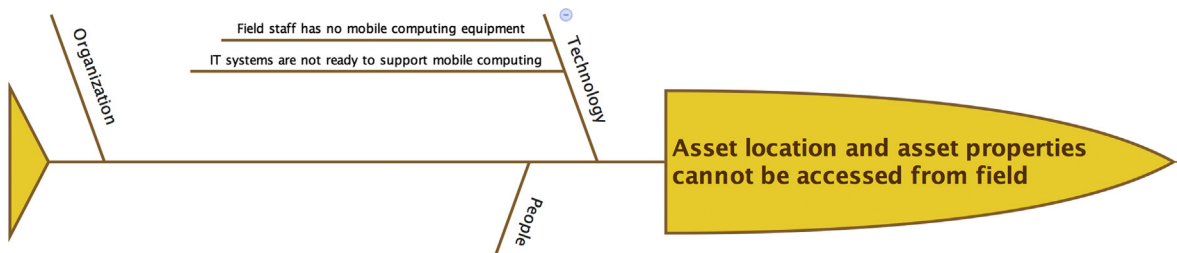


FIGURE 10.50

Root-cause analysis for information quality problems of asset location cannot be accessed from field and asset properties cannot be accessed from field.

Step C2: Identify and describe treatment options

Next, four potential information risk treatment options were identified, which are shown in Table 10.4. Besides the mobile GIS that was to be investigated as a potential investment as part of the goals of the TIRM process, a number of additional information risk treatments were identified.

Table 10.4 Identified Information Risk Treatments

ID	Treatment Name	Description	Information Quality Problems Tackled
T1	Enable mobile access to asset information	Purchase and deploy a new GIS that supports mobile devices. Migrate the data. Equip every field staff with a handheld device that gives access to the system.	All eight information quality problems shown in Table 10.2
T2	Create and enforce information policies	Formalize data capturing and updating processes and incorporate them as a formal part of the job requirements of the staff.	All eight information quality problems
T3	Educate the staff about the value of high-quality data	Increase the motivation of the staff to provide high-quality data.	All eight information quality problems
T4	Data definitions for asset fault data and known problems in the asset network	Develop clear data definitions and formats how asset fault data and known problems with assets should be captured in the future. Make changes in IT systems and educate staff about the new approaches.	Missing asset fault data and known problems are not up to date

Step C3: Estimate costs, benefits, and risks of treatment options

The TIRM steering council was aware that information quality improvement is a long-term investment; therefore, a decision was made to look at the costs, benefits, and risks over a ten-year horizon.

Step C3.1: Estimate costs of information risk treatment options

[Tables 10.5 to 10.8](#) show the estimated costs of each information risk treatment. The costs can be classified into four categories: software, hardware, external services, and human resource requirements. Moreover, there are some costs that occur only once at the very beginning of the investment. Other costs are incurred continuously year on year.

Table 10.5 Costs for Information Risk Treatment T1: Mobile GIS

Cost Category	Description	One-time Costs	Yearly Reoccurring Costs
Software	New GIS is necessary that supports mobile usage of the system	\$300,000	\$30,000
Hardware	Handheld devices for the staff are required	\$1,500,000	\$100,000
External services	Set up of new GIS and devices	\$2,250,000	\$50,000
Human resource requirements	Time of internal staff	\$450,000	\$250,000
Total Costs	\$9,800,000 over ten years	\$4,500,000	\$430,000

Table 10.6 Costs for Information Risk Treatment T2: Create and Enforce Information Policies

Cost Category	Description	One-time Costs	Yearly Reoccurring Costs
Software	Software tool for administrating information policies	\$250,000	\$30,000
Hardware	Server costs installation and maintenance	\$50,000	\$10,000
External services	Data governance consultants who help to set up information policies	\$450,000	—
Human resource requirements	New positions for managing information policies and software	\$30,000	\$150,000
Total Costs	\$2,680,000 over ten years	\$780,000	\$190,000

Table 10.7 Costs for Information Risk Treatment T3: Educate Staff about Value of High-quality Data

Cost Category	Description	One-time Costs	Yearly Reoccurring Costs
Software	Training software for data awareness	\$50,000	\$15,000
Hardware	Server costs installation and maintenance	\$30,000	\$7000
External services	External consultants who help to create training materials	\$80,000	—
Human resource requirements	Educator and course organizer costs	\$250,000	\$120,000
Total Costs	\$1,830,000 over ten years	\$410,000	\$142,000

Table 10.8 Costs for Information Risk Treatment T4: Data Definitions for Asset Fault Data and Known Problems in the Asset Network

Cost Category	Description	One-time Costs	Yearly Reoccurring Costs
Software	Software tool for administrating data definitions	\$200,000	\$30,000
Hardware	Server costs installation and maintenance	\$30,000	\$7000
External services	Data governance consultants who help to set up data definitions	\$250,000	—
Human resource requirements	New position for managing data definitions	\$10,000	\$70,000
Total Costs	\$1,560,000 over ten years	\$490,000	\$107,000

Step C3.2: Estimate benefits of information risk treatment options

Every information risk treatment will have an effect on some of the information quality problems, which will result in the reduction of the probability that an information quality problem occurs. To determine the benefits, the working group therefore estimated how much the probability of each

Table 10.9 Effect of Information Risk Treatments on Information Quality Problems

	T1: Enable Mobile Access to Asset Information	T2: Create and Enforce Information Policies	T3: Educate Staff about Value of High-quality Data	T4: Data Definitions for Asset Fault Data and Known Problems in the Asset Network
Inaccurate asset location	40%	15%	10%	0%
Missing asset fault data	15%	15%	15%	35%
Incomplete asset properties	40%	15%	10%	0%
Asset location cannot be accessed from field	100%	0%	0%	0%
Asset properties cannot be accessed from field	100%	0%	0%	0%
Known problems are not up to date	20%	15%	15%	40%
Inaccurate asset condition data	10%	15%	10%	0%
Some activities are not shown in system	15%	20%	15%	0%

information quality problem was likely to be reduced through each of the information risk treatments. The results are shown in [Table 10.9](#).

The TIRM process manager is aware that the benefits of the information risk treatments will only be achieved gradually over time, once the treatments are successfully implemented. Therefore, assumptions with regard to when the benefits will be realized were formulated in [Table 10.10](#). The working group has the expectation that after one year, one-third of the benefits will start to be realized. In years four to six, two-thirds of the benefits should be realized, while the full benefits will be only realized after year six.

Based on the total risk figures in [Table 10.1](#) and combining the expected effect of information risk treatments on information quality problems (see [Table 10.8](#)) together with the assumptions about benefits realization (see [Table 10.9](#)) allows the company to calculate the total benefits for each information risk treatment over the next ten years. [Tables 10.11 to 10.14](#) present the benefits for each information risk treatment T1 to T4 and each information quality problem and business objective. [Table 10.11](#) shows the benefits of enabling mobile access to asset information.

Table 10.10 Assumptions of Benefit Realization over Ten Years

Years	Percentage of Benefits Realized
Year 0	0%
Years 1–3	33%
Years 4–6	66%
Years 7–10	100%

Table 10.11 Benefits over Ten Years of Information Risk Treatment T1: Mobile GIS

T1: Mobile GIS Information Quality Problem	Cost Effectiveness	Service Reliability	Safety and Environment
Inaccurate asset location	\$3,941,919	3,198,439	6125
Missing asset fault data	\$1,571,603	75,222	470
Incomplete asset properties	\$936,192	1,939,438	0
Asset location cannot be accessed from field	\$2,595,159	1,504,440	15,044
Asset properties cannot be accessed from field	\$2,345,315	1,504,440	15,044
Known problems are not up to date	\$286,560	0	2866
Inaccurate asset condition data	\$458,496	22,925	143
Some activities are not shown in system	\$8060	0	766
Total Benefits over Ten Years	\$12,143,302	8,244,904	40,459

Table 10.12 Benefits over Ten Years of Information Risk Treatment T2: Create and Enforce Information Policies

T2: Create and Enforce Information Policies Information Quality Problem	Cost Effectiveness	Service Reliability	Safety and Environment
Inaccurate asset location	\$1,478,220	1,199,415	2297
Missing asset fault data	\$1,571,603	75,222	470
Incomplete asset properties	\$351,072	727,289	0
Asset location cannot be accessed from field	\$0	0	0
Asset properties cannot be accessed from field	\$0	0	0
Known problems are not up to date	\$214,920	0	2149
Inaccurate asset condition data	\$687,744	34,387	215
Some activities are not shown in system	\$10,746	0	1021
Total Benefits over Ten Years	\$4,314,304	2,036,313	6152

Table 10.12 shows the benefits of creating and enforcing standardized information policies.

Table 10.13 shows the benefits of educating the staff about the value of high-quality data.

Table 10.14 shows the benefits of having standardized data definitions for asset fault data and known problems in the asset network.

Step C3.3: Identify implementation risks for each information risk treatment option

For each information risk treatment option, there are a number of things that could go wrong during their implementation that would affect the assumptions about the costs and benefits of the treatment. A brainstorming session revealed a list of implementation risks, which are presented in Table 10.15.

Table 10.13 Benefits over Ten Years of Information Risk Treatment T3: Educate the Staff about Value of High-quality Data

T3: Educate Staff about Value of High-quality Data Information Quality Problem	Cost Effectiveness	Service Reliability	Safety and Environment
Inaccurate asset location	\$985,480	799,610	1531
Missing asset fault data	\$1,571,603	75,222	470
Incomplete asset properties	\$234,048	484,860	0
Asset location cannot be accessed from field	\$0	0	0
Asset properties cannot be accessed from field	\$0	0	0
Known problems are not up to date	\$214,920	0	2149
Inaccurate asset condition data	\$458,496	22,925	143
Some activities are not shown in system	\$8060	0	766
Total Benefits over Ten Years	\$3,472,606	1,382,616	5060

Table 10.14 Benefits over Ten Years of Information Risk Treatment T4: Data Definitions for Asset Fault Data and Known Problems in the Asset Network

T4: Data Definitions for Asset Fault Data and Known Problems in the Asset Network Information Quality Problem	Cost Effectiveness	Service Reliability	Safety and Environment
Inaccurate asset location	\$0	0	0
Missing asset fault data	\$3,667,073	175,518	1097
Incomplete asset properties	\$0	0	0
Asset location cannot be accessed from field	\$0	0	0
Asset properties cannot be accessed from field	\$0	0	0
Known problems are not up to date	\$573,120	0	5731
Inaccurate asset condition data	\$0	0	0
Some activities are not shown in system	\$0	0	0
Total Benefits over Ten Years	\$4,240,193	175,518	6828

Step C4: Evaluate and select treatment options

Once the information risk treatments and its costs, benefits, and risks have been identified, it is time for LightBulbEnergy Inc. to make a decision about which information risk treatments should be implemented. The TIRM steering council decided that the net present value (NPV) expected and the return on investment (ROI) should be calculated for each information risk treatment, which is shown in [Table 10.16](#).

The TIRM steering council also determines that a positive NPV and a ROI within eight years should be enough to justify the investment, as each information risk treatment would come with substantial additional benefits besides direct monetary values and would contribute toward the business goals regarding the objectives of service reliability and safety and environment, as presented in [Tables 10.11 to 10.14](#). The implementation risks are considered significant enough to be taken very seriously, but

Table 10.15 Implementation Risk Register for Information Risk Treatments

ID	Treatment Name	Implementation Risk Title	Implementation Risk Description
T1	Enable mobile access to asset information	Employees do not adopt new technology Technology will cost more than expected	The expected benefits cannot be realized because employees refuse to use the new technologies in the planned way. Complications regarding the software, databases, or hardware lead to higher implementation costs.
T2	Create and enforce information policies	No actual enforcement of information policies Employees do not conform with information policies	Leadership and management will not support the enforcement of information policies as required. Benefits of information risk treatment will not be achieved. Employees refuse to follow information policies and do not adapt the technology to track the compliance of information policies. Benefits of information risk treatment will not be achieved.
T3	Educate the staff about the value of high-quality data	Leadership does not lead by example	This information risk treatment effort could be jeopardized by the senior leadership if it does not show that it regards high-quality data as something very important to the business.
T4	Data definitions for asset fault data and known problems in the asset network	Data definitions are not consistently used	Data definitions are not consistently used throughout the organization, because (1) there is not enough appreciation of the value of consistent data, (2) the new data definitions are confusing or not clearly communicated, and (3) employees are not forced to use the new data definitions consistently. Benefits of information risk treatment would be not realized as expected.

Table 10.16 NPV and ROI for Information Risk Treatment Options

Information Risk Treatment	NPV (8.5% Internal Interest Rate)	ROI
T1: Enable mobile access to asset information	\$1,070,265	ROI after seven years
T2: Create and enforce information policies	\$909,742	ROI after six years
T3: Educate the staff about the value of high-quality data	\$999,127	ROI after five years
T4: Data definitions for asset fault data and known problems in the asset network	\$1,631,237	ROI after four years

they are not seen as a barrier preventing the company from going ahead with the investments. As all four information risk treatments comply with this criteria and the combination of these treatments is reasonable, it is decided to implement all four of them.

Step C5: Communicate the results to stakeholders

To engage all of the important stakeholders during implementation of the information risk treatments, the TIRM managing committee creates a list of stakeholder groups and creates tailored messages for each

Table 10.17 Communicating Results Tailored to Each Stakeholder Group

Stakeholder Group	Why are They Important?	Which Message Should be Sent Out?
Board members	They have a lot of immediate organizational power and can substantially support or hinder the implementation.	Implementing the information risk treatment measures helps deliver their business objectives.
Shareholders	Shareholders might not like the investments because it is bad for the short-term cash flow. They might force the board to abandon the investments.	Investment has positive NPV and would strengthen the company's position in the market.
Regulators	Investments need to be justified in front of regulators as they might impact the energy prices for consumers.	Implementing the information risk treatment measures improves service reliability and decreases prizes in the long term.
Field staff	Field staff has to adopt the practices and technologies to make the investments worthwhile.	Safety of field staff is improved. Helps field staff to deliver higher quality of work with less effort. Limits the amount of times work is done unnecessarily.
Middle management	Middle management is responsible for translating the goals of the executives into measurable outcomes.	Higher-quality asset information makes it easier for middle management to reach their business targets and control the work performed by field staff.
IT department	As many information risk treatments rely on new software tools, IT is a key player during implementation of the treatments.	Information risk treatments require a lot of support of IT and therefore strengthen the role of the IT department. IT staff can help to significantly contribute to achieve tangible business outcomes.

of them. The results from the information risk assessment and the selected information risk treatment options are communicated to each group, emphasizing different aspects of the results, as documented in [Table 10.17](#). The TIRM managing committee creates materials that can be handed to each of the stakeholder groups. The TIRM process sponsor is responsible for communicating the results to the other board members and for helping the CEO sell the investments to the shareholders. Moreover, Bill Mighty, the TIRM project manager, organizes a separate presentation with each of the remaining stakeholder groups.

After one month, the agreement of all the important stakeholder groups was obtained. Some of the stakeholders set particular conditions for the way in which the information risk treatments were to be implemented; this will be considered during the development of information risk treatment plans.

Step C6: Develop information risk treatment plans

Being sure of the support of the most important stakeholders and also receiving their input on how to actually implement the information risk treatments, the TIRM managing committee begins to plan the implementation of the selected information risk treatments. A summary of the information risk treatment plan is shown in [Figure 10.51](#).

Once all information risk treatment plans have been finalized, the TIRM steering council decides to take the next important step and start the actual implementation.

Implementation Plan

Completed by: Bill Mighty, TIRM Process Manager
Deadline: 01.04.15

T1	Enable mobile access to asset information	Completed - Due By	Responsible for implementation
1	Define requirements for mobile GIS	✓ 05.01.13	Head of Engineering and CIO
2	Evaluate offers by software providers	✓ 10.02.13	Head of Engineering and CIO
3	Decide on software provider	✓ 25.03.13	Head of Engineering and CIO
4	Prepare migration	✓ 30.06.13	CIO
5	Install software system and hardware	! 12.10.13	CIO
6	Migrate data	✗ 01.03.14	CIO
7	Test system	✗ 10.08.14	Head of Engineering and CIO
8	Trial handheld usage	✗ 19.10.14	Head of Engineering
9	Hand-off	✗ 13.01.15	Management board
10	Follow-up	✗ 01.04.15	TIRM managemeng committee

T2	Create and enforce information policies	Completed - Due By	Responsible for implementation
1	Define goals and scope of information policies	✓ 30.01.13	TIRM steering council
2	Create first draft of information policies	✓ 25.03.13	TIRM managing committee
3	Collect feedback on first draft	✓ 18.05.13	TIRM managing committee
4	Revise draft	! 04.10.13	TIRM managing committee
5	Create information materials	✗ 01.05.14	TIRM managing committee
6	Find effective ways to enforce information policies	✗ 19.10.14	TIRM managing committee
7	Hand-off	✗ 13.01.15	TIRM steering council
8	Follow-up	✗ 01.04.15	TIRM managing committee

T3	Educate the staff about value of high quality data	Completed - Due By	Responsible for implementation
1	Planning	✓ 01.01.13	TIRM managing committee
2	Preparation	! 10.07.13	TIRM managing committee
3	Trial training	! 20.09.13	TIRM managing committee
4	Delivery of training throughout enterprise	✗ 30.01.14	HR Function
5	Follow-up	✗ 01.10.14	TIRM managing committee

T4	Data definitions	Completed - Due By	Responsible for implementation
1	Planning	✓ 01.04.13	TIRM steering council
2	First draft of data definitions	✓ 17.06.13	Head of Engineering
3	Revised draft of data definitions	! 05.10.13	CIO
4	Trialling	✗ 02.04.14	CIO and Head of Engineering
5	Hand-off	✗ 23.08.14	TIRM steering council
6	Follow-up	✗ 01.12.14	TIRM managing committee

FIGURE 10.51

Summary implementation plan for information risk treatment options.

Step C7: Implement information risk treatment plans

Bill Mighty, as the TIRM process manager, is responsible for monitoring the progress of the implementation of the four information risk treatments (tracked in [Figure 10.51](#) using the status symbols). For each information risk treatment, a kickoff meeting takes place that includes all parties involved during the implementation. Every milestone shown in [Figure 10.51](#) is reviewed by the TIRM managing committee, which reports the current progress, quarterly, to the TIRM steering council. After one year, first problems arise, as the migration of data to the new mobile GIS turns out to be more difficult than expected. An external IT consultancy is hired to help with the migration. This increased the costs of the information risk treatment by \$225,000. The data migration can be completed with a one-month delay. The TIRM managing committee, to support the implementation, initiates active change management activities alongside the implementation of the information risk treatments. Luckily for LightBulbEnergy Inc., some two years later, all information risk treatments have been completed according to plan.

Step C8: Verify effectiveness of information risk treatments

The information risk treatments were implemented on time. But for the TIRM steering council, the more important question was, to what degree could the benefits have been realized? Therefore, after three, six, and ten years, the achievement of the benefits was monitored by updating the numbers for the frequency of the information quality problems and their overall impact from the information risk assessment stage. The actual realized benefits are compared to the planned benefits for each information risk treatment in [Tables 10.18 to 10.21](#).

Table 10.18 Planned versus Realized Benefits over Ten Years for Treatment T1

T1: Enable Mobile Access to Asset Information	Cost Effectiveness	Service Reliability	Safety and Environment
Planned benefits over ten years	\$12,500,000	8,600,904	30,900
Realized benefits over ten years	\$12,143,302	8,244,904	40,459
Difference	\$356,698	356,000	-9559

Table 10.19 Planned versus Realized Benefits over Ten Years for Treatment T2

T2: Create and Enforce Information Policies	Cost Effectiveness	Service Reliability	Safety and Environment
Planned benefits over ten years	\$2,614,700	1,900,600	7000
Realized benefits over ten years	\$4,314,304	2,036,313	6152
Difference	\$-1,699,604	-135,713	848

Table 10.20 Planned versus Realized Benefits over Ten Years for Treatment T3

T3: Educate the Staff about the Value of High-quality Data	Cost Effectiveness	Service Reliability	Safety and Environment
Realized benefits over ten years	\$3,700,300	1,382,605	4620
Planned benefits over ten years	\$3,472,606	1,382,616	5060
Difference	\$227,694	-11	-440

Table 10.21 Planned versus Realized Benefits over Ten Years for Treatment T4

T4: Data Definitions for Asset Fault Data and Known Problems in the Asset Network	Cost Effectiveness	Service Reliability	Safety and Environment
Realized benefits over ten years	\$3,850,000	172,557	7287
Planned benefits over ten years	\$4,240,193	175,518	6828
Difference	\$-390,193	-2961	459

The realized benefits indicate that the projected planned benefits were reasonably accurate.

SUMMARY

The TIRM steering council is fully satisfied with the results of the TIRM process and the realized benefits of the information risk treatment options. The head of engineering is now able to ensure that the business runs better, safer, and more efficiently. The CIO is also very pleased as she can show the contribution that the IT function is bringing to the business, in hard numbers. Learnings and problems encountered during the entire TIRM process have been captured and documented for the future. As the overall results are satisfactory, LightBulbEnergy Inc. decides to expand the scope of the TIRM process to other areas of the business. The TIRM process initially required an investment in resources to run the process that paid off relatively quickly. The assessment of information risks enabled LightBulbEnergy Inc. to focus the information quality improvement efforts on the things that really mattered for the company and also was able to convince other stakeholders in the company about the required information risk treatments. In the fictitious case of LightBulbEnergy Inc., which is very similar to the real-life case studies we have conducted in the past few years with companies in different industrial sectors, the investment in implementing the TIRM process was a real success story.

Risk Assessment Techniques for TIRM

WHAT YOU WILL LEARN IN THIS CHAPTER:

- The techniques available to carry out risk identification, risk analysis, and risk evaluation
- How to apply these techniques to manage information risks

INTRODUCTION

The core message of this book has been to emphasize and illustrate the use of risk as a means to quantify the value of good-quality business information. You might be wondering how the TIRM process can be integrated into the risk management techniques already in use in your organization. For instance, your executive team might be using risk matrices to identify critical business risks to help decide priorities and develop a business continuity plan. Or your product designers might be using failure mode and effects analysis or fault-tree analysis to identify different ways in which your product might fail, helping you to redesign the product with improved reliability. You might, therefore, be asking “Do I need to reinvent the wheel and start from scratch to apply the TIRM process?” The answer is “No, you don’t!” and this chapter is devoted to examining how the popular tools and techniques used for risk management in industry may be used in the context of information risk management.

It is critical to understand that if you wish to manage the information risks in your company, you must do so within your existing framework(s) of risk management (unless you do not have any, or feel current practices are not up to scratch). Most organizations where risk management is an embedded activity will be using a suite of tools and techniques to help them effectively identify, assess, analyze, and treat risks. This chapter is particularly useful to managers in those organizations who might want to integrate an instantiation of the TIRM process into the portfolio of current risk management activities and seek to use the tools and techniques already in use for information risk management.

The best place to start looking for risk management techniques is ISO.IEC 31010:2009—Risk Management—Risk Assessment Techniques. This standard provides a comprehensive list of techniques that can be used in the different stages of a business risk management process. On the one hand, some of these tools are qualitative (e.g., brainstorming, checklists) and have widespread use throughout the process. On the other hand, there are tools that are quantitative and specific that are used for particular activities within the risk management process (e.g., FMECA, RCA). Here, we describe a selection of these tools that are relevant to information risk management, and suggest ways to adapt/adopt the

tools to use within the TIRM process. A summary of the tools and techniques described in this chapter and their applicability across the different stages and steps in the TIRM process is shown in [Table 11.1](#).

BRAINSTORMING

“Let us have a brainstorming session to flesh this out!” This has become a very commonly (and often dreaded) phrase in the corporate world today. Brainstorming is probably one of the most frequently used group techniques in business life. The basic idea is to stimulate ideas by allowing thoughts to flow without imposing restrictions on the content of the thoughts. It encourages people to use imagination and to think “out of the box.” Brainstorming is particularly useful when not a lot of real data is available to support decision making, when problems and issues need to be identified, and when new solutions are required. The method is relatively easy to use and does not need a lot of time commitment.

How to use the technique

First of all, a team of people knowledgeable about the aspects that are going to be brainstormed should be assembled. For a successful/productive use of brainstorming, a facilitator (ideally independent—someone who is not affected by the outcomes and therefore unbiased) is needed. The facilitator guides the team throughout the method, and can use prompts and triggers to encourage and direct the thinking of the group. Moreover, a brainstorming process can incorporate rules and also set targets that the facilitator explains to the group at the very beginning of the process. The required (or desired) outputs of the session need to be defined so that there is a goal in mind for all the participants. All the points that are mentioned by the group should be put on a list, without filtering or evaluating the ideas or discussing their appropriateness. The emphasis should be on quantity rather than quality—the assumption here is that if you generate a sufficient number of solutions or ideas, there is bound to be at least one (hopefully a few more) very good ones! The brainstorming is completed when a set time runs out, there are no more new points to be added by the group, or the facilitator decides that the aims of the session have been achieved.

THE FACILITATOR

The key to successful brainstorming is the personality of the facilitator. A good facilitator exudes enthusiasm and invigorates the group, extracting the most out of the people and getting them to work together to produce creative output. The facilitator should be knowledgeable in the subject, but not necessarily an expert. Knowledge in the subject is essential for the facilitator to tease out initial

ideas from the group members, to ask follow-up questions encouraging the group to think the solutions through. The facilitator must also act as the “law enforcement officer, channeling the group’s energies and discussions in the right direction, stopping “illegal” conversations that digress from the key purpose, ensuring progress against time and required outcomes, while playing the “winning the hearts and minds” game.

You can use brainstorming for several steps in the TIRM process. In particular, brainstorming is useful for information risk identification in process steps B1 to B4 (see Chapter 7) and for information risk treatment identification in process steps C1 and C2. Brainstorming is obviously used if the task is carried out by a team of people, or if more than one person is affected by the problem being investigated.

Table 11.1 Summary of Techniques

Techniques	Stage A					Stage B									Stage C							
	A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	B6	B7	B8	B9	C1	C2	C3	C4	C5	C6	C7	C8
Brainstorming	X	X				X	X	X	X	X	X	X			X	X	X	X		X		
Interviews	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X		X	X	
Delphi method	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X		X	X	
Checklists	X	X	X	X	X	X	X	X	X	X	X				X	X						
Monte Carlo simulation						X	X	X	X	X	X	X		X								
Risk indices												X										
Scenario analysis						X	X	X	X	X	X	X										
FN curves												X		X								
SWIFT						X	X	X	X	X												
Root-cause analysis															X							
FMECA								X	X	X	X	X	X	X								
Fault-tree analysis									X	X	X	X	X	X	X							
Bow-tie diagrams								X	X	X	X	X	X	X	X	X	X	X				
Risk matrix														X				X				

Feasibility is also a criteria—it might just not be practical to bring the different people together to perform brainstorming, in which case, a structured/semi-structured interview with each person might be a more practical solution. For instance, when identifying information quality problems, the facilitator can use a list of critical information quality dimensions as a prompt. For information risk identification, the team should be knowledgeable about the business processes, how information is used, and the organization overall, whereas information risk treatment would require the team to be knowledgeable about different information risk treatment options and the information risks that should be treated.



EXAMPLE

An example of information risk in a management consulting company may arise when the customer data is not adequately shared across the enterprise. To identify innovative information risk treatment options as part of the TIRM process, a brainstorming session can be organized. The TIRM facilitator invites three general managers—a change management expert, a principal consultant, and a business process manager—who “feel the pain” of the problem and could create business solutions to the problem, and two people from the IT department who cover knowledge about potential IT solutions to treat the information risk. The TIRM facilitator prepares a stream of thoughts to start off the session. She explains the details of the information risks

discovered during the information risk assessment stage. Then, the brainstorming session commences by asking “What might be the reasons for the poor level of quality about our customer data, which is shared across the business?” to identify the causes of the information risk for process step C1. Each one of the participants adds, one by one, a further potential cause of the information risk to the list. At the end, the list is sorted according to the perceived importance of the participants. Then, the TIRM facilitator asks the group to come up with potential information risk treatment solutions that are first simply added to the list as part of process step C2. Afterwards, the group discusses each information risk treatment option.

SEMI-STRUCTURED AND STRUCTURED INTERVIEWS

Brainstorming is a group activity, whereas interviews are based on an individual. That said, you could use interviews with a number of different people (e.g., those who might have participated in a brainstorming session) when the group cannot be brought together due to some constraint such as clash of schedules. In some situations, a free flow of ideas is not appropriate and more structure is required. A facilitator who prompts questions to the interviewee is also needed. A semi-structured interview also follows a defined structure, but leaves room to discuss issues as they arise. Interviews are particularly useful to gather the opinions of different stakeholders. They are relatively time consuming for the facilitator, but allow more time to explore and discuss relevant issues in more depth. Semi-structured and structured interviews can be applied throughout all stages and steps of the TIRM process.

How to use the technique

Regardless of whether you are planning to conduct a structured or semi-structured interview, the key to success is *preparation*. The facilitator/interviewer must have a clear set of objective(s) for the interview. A structure or framework that breaks down the higher-level objectives into smaller objectives might help in deciding what to ask during the interview. The interview session needs to be carefully prepared by identifying a list of appropriate questions that are used to guide the interview. A question can be followed by alternative routes of a set of questions, depending on the answer given. For example, some

questions might be left out if an information resource is not used (e.g., How often is the information resource used? How is the information resource accessed?), or some questions could be added depending on the answer to the question. Questions should be open-ended to give the interviewee the possibility of expressing his or her opinion. Depending on the goal of the interview, the degree of flexibility of the interview should be determined. During the interview, the questions are read out by the facilitator to all of the interviewees and the answers are, if possible, recorded and transcribed, or at least documented by taking notes, and analyzed after the interview. Interviews of this nature can be done in a far more conversational manner, particularly if the interviewer is knowledgeable in the subject area concerned.



EXAMPLE

For understanding the external environment in step A2 (see Chapter 6), different stakeholders in the company are interviewed using a semi-structured questionnaire. The following questions are used by the facilitator to guide the interviewee through the interview:

1. What are important aspects of the social and cultural environment for the organization?
2. How would you define the political, legal, and regulatory environment?
3. Are there any important points regarding the financial environment?
4. How would you describe the technological environment?
5. How competitive would you say is the market that the company operates in?

The interview is conducted separately for each major business with one representative to get a unified view of the external environment.

DELPHI METHOD

Similar to brainstorming, the Delphi method requires a group of experts to provide their judgments, but unlike brainstorming, the input is collected independently from each expert who needs to be able to express their opinions clearly enough in written language. It is a good way to engage with key stakeholders and can help to avoid political and personal issues, as the experts provide their answers anonymously, which can bring out insights that would remain hidden otherwise. The method is relatively time consuming since it typically consists of several rounds, and it can sometimes be difficult to consolidate the results from different experts. The strength of this method is that it helps to build a consensus between different stakeholders. Like the previous two methods, you can apply the Delphi method throughout the TIRM process to obtain input from stakeholders.

To apply the Delphi method, a semi-structured questionnaire has to be developed. The questionnaire is aimed at capturing the judgments of the experts, which have to be tested. Then, a sufficient number of appropriate experts have to be identified. The experts will receive the questionnaire. Each expert answers the semi-structured questionnaire individually and anonymously in written form. The experts do not see the answers of other experts before they submit their own judgments. The responses are analyzed, combined, and sent back to the experts, accompanied by a second semi-structured questionnaire that aims to clarify disagreements. Afterwards, experts have the option to change their previous opinion as they see the summarized responses from the first round. The process is repeated until consensus among the experts is reached.

**EXAMPLE**

For step B5 of the TIRM process (see Chapter 7), stakeholders are asked to identify consequences of information quality problems that appear during information usage in a particular business process. A questionnaire with a list of previously determined information quality problems is sent to each business process representative, who are asked to think of potential direct and intermediate consequences of these problems. The results are gathered and analyzed by the TIRM process facilitators and then sent back to the business process representatives in a consolidated form (i.e., a list of direct and intermediate consequences for each information quality problem). Seeing the results from the other

stakeholders in an anonymous, summarized form allows them to rethink their own position, and if convenient, resubmit their view of the direct and intermediate consequences of the information quality problems, including a short textual description of their rationales behind these consequences. They can also state the disagreement with the summarized results and give an explanation as to why they disagree. This goes back to the TIRM facilitators who, again, analyze and consolidate the results and check if there is sufficient agreement among the business process representatives. If not, the process is repeated until there is sufficient agreement.

CHECKLISTS

Checklists help to make sure that all frequently occurring items are captured based on historical experiences within the organization or current best practices. Using checklists is a less creative process than brainstorming, interviews, and the Delphi method, but it has the advantage of making sure that all commonly found issues are covered.

First, the scope of the application of the checklist needs to be defined. This can be, for example, a particular step during the TIRM process. Then, an appropriate checklist needs to be created or identified. Checklists can be based on historical data from within or outside the organization. Finally, the checklist is applied by checking for each element on the list to see if it is actually occurring in practice.

A checklist is particularly useful for all steps that have to identify something, and where it is possible to find or create an appropriate checklist. This can include most process steps in stage A, process steps B1 to B6 during information risk identification, and to identify root causes of information quality problems in step C1 and during information risk treatment identification in step C2.

**EXAMPLE**

A fast-food chain applies the TIRM process and uses checklists at two points during the process. In step B3, a list of information quality dimensions is used to check if a problem occurs for each dimension. In step C1, a list

of frequently identified root causes of information quality problems is used that is based on a research report that analyzes information quality root causes in the fast-food industry.

MONTE CARLO SIMULATION

The Monte Carlo simulation is a method that allows you to obtain results when modeling the problem mathematically and/or finding that an analytical solution is too complex. Many software tools

are available to assist in helping build Monte Carlo simulations, such as the TIRM pilot software tool presented in Chapter 12.

The Monte Carlo simulation uses algorithms that can be run on any computer that creates a large amount of random numbers of a chosen distribution. First, the elements that should be represented and appropriate distributions are chosen for the simulation. Then, mathematical calculations are defined that should be executed on these elements and the number N of simulation runs has to be determined. The simulation generates N random numbers that follow the defined distribution for each of the elements and executes the calculations N times. The average, variance, and confidence intervals can be then calculated to summarize the results of these calculations.

The model, as presented in Chapter 5, is used to make the risk calculations for TIRM process step B9. The Monte Carlo simulation allows the collection of quantitative inputs for TIRM process steps B1 to B7 in the form of a probability distribution, instead of using exact values, which are often difficult to get. It makes it easier for experts to provide these quantitative inputs. For each input a statistical distribution is chosen. Commonly used distributions for Monte Carlo simulations are the uniform distribution, triangular distribution, and normal distribution. The uniform distribution assumes that values are equally distributed between a lower and upper boundary, which requires the expert to estimate a lower and upper boundary as the input. Additionally, the triangular distribution needs an estimate of the mode (i.e., the most likely value), therefore, values are assumed to be in the triangle between the lower and upper boundaries and the mode. The normal distribution also requires the estimation of a lower and upper value as the input, assuming that these are the points between which 95% of the values are supposed to lie and that values follow a normal distribution curve.



EXAMPLE

The business process representatives cannot give the exact value for the probability of an information quality problem in TIRM process step B3. But, they do note that the probability of the information quality problem is very likely to be between 30% and 50%. Therefore, 30% and 50% are used as

the parameters for the uniform distribution. At the end, in process step B9, risk totals are calculated using the Monte Carlo simulation, which simulates the results by using these parameters as the input.

RISK INDICES

Risk indices are a profiling methodology that quantify risk levels by examining a range of factors associated with an activity. Numeric scores are allocated to each factor; the resulting scores are a composite enabling comparisons to be made. Undertaken regularly, they can be used to measure changes in the levels of risk. The technique can be used in process step B7 in cases when it is not possible to estimate the likelihood and impact of a consequence.

A risk index is a semi-quantitative measure of risk that is calculated using an ordinal scale. An ordinal scale extends the information of a nominal scale to show order—that is, one unit has more of a certain characteristic than another unit. Scores are applied to each component (e.g., probability, exposure,

consequence) or for factors, which increase risk. The result is a composite (a series of numbers) that can be compared with other indices and enable ranking of the levels of different risks.

Developing an index is an iterative approach; a number of different systems for combining the scores may be required before the index is validated.



EXAMPLE

In applying the TIRM process at a telecommunications company, the impact of poor data quality regarding Internet usage (leading to incorrect billing) on customer satisfaction was found to be critical. However, customer satisfaction is often hard to measure in real terms (a company may choose to quantify customer satisfaction in terms of potential customers lost, but this often is very difficult to estimate). Therefore, risk indices are used instead, which are measured on a numeric scale from level 1 to 5. The company can

define clearly what each level means in quantitative terms in different dimensions. For instance, level 1 could mean a small impact on customer satisfaction, with no potential customers lost and no complaints registered. Level 2 could mean no potential customers lost, but complaints being registered by a minority of customers. This could progress all the way to level 5, which could mean a significant loss of customers and complaints being registered with the regulators, potentially leading to an investigation.

STRUCTURED “WHAT IF” TECHNIQUE

The structured “what if” technique (SWIFT) is a systematic team-oriented technique for risk identification. Originally developed for use in identifying hazards in chemical processing plants, SWIFT has since been adapted to fit many other situations. It utilizes a set of “prompt” words or phrases to help a team identify risks, such as “What if ...?” or “How could ...?” or “Has anyone ever ...?” It can be used to identify risks for further quantitative evaluation or alternatively provide a qualitative evaluation of risks and recommend action to manage those risks. This technique can be used for information risk identification as part of TIRM process steps B1 to B5. In particular, it can help identify low-probability, high-impact information risks.

There is no single standard approach to SWIFT. This is one of its benefits—it is flexible and can be adjusted to suit the particular circumstances. A suggested way forward is:

- A team is brought together under the direction of a facilitator. The team should comprise individuals who are experienced in the systems/processes being analyzed.
- Define and agree on the systems/processes and scope of the study.
- Discuss known risks and hazards, previous experience and incidents, known and existing controls and safeguards, and regulatory requirements and constraints.
- Discussion facilitated by using prompts “What if ...?” or “What would occur if ...?” or “Could someone or something ...?”
- Summarize the risks and consider what controls are in place.
- Confirm the description of the risk, and its causes, consequences, any safeguards, frequency, and consequences.
- Consider if the controls are effective; if not, consider risk treatment tasks and define potential controls. Further “What if ...?” questions are asked to identify other risks.

- The facilitator uses the prompts to monitor discussions and suggest additional issues and scenarios for discussion.
- Rank the actions created by prioritizing them; use a qualitative or semi-quantitative risk assessment method, taking into account the existing controls/safeguards and their effectiveness.



EXAMPLE

As part of identifying information quality problems in an airport, the TIRM facilitator may choose to use the SWIFT technique with representatives from the fuel company and the catering services organizations to identify information quality problems that can potentially occur due to lack of data sharing between the airport, airlines, and these companies. Examples of questions the facilitator may ask are:

- “What if a plane gets delayed? Do you get the information instantly from the airport management?”
- “What would occur if there is a delay in this information being shared?”
- “What if the delay results in gate changes? Does this information get fed to your systems?”
- What if the information is shared to your systems, but key decision makers are not notified of the changes instantaneously?”

SCENARIO ANALYSIS

Scenario analysis is a model for learning about the future. Scenarios are descriptive models that take into account uncertainties and factors that are complex and do not easily lend themselves to quantitative analysis. Scenario analysis can be used to identify risks by considering possible future developments and exploring their implications. Like the SWIFT technique, scenario analysis is particularly useful to identify information risks that are “out of the box,” or to analyze information risks in different ways to better understand their potential likelihood and impact. The technique can be applied during process steps B1 to B7.

Scenario analysis typically involves the following processes:

- Team formed of individuals who have an understanding of the issues and can think in “big picture” terms.
- Participants discuss how they see the future unfolding—consider micro and macro changes in society, technology, politics, governance, etc. These discussions, which reveal perceptions about trends and interrelationships, are often based on intuition and insights.
- The team identifies key internal and external uncertainties. The trends and uncertainties are combined into plausible yet wide-ranging scenarios.

To develop the scenarios, it may be useful to group the negative elements in one scenario and the positive elements in another one. Although these scenarios can sometimes be extreme, they offer a starting point for the development of different yet plausible scenarios.

One of the first organizations to use scenarios was Shell. Since the 1970s their “Shell Scenarios” have gained a global acceptance among governments, academia, and other businesses. Their approach starts with a series of interviews to capture intuition and insights. The process then moves

into a phase of workshops and research, in which ideas are gathered, shared, tested, and linked. The final step is crafting stories that embody the critical challenges that have emerged from the process.



EXAMPLE

The TIRM facilitator discusses with the business process representatives how particular information risks could evolve in the future, and when changes within the organizations or within the marketplace could happen. This enables the identification of potential future information quality problems in step B3 and potential future consequences as part of step B4 in such situations.

FN CURVES

FN curves or FN diagrams are used to graphically represent the likelihood and consequence of an undesirable event, which helps with evaluating information risks. The name FN curve comes from the use of the technique for accidents and catastrophes, where *F* means how frequently a consequence occurs, and *N* denotes the number of casualties or injuries that are affected by this particular consequence. The technique can be used for TIRM process step B7 during analysis of the impact and likelihood of consequences. The output helps to evaluate and compare information risks in step B9.

The frequency and impact of a consequence is plotted using an FN curve (Figure 11.1). Two lines are drawn that separate the curve into three distinct regions: (1) below the first line are the levels at which the risk is broadly acceptable, (2) below the second line are the risks that are tolerable and should be treated only if the benefits exceed the costs, and (3) above the second line the risks become intolerable and always have to be treated.

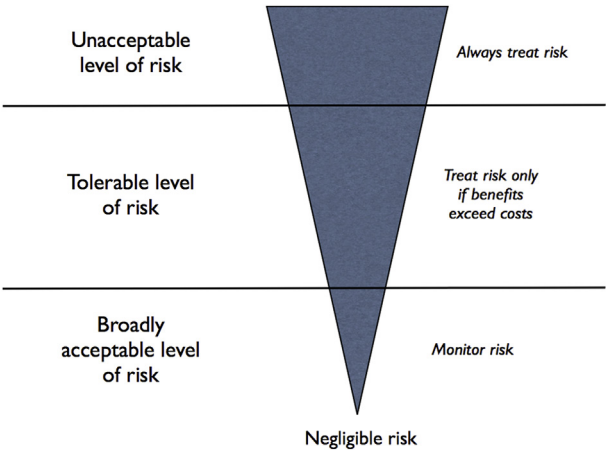


FIGURE 11.1
FN curve.



EXAMPLE

A public transport authority suffers from inaccurate signaling data, which occasionally leads to minor up to major train accidents if signaling equipment remains unmaintained or is not repaired when necessary. In process step B7, an FN

curve is drawn that shows the yearly expected frequency of accidents resulting from this information quality problem against the number of injuries that are caused by the accidents.

ROOT CAUSE ANALYSIS

Root-cause analysis (RCA) is a popular method of solving problems that tries to identify the failure mechanisms or the fundamental causes of faults or problems. In the context of TIRM, the RCA can be used to identify the factors that resulted in the nature, magnitude, location, and timing of information quality problems to identify what needs to be changed to prevent recurrence of similar problems. RCA can also be used to identify the lessons to be learned to promote the achievement of better information quality.

When investigating the root causes of information quality problems it is important to think of various categories of causes such as technology (including systems), organizational (including business processes, culture, rules, policies), and people (individual and team behavior, competency, skills, motivation, etc.).

RCA is primarily used as a reactive method of identifying causes, revealing the key problems with a view to solving them. In the context of TIRM, although RCA is performed retrospectively to understand the reasons for poor data quality (i.e., after the “disruptive event” has occurred), insights from the RCA will be useful as a proactive method to forecast or predict probable data quality problems in the future, and indeed to predict any residual data quality problems after improvement. In addition, investigating the root cause of a minor information risk could help prevent it from becoming a major one or a more frequent event.

The general procedure to conduct a RCA is as follows:

1. From the necessary business functions, build a team of experts who are qualified and motivated to explore the problem.
2. Define the information quality problem factually. Include the qualitative and quantitative attributes (properties) of the harmful outcomes. This usually includes specifying the natures of the consequence, the magnitudes, the locations (or business functions), and the timings of possible adverse events.
3. Gather data and corresponding evidence, classifying it along a timeline of events to the final failure or crisis. For every behavior, condition, action, and inaction specify in the timeline what should have been done when it differs from what was done. Typically, this would involve the development of an information flow map across the organization (where time and resources are limited, this analysis could be restricted to the business functions or information systems of interest).
4. Ask why and identify the causes associated with each step in the sequence toward the defined information quality problem. “Why” is taken to mean “What were the factors that directly resulted in the effect?”

5. Classify causes into causal factors that relate to an event in the sequence, and those root causes, which if eliminated, can be agreed to have interrupted that step of the sequence chain.
6. Identify all other harmful factors that have equal or better claim to be called root causes. If there are multiple root causes, which is often the case, reveal those clearly for later optimum selection.

A common obstacle is to identify the stopping condition to digging into the root cause. In the context of information risk analysis, we suggest that the analysis be stopped at the point beyond which the organization cannot exert meaningful and reasonable control over the events. For instance, the primary cause for improper data collection performed by an employee could be the lack of expertise in using data collection equipment. Going further (asking why there is a lack of expertise), the answer could move in the direction of personal issues such as financial constraints that resulted in the lack of education. However, such an analysis is meaningless, as the organization would be unable to rectify those issues (especially if they are past events). However, stopping the analysis at “lack of expertise” might be more meaningful, as the organization might be able to redress the problem by providing proper training to the employee, or indeed replacing the employee with someone with the necessary skills.



EXAMPLE

One of the popular techniques used for RCA is Ishikawa diagrams (also known as fishbone diagrams). An example of exploring the causes of a particular information quality problem using an Ishikawa diagram is shown in Figure 11.2. In this example, a company is faced with difficulties in accessing and interpreting data. The possible causes are

classified into three broad categories: technology-related causes, people-related causes, and organizational issues. Under technology, the key problem that was identified was the lack of proper functionality of the IT systems. This is further investigated to identify the reasons for the lack of functionality, as shown in the figure.

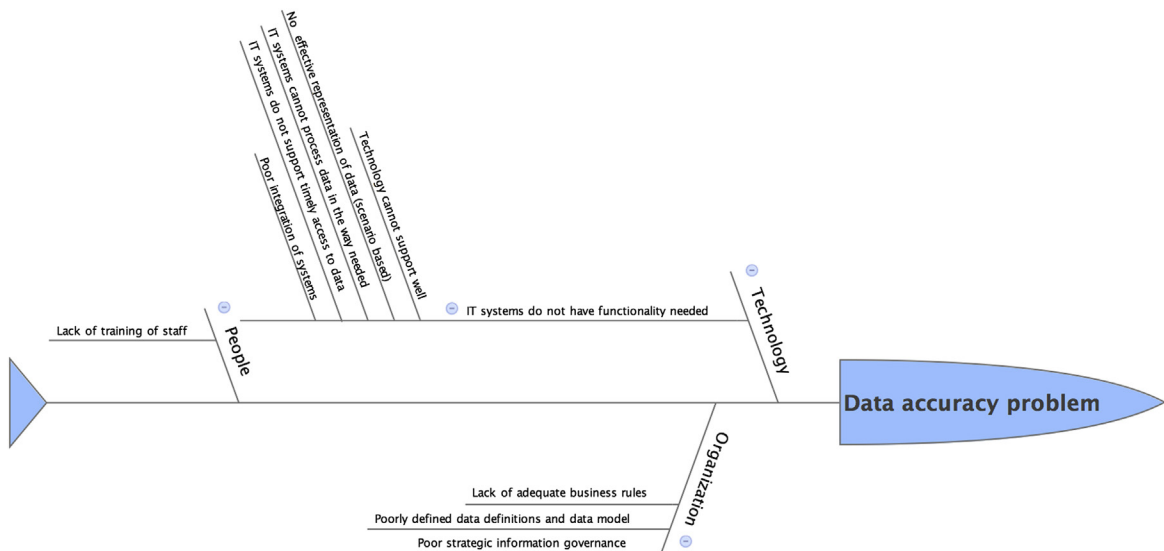


FIGURE 11.2

Ishikawa diagram example.

FAILURE MODE EFFECT AND CRITICALITY ANALYSIS

Failure mode effect criticality analysis (FMECA) is one of the first systematic techniques for risk analysis developed by reliability engineers in the 1940s to study problems that might arise from malfunctions of military systems. This is one of the most established and prevalent techniques in use in most industrial organizations, and the technique that has the most similarity with the TIRM risk assessment phase. There are a number of military and industry standards for FMECA, MIL-P-1629 being the earliest one, published by the U.S. military in 1949. CENELEC published the European standard IEC 60812 in 2006 on FMECA.

From a general perspective, FMECA involves reviewing the components, assemblies, and subsystems in, say, equipment to identify the different ways in which they can fail (failure modes), and their causes and effects. For each component, the failure modes (and their probability of occurrence) and their resulting effects (and the severity of the effects) on the rest of the system are recorded in a specific FMECA worksheet (Table 11.2).

FMECA in its raw form is a full inductive “forward-logic” analysis. However, the failure probability can only be estimated or reduced by understanding the failure mechanism. Therefore, it is important to include RCA along with the FMECA.

Considering that FMECA is predominantly used in the context of failure of physical systems (and in some cases failure of IT systems as well), in the context of TIRM, we need to draw some parallels between the typical terminology used in FMECA and information risks (which in other words is a result of an information system failure; see Table 11.3).

Table 11.2 FMECA Worksheet

Description of Unit			Description of Failure			Effect of Failure					
Ref No	Function	Operational Mode	Failure Mode	Failure Cause	Detection of Failure	On the Sub-system	On the System Function	Failure Rate	Severity	Risk Reduction Measures	Comments

Table 11.3 How to Use FMECA as Part of TIRM

FMECA Terminology	TIRM Equivalent
Failure	Poor information quality
Failure mode	Information quality problem/dimension
System	Information system
System function	Business function
Failure rate	Probability that information quality problem appears × probability that the information is used in a business task × the frequency of task execution
Severity	Impact of a consequence on business objectives
Risk reduction measures	Risk controls

Conducting a FMECA on information risks would involve the following steps:

1. Identify the different information quality problems that result from the information resource (step B3 in TIRM) (i.e., the failure modes).
2. Describe the effects of the information quality problem that can actually appear (step B4 in TIRM).
3. Describe how this information quality problem is detected (if it can be detected).
4. Estimate the inherent provisions that are to be provided in the design of the information system or the management system to compensate for these problems (step B6 in TIRM).
5. Describe the criticality of these failure modes in terms of the probability of the effect and the consequence of the effects (step B7 in TIRM).



EXAMPLE

An example of a FMECA worksheet that can be used for information risk assessment is shown in [Table 11.4](#).

FAULT-TREE ANALYSIS

Fault-tree analysis (FTA) is a deductive technique mainly used in safety and reliability engineering for analyzing failures. FTA is applicable in scenarios where an undesired state of a system can be examined using Boolean logic to combine a series of causes. It is used to build a logical understanding of the conditions that cause system failures. Consequently, FTA can be applied for analyzing the reasons for information quality problems in a logical and structured manner. Moreover, due to the mathematical nature of Boolean logic used in FTA, this technique can also be used to calculate the likelihood of information quality problems and their consequences. FTA is described in several industry and government standards, including the European standard IEC 61025. Similar to RCA, this technique can be used in the information risk treatment phase for analyzing the causes of information quality problems (TIRM process step C1). Moreover, conducting FTA early on in the TIRM process (i.e., not doing it as part of stage C, but within stage B when assessing the information risks) will help in quantifying the probability and the impact of information quality problems.

In the context of TIRM, FTA can be used for:

- Identifying the reasons for information quality problems.
- Identifying the pathways from business impact to information quality problems (backward analysis).
- Quantifying the probability of information quality problems.
- Quantifying the probability of business impacts.

The “undesired effect” is taken as the root or top event of the tree of logic. The undesired effect could either be taken as the business impact or the information quality problem. Traditionally in FTA, only one undesired effect is considered at a time, therefore, there will only be one top event. However, when using FTA for information risk analysis, multiple undesired effects need to be considered in a single analysis since there could be many interdependencies between information quality problems and business impact (e.g., one problem affecting multiple business objectives).

Table 11.4 FMECA Worksheet Example

Context			Description of the IQ problem			Consequence chain		Information Risk analysis			
Ref No.	Decision	Information	Information Quality Problem	Cause(s) of the IQ Problem	Possibility of Detection of Poor IQ	Direct Consequence	Intermediate Consequences	Probability of Risk Occurrence	Impact on Business Objectives	Risk Controls in Place	Comments

Once the undesired effect is identified, each situation that could cause the effect is added to the tree as a series of logic expressions. Such trees are also known as fault-tree diagrams. Once each node in the tree is labeled with probabilities, the resultant probabilities of the undesired effect can be then computed. It is possible to use software tools to make the calculations.



EXAMPLE

Figure 11.3 shows an example of a fault-tree diagram exploring the possible causes of data unavailability and unusability.

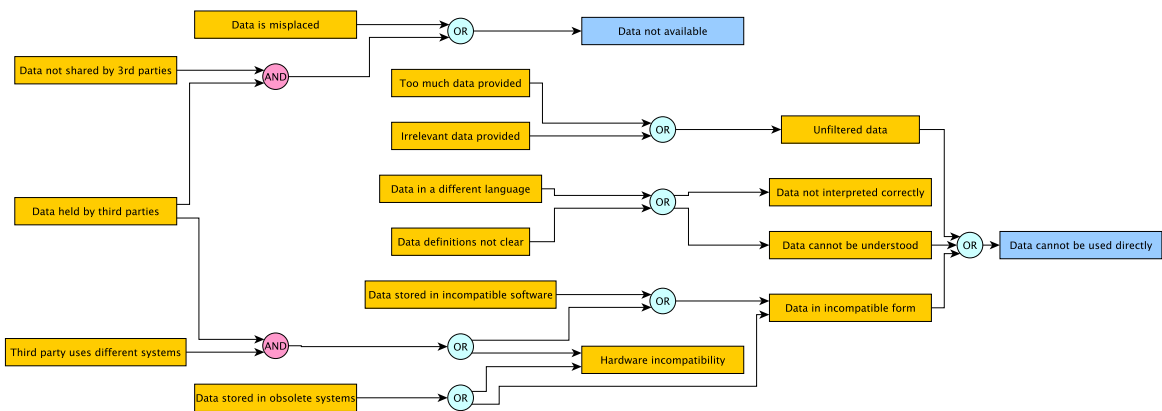


FIGURE 11.3
Fault-tree analysis.

BOW-TIE DIAGRAMS

Bow-tie diagrams (Figure 11.4) are a risk evaluation technique that can be used to analyze and demonstrate causal relationships between a sequence of causes of an undesired event, and the sequence of outcomes of the undesired event. For example, the sequence of causes could be the improper training of personnel leading to improper inspection of sensors leading to faulty sensors; an undesired event could be data inaccuracy; and the sequence of outcomes of the undesired event could be the wrong maintenance decision leading to machine failure leading to production loss leading to drop in profit.

In addition to the causal relationships, bow-tie analysis also identifies the possible control measures that can be put in place to reduce or eliminate the likelihood of the undesired event (also known as preventive controls), and also to reduce the impact of the undesired event (also known as recovery preparedness).

Essentially, the key steps in performing a bow-tie analysis are:

1. Establish the links between causes and the information quality problem (e.g., using RCA).
2. Establish the links between the information quality problem and its consequences (e.g., using FMEA).

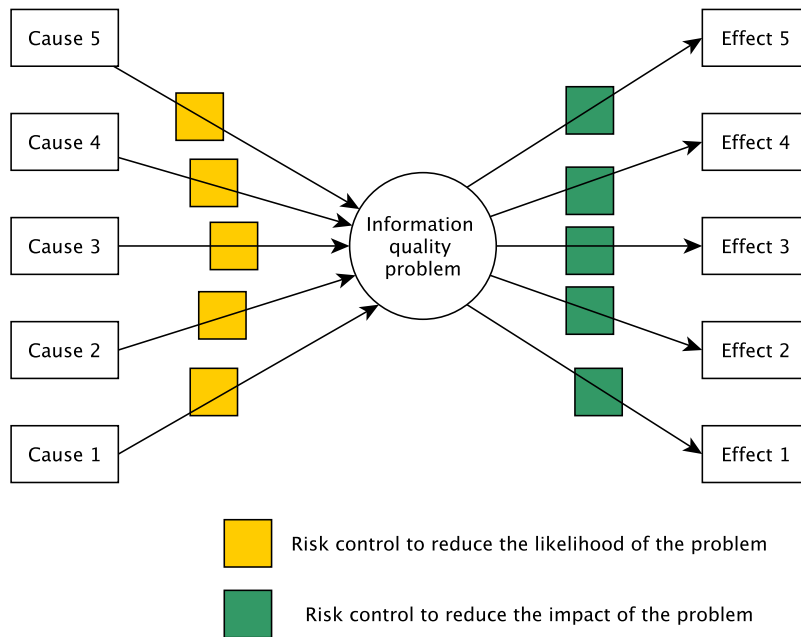


FIGURE 11.4
Bow-tie diagram.

3. Identify existing risk controls in place on both sides of the bow tie.
4. Identify risk treatment solutions to reduce the risk (either the likelihood or the impact).

In the context of TIRM, this technique is applicable for analyzing information risks as well as identifying information risk treatment methods. Specifically, the right side of the bow-tie diagram is useful for identifying and visualizing the chain of consequences arising from information quality problems right up to the impact on business objectives. The left side of the bow-tie diagram is useful for identifying and visualizing the different causes of the information quality problem and existing controls to manage the risk. Once the bow-tie diagram is completed, the analyst can examine both sides of the bow tie to identify possible treatment options and evaluate them.

RISK MATRIX

Risk is defined as the product of the probability (or frequency) and the impact (or severity) of the consequence of an undesired event. A risk matrix is a graphical technique used during risk assessment to explicitly represent different levels of risks as the product of probability and severity of the consequences of the undesired event on a numeric/verbal scale. [Table 11.5](#) shows examples of numeric and verbal scales.

Once these scales are identified, it is easy to come up with a numeric matrix, where one can highlight the risk “zones” in terms of their level of acceptability; see the example in [Figure 11.5](#).

Table 11.5 Risk Matrix

Severity			Frequency		
Verbal	Numeric	Description	Verbal	Numeric	Description
Catastrophic	5	Likely to result in death	Frequent	5	Hazard likely to occur
Critical	4	Potential for severe injury	Probable	4	Hazard will be experienced
Moderate	3	Potential for moderate injury	Occasional	3	Hazard may occur
Minor	2	Potential for minor injury	Remote	2	Hazard unlikely to occur
Negligible	1	No significant risk of injury	Improbable	1	Hazard highly unlikely to occur

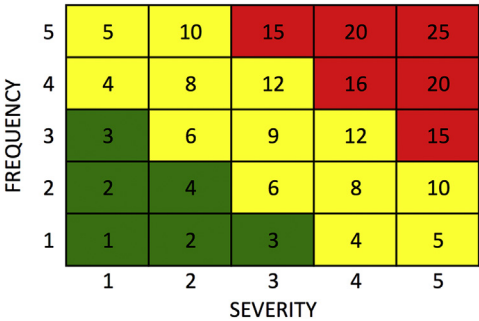


FIGURE 11.5
Risk matrix.

In the risk matrix shown in the figure, we have a low-risk (acceptable risk, no action needed) grey (green in online version) zone and a high-risk (unacceptable risk, immediate action required) very dark grey (red in online version) zone. Evidently, there is a rather large light grey (yellow in online version) zone, where the risk tolerance is unclear. For risks that fall into this zone, further analysis might be required to determine what action (if any) needs to be taken. The highly visual nature of this technique makes it very suitable for presentation of risks to executive decision makers and to aid business decision making.

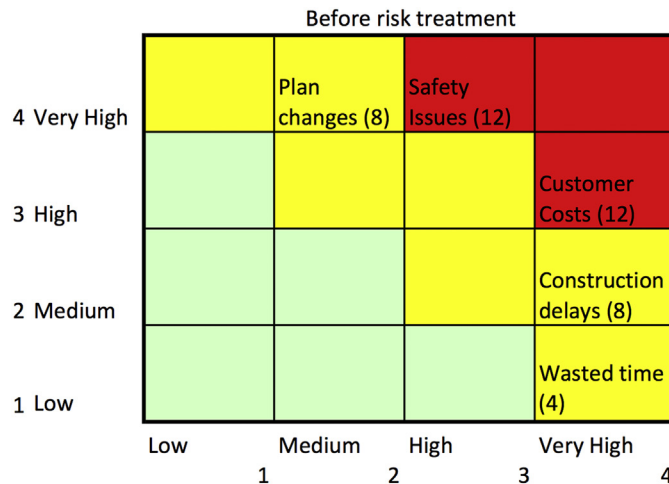
Although risk matrices are very popular in many industries, the technique is often criticized for its poor resolution and ambiguity. However, these shortcomings are mostly associated with particular implementations of the technique instead of being a problem with the technique itself.

The key starting point in the development of an information risk matrix is to identify the organizational objectives, measurement units, and risk criteria (step A4). For instance, a company may identify different business objectives to be considered for the analysis, develop numeric scales for each objective, and assign risk tolerance levels as shown in Table 11.6.

After performing information risk assessment steps B1 to B8, the risk matrix can be used to present a one-shot quick overview of various risks and help in ranking. An example of such a risk matrix is shown in Figure 11.6, where a scale of 1 to 4 is applied to the different consequences arising from an inaccurate asset register.

Table 11.6 Risk Criteria

	Costs (CAPEX+OPEX)	Customer Satisfaction	Health and Safety	Employee Satisfaction	Society and Environment	Action Needed?
Very low	> 0	> 0	> 0	> 0	> 0	No action
Low	> 50,000	> 0.1	> 100	> 1000	> 1000	Action only in special cases
Medium	> 100,000	> 0.3	> 400	> 2000	> 2000	Action potentially
High	> 250,000	> 0.6	> 1000	> 5000	> 5000	Action preferable
Very high	> 750,000	> 1	> 2000	> 7500	> 7500	Not tolerable

**FIGURE 11.6**

Risk matrix example.

Clearly, the safety issues and customer costs lie in the high-risk category, and therefore this information quality problem is a good candidate for further investigation and rectification.

SUMMARY

The message of this chapter is clear and simple: there is no need to reinvent the wheel. The critical thing is to effectively embed TIRM within the risk management practices in the organization. Since TIRM is derived and based on fundamental risk management theory and practice, it is quite straightforward to adapt and adopt existing tools and techniques to information risk management. This chapter provides a glimpse of how this can be achieved using a few examples found in risk management practice. This by no means is an exhaustive list of tools. By careful understanding of the similarities and differences between information risks and other types of risks, other tools can also be used in appropriate areas within TIRM.

Software Tools: Automated Methods for TIRM

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to automate some of the TIRM process stages
- What information management tools and technologies are currently available for detecting and mitigating information risks

INTRODUCTION

The vast amount of information that an organization collects on an almost daily basis offers a wide range of new opportunities that can be leveraged to increase an organization's decision-making capability. The automation of business processes has led to a vast increase in the amount of information captured and used throughout organizations. This already immeasurable amount of information from within the various departments and business units is being augmented with rich data sets sourced externally from resources as diverse as social networks, publicly available government data, and partner organizations. For example, smartphones have the capability to connect to the web and facilitate the upload of information to core organizational information systems about events as they happen. Wireless sensors provide continuous streams of operational data, and integration technologies like virtualization can extract and present data from millions of websites, including social networks, directly to the operational staff.

The challenge posed by the availability of all of this data is the speed at which organizations need to operate to make effective use of it. Automating the management of this data in today's overflowing and information-rich environment is critical. Automation within the TIRM process is no exception. Leading managers must consider the ways in which automation of the relevant steps in the TIRM process can save time and ensure an accurate output.

There are a number of available software tools that can be used to support the automation of various TIRM steps. The following sections describe how the steps of understanding the information environment, identifying the information quality problems during task execution, and the information risk assessment stage of the TIRM process can be supported with such tools. Automating the TIRM steps is only one part of the story. The other part is concerned with the identification of technologies that need to be applied to help mitigate the risks that are posed by information errors. The final section of this chapter, therefore, provides two example cases of information risks and how these can be mitigated with the aid of automated information management technologies and their associated architectures.

AUTOMATING THE UNDERSTANDING THE INFORMATION ENVIRONMENT STEP

Investigating the information environment in the TIRM process involves creating a register of the information resources that are in the scope of the project under consideration. These could be resources such as databases, electronic or paper-based documents, ERP systems, spreadsheets, etc. With this as a basis, it is necessary to identify the type of information in each system, categories how this information flows within and between these systems, and document any known quality issues.

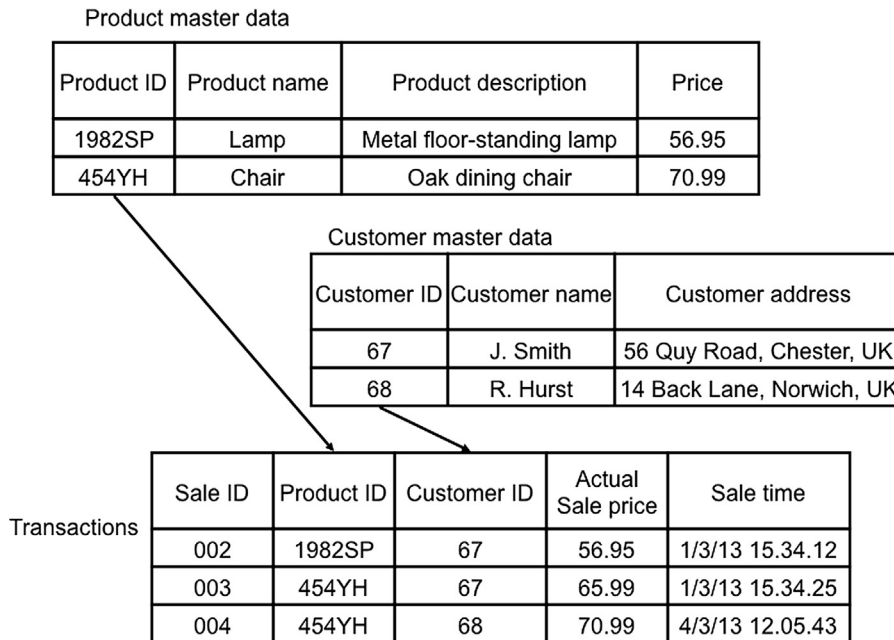
First, the type of information is an important concept to capture, because it not only dictates how it is to be used, but it also indicates the types of problems that are likely to occur, as well as the types of automated information management technologies that will be appropriate to mitigate these problems. There are four main categories of organizational information: master data, transactional data, reference data, and metadata. The first two categories are described together because of their linkages.

Master and transactional data

Transactional data relates to the transactions of the organization and includes data that is captured, for example, when a product is sold or purchased. Master data is referred to in different transactions, and examples are customer, product, or supplier data. Generally, master data does not change and does not need to be created with every transaction. For example, if one customer purchases multiple products at different times, a transaction record needs to be created for each sale, but the data about the customer stays the same. [Figure 12.1](#) shows how master data forms part of a transactional record. In this case, when the lamp and chair products are sold, the transaction references the relevant product IDs and customer IDs. The product and customer records, if they already exist, do not need to be recreated or modified for this new transaction. The other data in the transaction, such as the unique identifier for the transaction (i.e., sale ID) and sale time do, however, need to change. Transaction data is therefore typically more volatile than master data as it is created and changes more frequently. Note that this simple example shows the actual sale price in the transaction and price of the product in the master data. There are different ways to model this, but the example shows that the actual price can change depending on the transaction and it may only be calculated from the product price in the master data (after including discounts, etc.). Transaction 003 in [Figure 12.1](#) shows that a discount has been applied to the retail price.

Another property of master data is that it is often shared and used by different business units. For example, a customer record will be used by marketing as well as sales. Problems arise when one business unit updates the master record and does not inform the other business unit. For example, the marketing department could update the address of a customer and, if they do not inform the sales department, orders could be sent to an out-of-date address.

Although these are the general properties of master and transactional data, there are occasions when these data types behave differently and, thus, this distinction becomes blurred. For example, master data can also appear to be transactional when changes to a supplier address, for instance, are not overwritten in a record, but instead a new record is created. An organization may choose to retain all previous addresses of a supplier, especially if they wish to analyze a supplier's movement. It is worth

**FIGURE 12.1**

Master and transactional data.

paying attention to cases such as these, because it may be better to apply transactional solutions to the problems in this data type so that it is managed correctly.

When considering the information environment for the TIRM process, transactional data is often found in data warehouses and point-of-sale systems where the transactions occur. Master data is often found in customer relationship management (CRM) software, product life-cycle management (PLM) software, and supplier relationship management (SRM) systems. However, it can also be identified by tracking back from transactional records that refer to customers, products, suppliers, etc. If you find that the only source of the master data is stored in the transactional record, then this is a prime place to look for information risks that may arise from faulty master data.

**ACTION TIP**

Do not always assume that master data needs to be treated with only master data-related solutions, especially if the master data behaves like transactional data.

**ACTION TIP**

If you find that the only source of the master data is stored in the transactional record, then this is a prime place to look for information risks that may arise from faulty master data.

Reference data

One common problem in business systems is that information is not always entered into the systems consistently. For example, in a supplier table, a field such as “country” could contain many inconsistent

Table 12.1 Reference Data for Country Codes	
Country Code	Country Name
GB	United Kingdom of Great Britain and Northern Ireland
DE	Germany

values for different suppliers. The problem is that there are many ways of referring to one country. For example, some records could refer to the United Kingdom as GB, UK, Great Britain, or United Kingdom. Reference data is used to address this problem by providing a global reference of standardized and allowable values. Reference data can be best thought of as *clarification data* because, as the name suggests, it clarifies and expands on the data in transactional and master records. For the supplier country problem, reference data would define the allowable domain of values for each country and would give a clear indication of the real-world entity that each value refers to (Table 12.1 is an example). Reference data is often used in instances where there are codes (such as country codes) or numeric codes that help to reduce storage requirements and make expanded concepts more concise. When arbitrary numeric codes are used, reference data is essential to define the real meaning.



IMPORTANT

Reference data can be best thought of as *clarification data* because, as the name suggests, it clarifies and expands on the data in transactional and master records.

Reference data may be managed internally or could reference externally managed codes. For example, the International Organization of Standards (ISO) has a standard that defines country codes (ISO 3166-1) that could be reused in different organizational information systems. Using external codes relieves an organization of the job of managing them, but the disadvantage is that there will be less control over managing changes to the values. It is worth noting that reference data changes infrequently in contrast to master and transactional data.

When investigating the information environment for the TIRM process, reference data can be found in the actual databases as lookup tables. Some database vendors provide options to specify domains of values (or lookup values) within the database management software, and database administrators will know where to find these values. Also, ask the users about where they are constrained (e.g., dropdown lists) when entering values into fields in the applications they use; this can indicate the use of reference data. Note that if you cannot find the reference data, at this stage it would be unwise to start to introduce reference data in places where you would expect to find it. Use data profiling (described later) as a final check to determine if there is a need for reference data in these places.

It is possible to partially automate the discovery and validation of reference data. Column analysis, which is one of the automated methods in data profiling tools, can be applied to identify what values appear for a particular field. Domain analysis can be used to check whether the values in

a field match those in the domain. Another option is to cross-check the values used in different databases to see if consistent codes are used; again data profiling tools can be used to support this. Both column and domain analysis are described later in this chapter.



ACTION TIP

If you cannot find the reference data, use data profiling column analysis to identify areas where it may need to be introduced.

Metadata

Metadata is broadly defined as data that describes other data. There are two clear categories of metadata that are important to distinguish: metadata about the operational (actual) data in the system (sometimes referred to as business metadata) and metadata about the system structure (also referred to as technical metadata). Metadata about the actual data in the system includes items such as when and who created or updated the data; how the data was calculated, aggregated, or filtered; and what the quality of the data is. The metadata about the system includes the data model—that is, the details of the structures inside databases and data types used.

It is important to make the distinction between these categories of metadata because of the way in which they are used. The metadata about the actual data is used operationally by the users of an organization's information system in their daily work. For example, if purchases above a certain amount need to be authorized before they are sent out, the operational staff need to know how the final amount is calculated (e.g., is it the gross amount or net amount, and does it include shipping) before they can assess whether it is above a certain threshold and require authorization.

The structural metadata is not needed for operational tasks but is closer to the design of the system. Clearly, the system needs to be well designed and suitable for the users for the operational work to be successful, but the structural metadata is not needed directly for operational purposes. Database administrators will be able to identify and report what the structural metadata is.

When data needs to be transferred from one system to another (e.g., to a data warehouse), then extract, transform, and load (ETL) operations are used for this purpose. The extract step extracts the data from the source's system. The transform step is needed to convert the data into a form that is suitable for the target system (because the source and target systems will often have significant variations). Finally, the load step is used to push the data into the target system. Knowing both the operational and structural metadata is essential if ETL is to be a success. For instance, if the field names between the source and target databases are different, then the mapping between the different fields needs to be specified in the transform step so that the data goes to the correct place. Note that two databases may have the same fields (with the same names) but have different meanings—the field "total" could be in two systems, but could mean the gross total in one system and the net total in another system. The data about the operational data is, therefore, also needed to determine how the actual totals have been calculated and whether they are semantically equivalent or not.

The fact that data may have been moved from one system to another via ETL (or other data synchronization techniques) is an important piece of operational metadata to capture: it informs the users of the reliability of the data (i.e., that it has probably been subject to an automated transformation that may not have been verified). This is also referred to as data lineage, which defines where and how

information was created—where it flows to, and how it was transformed as it is passed from system to system within the organization.

When understanding the information environment for the TIRM process, identify the two types of metadata that relate to the systems of interest. For the structural metadata, speak to the IT personnel such as database administrators. For the operational metadata, first speak to the users and then the IT personnel. Both of these groups of people should know what is really happening to the data, and their thoughts should be aligned. If not, then this is a prime place that could be causing information risks. In particular, as shown in the previous example, there could be situations where purchases are not being correctly authorized before being sent out, through misunderstandings in the data and the ways it is transformed.

Automated information flow discovery

Information flow refers to the path the information takes while it is being used for a business process. Information may be created in one system, then transferred to another system, modified in that system, then merged with other data, and so on. Be cognizant that the flow of information may be more complex than the business process because there may be multiple information systems and multiple actors using the information in a single business step.



ATTENTION

The flow of information may be more complex than the business process because there may be multiple information systems and multiple actors using the information in a single business step.

New research has emerged that shows a promising approach to help automate the discovery of information flow ([Gao et al., 2010](#)). Even more than just automation, it aims to discover what is really happening to the data, and not what users say is happening to it (which may not always be correct). The approach relies on using database log files to see when, what, and where data is being created, read, updated, and deleted. However, this approach is still in the research phase, and therefore, there are no current commercial tools available to support this. It may not be a practical solution for many organizations. That said, organizations with the relevant capabilities in place might want to investigate this further.

The idea of the research is to inspect the information system logs and observe when a data item was created, read, updated, and deleted, and then piece these actions together to gain an overall picture of what is happening to the data. For example, a simple insert statement into a database could indicate that a new product has been created, a new customer has been registered, or a request to purchase a new product has been made. Insert statements are good candidates for indicating the start of a process or when data has been transferred to another system. Also, whether the insert statements are for transactional data or for master data, they can help with the overall understanding of the process.

As an example of this approach, you can see how the following statements, recorded in different system log files, map to the business process in [Figure 12.2](#).

1. [1023] (02/06 09:14:22:57.260): Performing INSERT INTO partRequests (partNumber, requestor, supplierName, totalNet, ...) VALUES (...)
2. [1024] (02/06 09:14:25:34.420): Performing SELECT partNumber, requestor, supplierName, totalNet FROM partRequests WHERE totalNet>100
3. [25423] (02/06 09:14:26:15.130): Performing INSERT INTO requestReviews (requestID, partNumber, requestor, supplierName, totalNet) VALUES (<values from query 2>)
4. [25425] (02/06 09:14:45:12.543): Performing UPDATE requestReviews SET approved=true WHERE requestID="43"
5. [25426] (02/06 09:15:00:05.103): Performing SELECT partNumber, requestor, supplierName, totalNet FROM requestReviews WHERE approved=true
6. [562983] (02/06 09:15:01:14.330): Performing INSERT INTO orders (POnumber, POdate, supplierName, totalNet, ...) VALUES (<values from query 5>))

Initially, the part request (in this example this refers to an engineering part that the organization is procuring) is created by inserting a record into the `partRequests` database (query 1). Queries 2 and 3 show an ETL process where data is taken from the `partRequests` table and entered into the `requestReviews` table in another data source. In addition, it is possible to observe a business rule that determines what data is to be transferred in query 2: when the `totalNet` value is greater than 100, the data is moved to a system that requires the purchase to be approved. By observing other queries that select this data, it would be possible to determine in what other conditions the data is transferred to other systems. For example, one may observe that all part requests that have a `totalNet` below 100 may go straight to the purchase ordering system (see the dashed line in [Figure 12.2](#)). The update statement in query 4 shows that the user has clarified part of the data by approving the part request. Note that there would most likely be a select statement before the update statement, but it is not necessary to consider this in this specific example. In general, there will be many log file entries that are irrelevant and do not help the process of determining information flow. The challenge is, therefore, to extract the entries that provide the most valuable information.

Queries 5 and 6 show another ETL process that moves the data to the purchase ordering system and creates the purchase order for the part. After this, one would expect to find other log file entries that show the purchase order being sent out, especially in the case where it is transferred electronically.

Note that the timestamps are needed to determine the correct sequence of actions, and it is often the case that timestamps from multiple systems will not be in synchronization. In this case, it is necessary

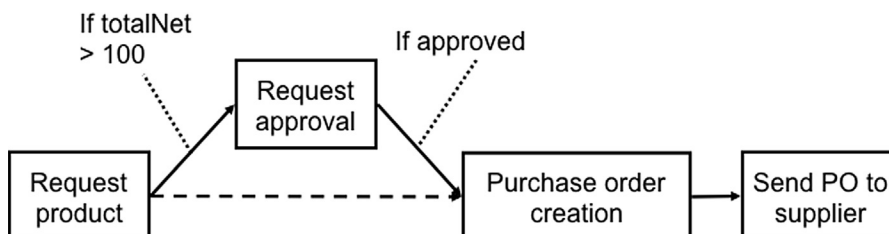


FIGURE 12.2

An example of information flow.

to determine the offset of the timestamps (i.e., the difference in time) between each system and use this to determine what actions occur simultaneously.

Bear in mind that in simple cases, it is often faster to speak to the people involved with the business process, but in more complex scenarios where the data is integrated from multiple systems and it is not easy to establish what happens in every case, log files can provide an invaluable source of reference for what is really happening.

Furthermore, if common groups of operations can be used to determine an information flow scenario, such as an ETL process or business rule being applied, then software to detect and extract these patterns can be developed to automate the process. In this example, there are two ETL processes and these were indicated by a select action from one database and an insert action into another, where the data is similar and the timestamps are close. A rule that governs where the data moves can also be observed in the `WHERE` clause of query 2.

When investigating the information environment for the TIRM process, use your knowledge of transactional data, master data, reference data, and metadata to help you categorize and understand what is really happening to the data and why it is occurring.

IDENTIFY INFORMATION QUALITY PROBLEMS DURING TASK EXECUTION

As part of TIRM, after examining the information resources that are used within the different business processes, it is necessary to identify the actual information quality problems within these resources. The vast quantity of data in many business information systems makes this task extremely challenging and infeasible to conduct manually in many cases. Tools that can automate the discovery of data characteristics within large data sets have already been developed, and these characteristics can give a good indication about whether the data set contains information quality problems. Data profiling tools, the commonly used name for these types of tools, can be used to build a report about the data that shows very detailed statistics about the characteristics of the data.

The limitation of data profiling tools, however, is that, when directed to a particular data set, they do not directly report all the information quality problems in a way that managers can easily digest and understand. Instead, they operate the other way around: an analyst is needed to specify what statistic needs to be known about the data, and the tool will calculate this statistic based on the data set. Therefore, the tools do not directly report what data is inaccurate. The analysts, therefore, need to know what they are looking for, and should carefully report their statistics in a way that can be interpreted by managers and operational staff as meaningful information quality problems.

The following sections describe the different types of analysis that data profiling tools can perform automatically and how these can be interpreted to determine whether information quality problems exist.

Column analysis

Column analysis refers to the different types of statistics that can be gathered from all values within a column of a database table, otherwise referred to as database fields or attributes. If “DateOfBirth” is chosen for the analysis, then data values for the “PostCode” field will not be analyzed ([Table 12.2](#)).

Table 12.2 Typical Table Structure

Date Of Birth	Post Code
8/24/1974	CB3 0DS
1/6/1967	SD32 1FZ
12/13/01	CB3 0DS
11/9/1999	
1/12/00	WL8 5TG
5/3/0	TG1 5QW

Various measures can be obtained using column analysis, such as the frequency with which each value occurs, the number of unique values, the number of missing values, and standard statistics (maximum, minimum, mean, median, and standard deviation) for numeric values. For example, for the PostCode field a frequency analysis would indicate that CB3 0DS occurs twice and all the other values (including the missing value) occur once. The number of unique values for PostCode is two and there is one missing value for this field. An analysis of the format of the values in a column can be used to identify possible erroneous values. For instance, it is possible to check all the dates in the DateOfBirth column against the formats mm/dd/yyyy and mm/dd/yy. This would indicate that all except the last value match this format in [Table 12.2](#). Similarly, postcodes have predefined formats that can be used to check the postcodes values for errors. Furthermore, especially with numeric data, inaccurate outliers can be identified, while performing a sanity check on the distribution can help to see if there is any suspicious skewing of the data.



EXAMPLE

A car insurance company may know that their customers are mostly between 17 and 27 years old (if they specialize in providing insurance coverage for inexperienced drivers).

You may expect to find a small number of people who start driving at an older age, but the distribution should be skewed toward, and truncated at, 17 years old.

One of the best ways to identify problems using a column analysis is to inspect outlying values for the various statistics. For example, if there is only one value that is far from the mean of a range of numeric values, then this is a good candidate to check for an error. Similarly, looking at the values that occur infrequently can help identify problems such as spelling errors and values that have not been formatted consistently. Conversely, excessive use of inaccurate default values (i.e., values that are entered by default by the system and the user does not change them to the correct value) can be spotted by inspecting the very frequent values occurring in a column.

When databases are developed, the data type that will appear in a column is specified as part of the data model (metadata about the system). Types include dates, numeric values, alphanumeric (or string) values, etc. This type may not always match the actual data that is contained within the column when it is used on a day-to-day basis. For example, a field that is defined as a string type could be used to record

date values, and a variety of date formats may result, along with text descriptions of dates (e.g., “1950s”). This problem may also occur when data is transferred from one system to another and the data ends up in the wrong column; erroneous ETL operations are one example where this may occur. ETL operations also need to double-check the “real” type of the column data to ensure that it can be successfully loaded into another system without mismatches (a date value will not enter correctly into a numeric field). A column analysis could be used to infer the data type by inspecting each actual value for the column, and therefore detect when there are mismatches between the recorded type and the actual type of data.

Using a column analysis can help to indicate whether reference data is needed: if there are many inconsistent values between different records for a particular field, then it could mean that the users are given too much freedom to enter any value they wish. When addressing this problem, speak to the users of the system and, with their assistance, develop a thorough domain of values that they can choose from to enter into the field.



IMPORTANT

Guard against the problem where the users cannot find the exact entry they need. This results in the situation where the users leave the default value in place or they select the first value in the list. You can detect this by using a column analysis to count the frequency of these values to determine any abnormalities.



ACTION TIP

After introducing a new dropdown list, it is advisable, in the first few months, to profile what values are being entered. Investigate if one value seems to be too frequent compared to the others. You could get the users to broadly estimate the frequencies of each value in the domain and automate a column analysis to count the frequencies and check whether there is a large discrepancy between predicted and actual frequencies. This will tell you if you have the problem where the users are entering false values to work around the system constraints.



ACTION TIP

Use the reference data found in the understanding the information environment step (TIRM step A5) to identify relevant domains of values.

Domain analysis

Column analysis can be used to discover what the domain of a particular field is, while domain analysis is used to check whether a specific data value is contained within a domain of values. For instance, if you use column analysis to help develop a domain for a particular field, domain analysis can then be used to validate that the data lies within this domain. The way in which the domain is represented depends on the data type: for numeric values the domain can be represented by a range (e.g., between 1 and 20), whereas for non-numeric data each domain value must be specified (e.g., country codes EN, DE, AU, US, etc.). Domain analysis can report values that are outside of the required domain, and therefore, flag inaccurate data.

Cross-domain analysis

Cross-domain analysis enables the identification of redundant data between different data sets by comparing the domains of the values within a column. If there are overlapping domains (even partially overlapping), then these can be investigated further to check

for redundancy. Eliminating redundancy is desirable in many cases to ensure that data inconsistencies do not occur and that unnecessary work is not being carried out to update and synchronize multiple data sets.



EXAMPLE

Two fields in different databases may be called different names but could represent the same thing (i.e., be semantically equivalent). In this case, inspecting the field headings would not reveal the overlap, and therefore inspection of the values

is needed. The cross-domain analysis will do this inspection to confirm whether the sets of values are likely to be the same. It would then be necessary to verify this with domain users and cross-check against any other relevant metadata.

Lexical analysis and validation

Lexical analysis is used to map unstructured text into a structured set of attributes. One common example is the parsing and dissection of an address into street, city, country, etc. External data sources, such as dictionaries, can be used with lexical analysis to validate the values, and with the vast number of data sets available online, this can be a powerful approach to check the validity of the information. For example, postal databases can be used to validate whether an address refers to a real address.

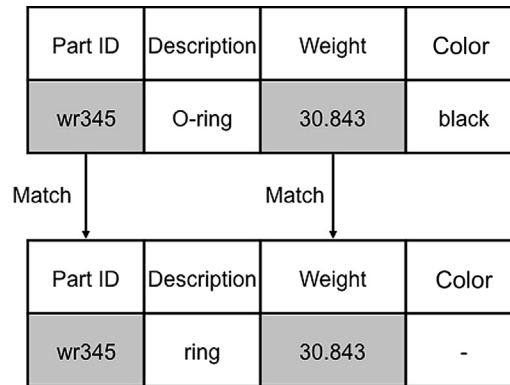
Primary and foreign key analysis

Primary and foreign key analysis (PK/FK analysis) is used to identify columns in a table that can serve as a primary key (unique identifier) or foreign key (reference from records in one table to a primary key in another table). These types of methods reuse the statistics used in column analysis, such as the number of unique values in a column, to identify single columns or groups of columns that can serve as a primary key. PK/FK analysis is useful in the configuration of matching algorithms, which help to identify duplicate records.

Matching algorithms

In addition to the redundancy between columns of a data set, the records in the data set may contain duplicate entries. A common example to illustrate this is duplicate entries of customer records within organizational CRM systems. In this case, a customer may be recorded twice (or multiple times), and each of these records needs to be merged into a single customer record. This often happens because a customer may have been recorded at different addresses, women may be known under both maiden and married names, and children may have the same name (or initials) as parents, etc. It is, therefore, very difficult to determine whether two customers are distinct or not.

Many algorithms exist for detecting problems, such as whether any two (or more) records in a database refer to the same entity that the record represents. If identical records are detected, then there are additional algorithms that can merge the two records according to predefined preference rules. These algorithms are commonly found in master data management (MDM) systems, within which one of their aims is to remove duplicates in master data. One reason these algorithms are considered separately is that not all cases can be resolved automatically. The detection algorithms can be used to flag candidate

**FIGURE 12.3**

Deterministic record linkage.

records for merging and pass these either to the automated merging algorithm or to a human operator who can manually review the decision and perform the merger if necessary.

The challenge with the detection algorithms is to correctly configure them so that they capture all the cases you want them to, and that they do not miss cases where records should be merged. There are many names for these algorithms, including record linkage, merge/purge problem, object identity problem, identity resolution, and de-duplication algorithms.

The detection algorithms can be placed into two categories: deterministic and probabilistic. Deterministic algorithms work by comparing the values for certain attributes between the two records, and if they all match, then the records are flagged to be merged. The example records about engineering parts in Figure 12.3 show two records that can be deterministically linked. These two records are both about the same part, but the descriptions are slightly different and the color is missing for one of the records. However, the part ID and weight attributes contain the same values and therefore indicate that these refer to the same part. From this example, you can see how the challenge is to configure the algorithm correctly by specifying the attributes that indicate when the records match. If the description attribute was also required to have matching values, then the algorithm would indicate that the records do not match. For deterministic matching, you must be sure that the set of attributes that must match are correct. Otherwise, there are two possible erroneous outcomes: two records will be thought to be the same when they are not, or two records do refer to the same entity but they are not considered to match. Deterministic record linkage is, therefore, ideal when reliable unique identifiers can be found for an entity.

Probabilistic algorithms provide a further level of configuration, and allow weights to be set for every attribute. Usually, there are two probabilities that need to be specified for an attribute. The first, m , is the probability that a common attribute agrees on a matching pair of records, and the second, u , is the probability that a common attribute agrees on an unmatched pair of records (nonmatching records agree simply by chance). For instance, gender usually has two possible values (female and male) that are uniformly distributed, and therefore there is a 50% chance that two records will have the same

Table 12.3 String Differences

Operation	Example
Insertion	abc → abcd
Deletion	abc → ab
Substitution	abc → abd
Transposition	abc → cba

value for this attribute when they are not a match. These probabilities are used in the standard record linkage algorithms to give a final weight for each attribute, and then are summed to give an overall value that indicates whether the algorithm considers the two records to be a match or not.

In many cases, for a particular attribute, two records may have very similar values that are not exactly the same. Observe the “Description” field values in [Figure 12.3](#) (O-ring and ring) that differ only by two characters. This type of difference is very common in all areas; names of people, addresses, and customer reference numbers may all contain small typographic errors that mean they do not match exactly. Approximate string matching (also known in some instances as fuzzy matching) can be used to address this problem, which effectively tolerates the various differences that can arise between values. [Table 12.3](#) shows the typical examples that approximate string matching algorithms can handle. Using approximate string matching algorithms with record linkage algorithms is therefore very common and can lead to a more reliable record matching solution. Standard MDM solutions already contain these algorithms and they often provide intuitive and convenient ways of configuring the parameters to suit various cases.

To assist with approximate string matching, lexical analysis can first be applied to the data to help standardize the values. The difference is that with lexical analysis, the values are actually changed before the matching algorithm runs, whereas relying on approximate string matching means that the values do not actually change. The algorithm can tolerate the differences during its execution.

Semantic profiling

Semantic profiling is used to check predefined business rules that apply to a data set. There may be no explicit reference to the business rule within the data model, and only the users of the data set know what the rule is. Evidence of the rule may only exist in the data itself. An example business rule between two columns could be:

If “location” = 1, 2, 3, or 4, then “warehouse” = W1

If “location” = 5 or 6, then “warehouse” = W2

The “warehouse” field may be calculated automatically by the software application. However, if the data in the database is moved to another database that does not automatically calculate this rule, then violations of the rule may exist and the data would be inaccurate. Semantic profiling can, therefore, be used to detect violations of rules within the data by inspecting each instance of data and flagging values that do not adhere to the rule.

Summary

Each of the methods described in this section are powerful methods of automating the detection of information quality problems in large data sets. The methods are typical of what can be found within data profiling software tools. Information quality professionals use these software tools to support the analysis of the data, interpret the results, and report the information quality problems in a way that is meaningful to business managers.

Besides supporting professionals who provide information quality-related services for organizations, these types of methods can also be attached to information systems and applied continuously to detect reoccurring information quality problems. Many vendors provide “bolt on” data quality software that uses these types of methods to detect and also correct the problems before the data is entered into the relevant information system. The correction of the problems is often referred to as data cleaning, which is the process of modifying the actual data to correct problems. However, before jumping in and correcting each problem as it is found, the TIRM process suggests that first you need to assess the overall risk posed by the problems so that improvement of the information can be focused on the most critical areas.

INFORAS: A RISK ANALYSIS TOOL COVERING STAGE B OF TIRM

While there are tools that can be used to perform some of the TIRM steps, one single tool has been developed by the authors to support all of the steps within stage B of TIRM process. The aim of stage B is to assess the information risks in the organization. The tool, referred to as the InfoRAS tool, provides features that can model and record the information captured for each step and also calculate the final risk score for each business process. This is an example of automation that supports humans in calculating the risk, rather than fully automating stage B of TIRM. [Figure 12.4](#) shows the different components of the TIRM model that were introduced in Chapter 5 and that can be modeled within InfoRAS, starting with the business process on the left and finishing with the impact on business objectives on the right. We now briefly revisit the TIRM model before explaining the functioning of the InfoRAS tool.

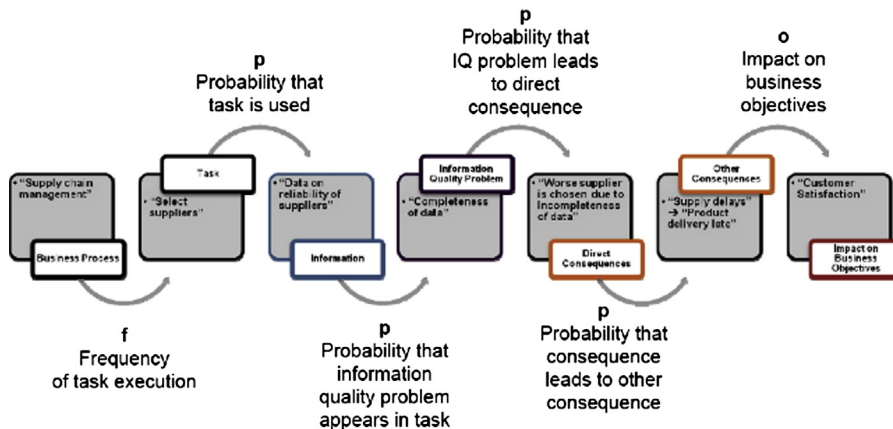


FIGURE 12.4

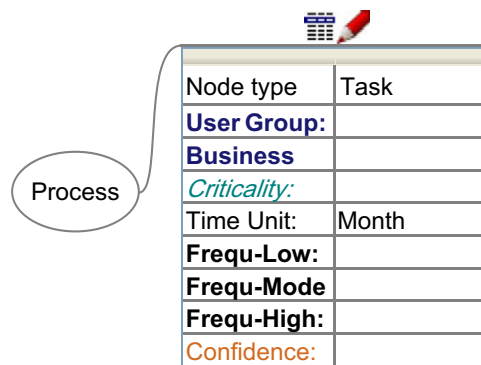
Components that can be modeled by the InfoRAS risk tool.

Each business process in the TIRM model contains any number of tasks that are carried out as part of that business process. For example, in Figure 12.4 selecting suppliers is an example task that is part of the supply chain management business process. A task may require the use of a particular piece of information (or multiple sets), such as, continuing the example, data on the reliability of suppliers. Each piece of information may contain information quality problems, such as missing entries (completeness of the data), which result in direct consequences. In the example in Figure 12.4, the worst supplier could be chosen based on not having the complete list of the suppliers. A direct consequence can lead to one or more intermediate consequences, and these intermediate consequences can have further consequences and so forth. For example, a poorly chosen supplier could result in supply delays, leading to a delayed final delivery of the product, which, in turn, could result in customer dissatisfaction. This is an example of an impact on the business objectives, which is the final part in the model in Figure 12.4.

As explained in Chapter 5, there are also five different parameters in the TIRM model that specify the link between the components in the model:

1. The frequency of task execution, which is the number of times (e.g., per month) that the task is actually carried out.
2. The probability that the information with the quality problems is needed.
3. The likelihood that the information quality problem appears in the information that is needed for the task needs to be specified.
4. The likelihood that the problem leads to the direct consequence along with the likelihood that each consequence leads to other consequences.
5. The severity of the impact in the impact on business objectives component.

InfoRAS actually accommodates a more in-depth recording of parameters than those described in the previous section. This is illustrated in Figure 12.5, which shows the parameters associated with a task node. As noted before, for each process the frequency with which the task is executed is recorded; however, rather than specify a single frequency number, it is far wiser to record a range that is very likely to contain the frequency. This was confirmed in the trials of the TIRM process in organizations,



Node type	Task
User Group:	
Business	
Criticality:	
Time Unit:	Month
Frequ-Low:	
Frequ-Mode	
Frequ-High:	
Confidence:	

FIGURE 12.5

The process node and parameters for the task node in InfoRAS.

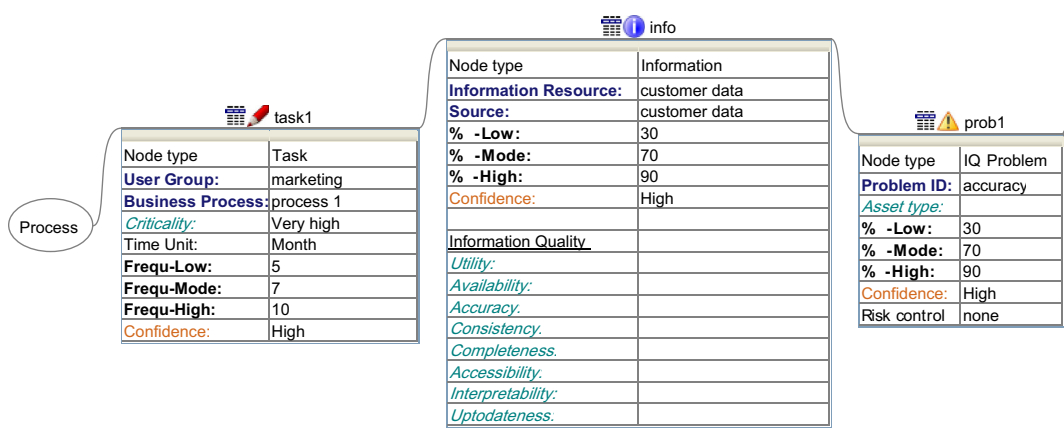


FIGURE 12.6

The parameters for the task, information, and information quality problem nodes in the InfoRAS tool.

which found that it is often difficult to ascribe a single frequency number to a task with confidence, and it is easier to specify a range where the frequency resides. InfoRAS, therefore, allows the user to enter the lower bound, mode, and upper bound of the frequency with which the task is executed. The trials also found that in some cases the experts providing the estimates are very confident that the range captures the actual frequency, but in other cases they were found to be less confident. InfoRAS captures this uncertainty and allows the user to record the confidence, shown as the last parameter in Figure 12.5.

Specifying the range is not just applicable to the frequency that the tasks are executed in the process, but for every subsequent probability, as shown in Figure 12.4. InfoRAS allows the user to specify the range for every component. For example, in InfoRAS, each component contains the lower bound (%-Low), mode (%-Mode), upper bound (%-High), and confidence parameters, and these can be seen in Figure 12.6 for the information and information quality problem nodes. In some cases, an exact frequency may be known, in which case the same value can be entered in the lower bound, mode, and upper bound fields of InfoRAS. The final calculation performed by InfoRAS uses each of these values, with the confidence to calculate the overall risks to the business posed by the information quality problems. For the other parameters for the task, information, and information quality problem nodes, such as user group, and business process are informational only and can be used to provide further documentation about the different nodes. InfoRAS also provides a free text field that is associated with each node and can be used as needed; Figure 12.7 shows a screenshot of InfoRAS with the task1 node selected and the description field at the bottom. In this field, it is advisable to specify links to other documents, such as:

- Process models that can help define the scope of the process and tasks.
- The names of the databases or documents containing the information that is represented by the information node.
- Information quality problem assessment documentation that is associated with the information quality problem nodes.
- Detailed information about the risk controls that are already in place for the consequences.

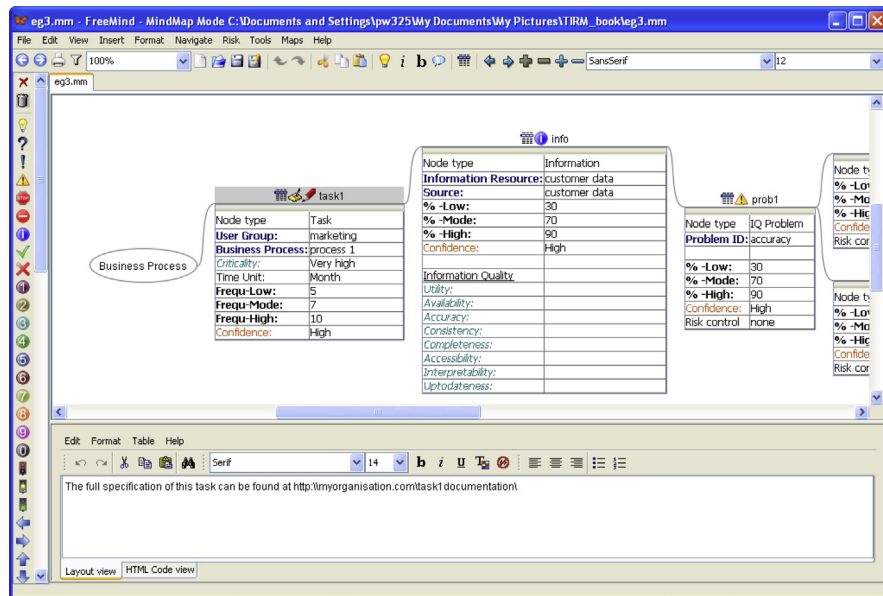


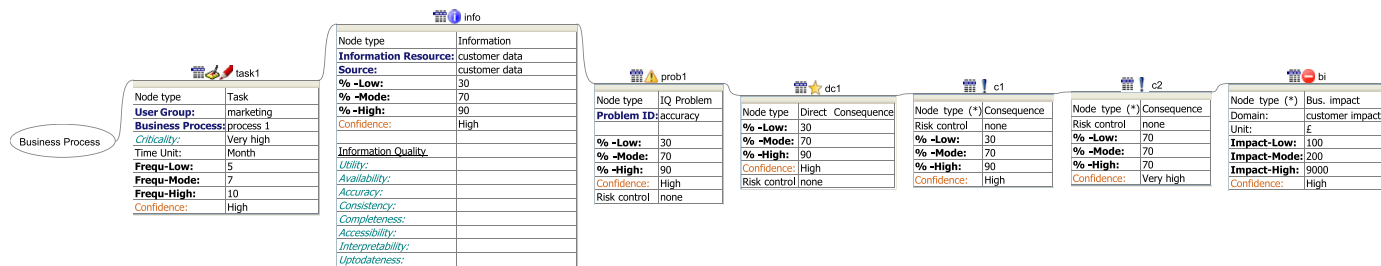
FIGURE 12.7

Screenshot of InfoRAS with notes.

Of these parameters, the time unit in the task node and the unit in the business impact node are very important, because when the final risk is calculated, it needs to be interpreted as, for example, pounds per month. The time unit in the task node is used to record whether it is per month and so forth, and the unit in the business impact is used to record the relevant currency. Note that this may not always need to be a currency: in some cases it could be a rating for health and safety or a measure of availability of a service.

The modeling of the consequences and the business impact using InfoRAS is shown in Figure 12.8. As noted before, any number of consequences can be recorded before reaching a business impact, and in the example in Figure 12.8, two consequences (c1 and c2) and their direct consequence (dc1) have been recorded. Note that this is the first version of the InfoRAS tool and therefore some functionality is yet to be included.

For simplicity, the example model of consequences and business impacts discussed previously was linear. InfoRAS, however, is capable of representing more complex relationships and can handle multiple tasks for a business process, multiple information resources for each task, and so on. Figure 12.9 shows a typical model that can be created with the tool, which contains two direct consequences that may result from a problem, three consequences, and three different business impacts (two are related to the impact on the customer and one to operational efficiency). As shown in Figure 12.9, InfoRAS presents this model in a clear and concise way, which enables analysts to clearly visualize the different impacts and chain of consequences.

**FIGURE 12.8**

The direct consequence, other consequences, and business impact nodes in InfoRAS.

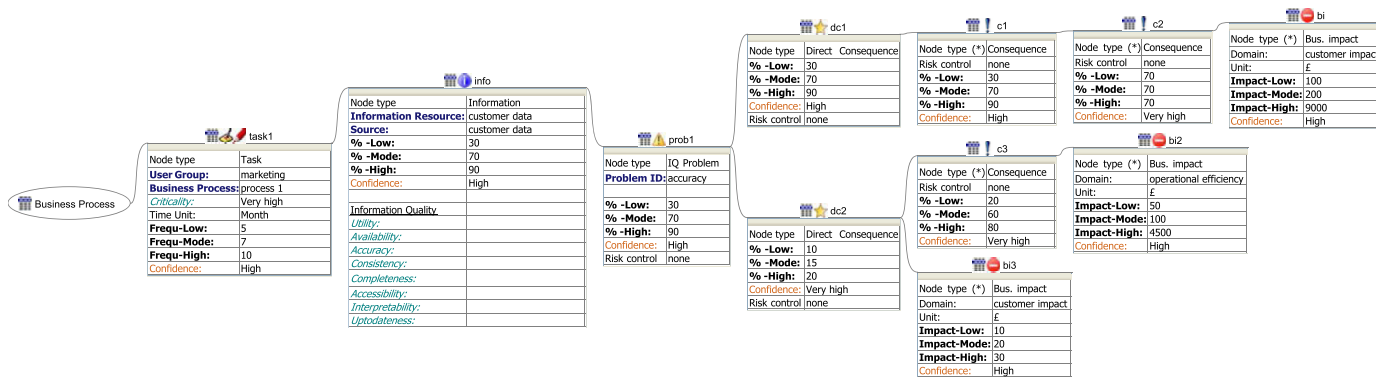


FIGURE 12.9

A more complicated example of the structures that can be modeled by InforAS.

One of the main advantages of InfoRAS is that it is able to calculate the total risks regardless of the complexity of the model and present aggregated results at each stage. Figure 12.10 shows the calculation for the example risk model in Figure 12.9, and the risk per annum is shown for each business impact node. For example, for bi1 the total risk is £30,632, for bi2 the total risk is £4243, and for bi3 the total risk is £105 per annum. The aggregated risk given by prob1 is the sum of each business impact that is related to this problem (in this case, £34980). There is only one problem and one task in this example, and so the overall risk to the business process is the same as for prob1. At the business process node, the results give a breakdown of the aggregated risk values for the IQ problem, data type, and business impact. When there are many IQ problems, information sets, and business impacts, having the results aggregated in this way is useful to help identify particular “pain points” within the business process that have a large effect on the overall risk.

SOFTWARE TOOLS FOR DETECTING AND TREATING INFORMATION RISKS

In this section we discuss some of the example data risks that we found were common to many organizations, and show how existing software tools and techniques for managing information can be applied to automatically detect and mitigate the problems.

Example risk 1: Engineering Asset Management

Many organizations need to keep records about the locations and state of their physical assets. These may be trains, aircraft, underground water or gas pipes, electricity supply cables, and so on. Immediately, this does not sound like a very difficult task until you realize that some companies need to manage millions of physically distributed assets, of differing types that may be static or moving, cannot be easily taken offline for maintenance, and contain many dependent subcomponents. The asset management division in one organization we studied needs to maintain all of their assets in the most optimal way possible by saving time, resources, and costs. They carry out inspections of their assets, which are distributed throughout a large geographic area, before deciding whether or not to replace, repair, or refurbish an asset. These inspections take time, resources, and have an associated cost, and additionally, need to be optimized. These processes clearly rely on having good-quality information about the assets. Information about the assets includes details such as asset type, current and previous locations, current physical state, dates of previous (and predicted dates for) inspections and maintenance, and the subcomponents that may require maintenance. With poor-quality information about the assets, engineers struggle to keep track of what assets they have, which ones need maintaining, and which ones need replacing.

This information is stored in a combination of asset management systems, but the main system for location information is the geographic information system (GIS). The problem with the location information is that some asset locations are recorded in the system and the asset is not physically at that location. Other times, the asset information is not recorded in the system, but does actually exist in reality. This happens because there are limited procedures in place to help keep the actual state of the asset and the information about the asset in synchronization. For example, an asset may be moved physically from one place to another, but the records about this asset are not properly updated.

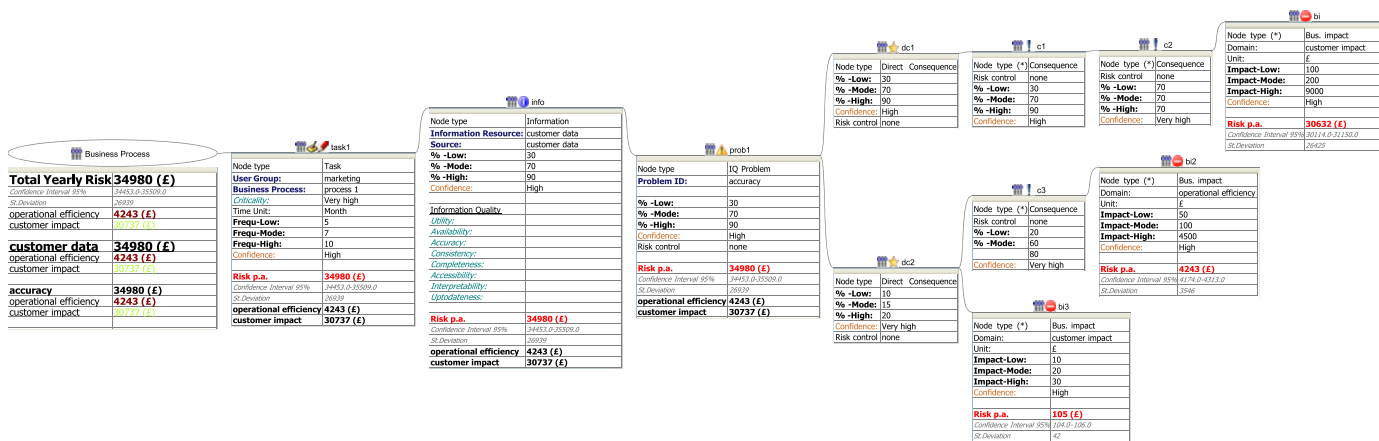


FIGURE 12.10

Risk total calculations with different levels of aggregation.

The impact is that inspectors go out to the wrong locations expecting to find an asset (sometimes traveling long distances, costing time and fuel) only to find that it is not where it is expected to be. It is very costly, therefore, to find missing assets! Clearly this does not just affect inspections, but maintenance of the assets is not optimized, and some assets are not maintained at all because the GIS does not record their existence. In the cases of critically important assets, not properly maintaining the asset could cause it to fail and incur serious risks to the business.

With millions of assets to inspect and maintain and the current poor-quality data in the system, the question is what could the company do to address this and move toward being able to develop optimal inspection/maintenance strategies?

There are two approaches that can be taken to address this: either to leave the information as is and use risk controls to ensure that decision making does not result in a negative impact to the business, or attempt to improve the information.

The first approach aims to ensure that subsequent analysis and decisions are taken with suitable risk controls, based on the expected level of quality of the data needed to make the decision. This is appropriate if the information only supports the decision.

However, if the information is used as a direct input to the decision, and it cannot sensibly be made without it, then there is no option but to attempt to improve the information.



ACTION TIP

When considering an automated solution to solve a data problem, consider both how to address the problems with the existing data, as well as how to address problems that could occur with new data that will be entered into the systems in the future.

When seeking to improve the information there are two parts to be considered: what to do to ensure that new information entering the GIS system is correct, and what to do to correct the existing poor-quality information.

Addressing the problem for new data entering the system

The current process, where engineers record their actions on paper and then enter the details into the GIS system later, is fraught with problems. Engineers forget to update the GIS system from the paper records, and it is also easy to misinterpret the paper notes if someone else is entering the data.

With the widespread use of handheld electronic devices, such as mobile phones and tablets, that are able to connect wirelessly to the Internet and therefore to the organizations backend systems, there are many possibilities to improve the quality of data capture. This data capture can now be done in real time (e.g., when the engineer has just finished an inspection or repair of an asset), increasing the chances of correctly capturing what has been done. In this case, entering the data gets closer to being part of the actual maintenance job, and is therefore less likely to be neglected.

Organizations are beginning to develop their own applications on mobile devices with bespoke user interfaces, which allow field workers to capture critical data in the easiest way possible while also supporting real-time validation checks. Being able to validate data in real time is a tremendous advantage because it can provide immediate feedback on the quality of the data and at the time when the

engineer is observing the real entity that the data is describing. Obvious mistakes can be caught immediately and prevented from being entered into the backend system.

Improving the existing information

For improving the existing information, the obvious approach is that the organization could send out a team of people to check every asset and then perform a cross-check of this against the information in the GIS. Correctly, you may observe that this sounds rather resource and time intensive. In fact, because in many organizations of this type there are hundreds of thousands, if not millions, of assets that need to be cross-checked, the whole idea is just not practical. Some level of automation is required. How can the information be corrected without having to go and inspect every single asset?

If some of the information in the system (and other related systems) is known to be correct (e.g., due to recent asset inspections), this can be used to infer properties about the incorrect information based on knowing some of the rules about the assets. For example, if you know that if asset A exists, then so must asset B, and asset B is not in the GIS, then this implies that asset B is missing from the GIS. Note that if, to correct the data, asset B is entered into the system, then it is important to accompany this with metadata describing that inference was used to determine the existence of this asset.

In many cases, there may not be many rules or known-to-be-correct information in the system, but correcting all the information possible using this approach helps reduce the number of necessary physical inspections. This could drastically reduce the time and cost associated with improving the information.



ACTION TIP

Use the information in the systems that is known to be correct to infer properties about the other information to validate its accuracy and determine what the correct values are most likely to be. Moreover, update the metadata to describe when any inferences have been made when correcting the data.



ATTENTION

Do not expect to be able to correct all the data with inferred values because there may be many cases where there is no reliable (or authoritative) data to be used as a basis for inference. However, just validating and improving the data that is possible within this approach could prioritize what physical checks are required, as well as drastically reduce the need for these physical checks.

To automatically discover rules in data, data mining tools can be used. The following sections describe the different data mining methods that can be used to assist with automating the detection and correction of the data errors in the GIS while minimizing the need to physically cross-check the assets.

Association rule mining

Association rule mining can help to automatically discover regular patterns, associations, and correlations in the data. It is an ideal method to use to discover hidden rules in the asset data. In the asset management example, it could be used to discover the rules between different assets and their

properties so that, for example, when there are assets missing in the GIS, it could be possible to infer what they might be.

Association rule mining can uncover what items frequently occur together and is often used in market-basket analysis, which is used by retailers to determine what items customers frequently purchase together. If dependencies exist between assets, such as asset A is always replaced with asset B (asset B may be a subcomponent or supporting device), then association rule mining can help identify these rules. The method does not operate only on simple examples like this, but can be used in general to find groups of assets that frequently “occur” (are replaced, maintained, disposed of, etc.) together, thus giving an indication of what you would expect to find in the GIS.

The analysis of what items frequently occur together is supported by two measures, and these give an indication of whether a pattern is interesting and should be investigated further. Considering a database that contains information about asset replacements, one may perform the analysis on this to determine what asset groups are usually replaced together and therefore what assets should exist in the group. Any missing assets in the system can be detected by requesting the assets at each physical site from the GIS and comparing this list to the list of assets in the group. Two measures that support this analysis to help determine the asset groups are confidence and support. A confidence value, for example, of 70%, indicates that when asset A is replaced there is a 70% chance that asset B will also be replaced. The support measure shows the percentage of transactions in the database that support this statement. For example, a support value of 20% means that of all the transactions in the database, 20% of them showed assets A and B being replaced together. Usually, thresholds are set so that only the most significant patterns are shown, rather than all patterns with low confidence and support values.

Maintained assets may not always appear as part of a single maintenance action, in which case the preceding method would not be able to identify patterns among the assets. To assist with this, within association rule mining there is another method that analyzes patterns that occur within a time sequence. If the maintenance actions each appear as a record in a database (transactional data), then sequential analysis can be applied to determine what records commonly occur close together. If the maintenance records indicate that it is common for the engineer to repair asset A, B, and then C within a short time span, then assets A, B, and C should be recorded in the GIS as appearing in relatively close proximal physical locations.

Semantic profiling

The data quality profiling method of semantic profiling (described previously) is a useful technique to apply to check the validity of any rules discovered by association rule mining. Rules can be encoded and then the profiler will traverse the data and record any violations of the rule.

As an example, association rule mining may have discovered the rule that water-pumping stations are often needed by canal locks. Semantic profiling could be used to check all cases when a pumping station does not exist near a lock, and it could flag these cases for further inspection. In this GIS, this requires checking the type of asset (e.g., water-pumping station or lock) and possibly its physical location (usually via latitude, longitude, and elevation coordinates). If for a particular water-pumping station there is no lock within say a half mile, then this would be something to investigate.

Furthermore, the simplest cases arise when there is a reference to an asset in one system, and the asset does not exist in the other. For example, semantic profiling could be used to identify missing references between the transactional maintenance records and the master data GIS records. If there is a maintenance record about a water pipe inspection, then the associated master data about this water pipe should exist; if not, then clearly there is a missing record.

Summary and discussion

Numerous organizations need to ensure that they properly maintain their business assets, whether they relate to managing facilities or the core engineering assets of the organization. For some organizations, such as utilities, transport, and engineering firms, this is a core part of the business. Errors in the data about the assets can easily result in serious risks to the business, as poor decision making is likely to result from erroneous data. The sheer scale of the data within many asset management-related systems makes automation a necessity for helping to improve the data. The automation may support the data gathering process, such as with mobile devices with instant data validation, or could support intelligent processing of the data to help reduce the time needed for physical validation of the data against the real-life situation.

Example risk 2: Managing spares and consumables

One information risk that we encountered was within the managing spares and consumables business process of a manufacturing organization. This organization needs to order parts that are used as material for their manufacturing processes. The organization strives to procure quality parts at the most competitive price from various suppliers. In some cases, supplier relationships and contracts are in place and in other cases procurement agents find other suppliers on an ad-hoc basis. The recording of their material consumption is critical for the organization to optimize the procurement of parts for their manufacturing, as well as ensuring that inventory levels are manageable. If perishable parts are ordered and not used within a certain time, then they need to be disposed of. This incurs significant costs for purchasing the part, storage of the part, and part disposal. Even nonperishable parts if they are not used within a reasonable length of time can degrade (as well as fall outside their warranty period) and take up valuable warehousing space. Conversely, if there are no parts available at the time the manufacturing process needs them, the manufacturing cannot continue. It is, therefore, imperative that the ordering of parts is optimized to keep the manufacturing processes operational while ensuring that the warehouses are not overloaded and parts are not degrading beyond their useful life.

In this organization an ERP system was being used to hold information about materials consumption from the manufacturing process. However, users of this system were complaining that the information was often out of date, sometimes incorrect or incomplete, and often difficult to interpret because there was no unified terminology for materials. The main reason for this was that the data on consumption was being recorded manually on paper-based forms and then being manually entered into the ERP system.

The impact was that parts were being ordered unnecessarily as it was not transparent which exact spares and consumable materials the company needed to order. This resulted in between 10% and up to 1000% higher prices for parts. The estimated risk probability was 10–20% for parts and 30–40% for consumables. This information risk resulted in yearly estimated losses of \$6 million on average per production site.

The various problems found in the consumption information can be divided into two groups, which necessitate two different solutions. First, the problems of out-of-date, incorrect, and incomplete information caused by poor manual data entry can be addressed by reducing the manual data entry and introducing automated solutions to capture what is really happening with parts consumption. Second, the problems of not being able to interpret the parts because there is no unified terminology for materials requires changes to the information system that stores and provides access to the data for its users.

Automated track and trace technologies

Rather than having humans sense when a part has been taken from the warehouse and has been used on the production line it is possible to introduce automated methods that can detect these events and record them in a database. Technologies such as radio-frequency identification (RFID) can be used in appropriate situations to track and trace parts to determine their actual locations. These work by installing a small tag on the part, which uniquely identifies the part, and then installing readers at various locations (e.g., at the entry to a warehouse). When the tag passes by (or is near to) the reader, then the reader can record this event and the result is stored in the database. In its simplest form, this event can record a timestamp for when the event occurred and the unique identifier of the part. With this simple level of detail of data and a small amount of inference, it is possible to determine the location of parts. For example, if we wish to determine which parts are currently stored in a warehouse and when a part is taken out of the warehouse, we could first tag each one of the parts before they enter the warehouse. Then we could install a reader at the entrance to the warehouse that would record the new part entering the warehouse; we would know that it is a new part because there would be no previous record of the part in the database. When the part is taken from the warehouse it would pass out of the entrance and be read by the reader, and in this case we would know that the part is being removed because the previous database entry about this part would have recorded it coming in. So by observing the entries in the database and correlating these with reads of the part by the reader, we can determine where the part is. Clearly, this is a very simple example, and often there needs to be a series of readers at various locations. For example, there may be more than one exit or entrance to the warehouse. The same principle can be applied to determine the location of the part near the manufacturing line to determine when it is in the queue to be used as material input into the manufacturing process. The level of detail of the location of the part depends on the number of readers installed and how accurate these readers are at capturing the parts' presence.

A side benefit to using this sort of technology is that business intelligence (BI) questions can be answered that give the business further insight into how the operations can be improved. For example, it would be simple to calculate the time each individual part spends in the warehouse if you automatically record time in and time out (by subtracting the timestamps for the part-out and part-in events recorded by the reader). With detailed records of each part's time in the warehouse, it would be possible to optimize the purchase of part warranties to reduce the costs associated with parts falling out of warranty, as well as have a better understanding of which parts can be bought in batches of a certain size. As well as BI questions, this automation technology can clearly assist the operational decisions that are incurring unnecessary additional costs to the organization, such as whether to procure more of a certain type of part immediately or not. Any ways of improving the operations identified by these activities could be used to inform the information risk treatment stage of the TIRM process. By identifying and focusing

on ways to optimize operations, the organization is essentially removing unnecessary procedures that may cause information risks in the first instance. This can operate the other way around too: if certain information risks are identified with the TIRM process, then treating these risks at the operational level is one option, but the organization may want to take a more strategic approach to avoiding the information risk. The TIRM process could, therefore, be used as an indicator for what BI-related questions should be posed to help steer the organization around information risks that cannot be treated with operational risk treatments.

Master data management

Regarding the problem of not having an unified terminology for materials, MDM is a key information management technology that can help to solve the problem.

At a simple level, a database could contain a list of parts that are referred to in multiple different ways. This same problem was introduced when describing reference data previously, with differences occurring in the recording of a country. In this example, it is a part that could be recorded in the database in multiple ways. For instance, the descriptions of parts are often in free text fields that allow the users to enter any description they like, which can clearly lead to all sorts of differences. However, even the part numbers can differ: the manufacturing organization may have their internal part number for a particular part, and this is likely to be different from the vendor's part number. When the manufacturer receives the part from the vendor, the goods-received note contains the vendor number for the part, and this needs to be correlated with any other numbers for the part, just to establish if it is the same part.

MDM is a solution to this problem and can help provide the users of the organization's information system with a single, consistent view of parts. Inconsistencies between master data are a problem common to many organizations; MDM is often used in other applications such as CRM and SRM. MDM relies on effective data governance, which provides the rules that the organization must adhere to when managing their data. With the preceding example, data governance should define exactly what a part is (and how it can be uniquely identified) and state, for example, what particular part numbers the organization will use (i.e., manufacturer or vendor part number) in different cases. Without this supporting knowledge, a master data solution has no basis from which it can sensibly merge duplicate parts. MDM solutions may not only be software but could also be a set of procedures that an organization follows. The aim of MDM is to provide a single (often referred to as a golden) version of the data and deliver it to the enterprise (any business unit) while enabling users to update the data in a way that does not reintroduce inconsistencies or errors into the data.

The key ongoing functions of MDM that are needed to ensure that entities (e.g., parts, customers, etc.) are consistent are to:

- Detect and merge, if necessary, any duplicate entities into a single record.
- Standardize any properties of the entities so that they are shown to the users consistently.
- Provide data movement and integration facilities (e.g., ETL).
- Collect all instances of an entity from various databases and present them as a single, consolidated list to the users.
- Provide transaction services that support the creation, reading, updating, and deleting of the entities.

A dedicated software solution to MDM alone is unlikely to be effective to provide these functions. Organizations should also establish an effective data governance program and treat MDM as a data quality improvement process. The software solutions can therefore support these activities as required. There are many MDM solutions available from various vendors and they typically provide ways to automate the preceding functions. The following sections describe these various functions from the perspective of how they can be automated.

Detect and merge records

MDM solutions include matching algorithms (described previously), which help to detect whether two records refer to the same entity. These algorithms could help to detect overlaps in parts in the ERP system of the manufacturing organization. Once these algorithms have detected possible matching records, it is necessary to merge them, and this is one of the key pieces of functionality within MDM solutions.

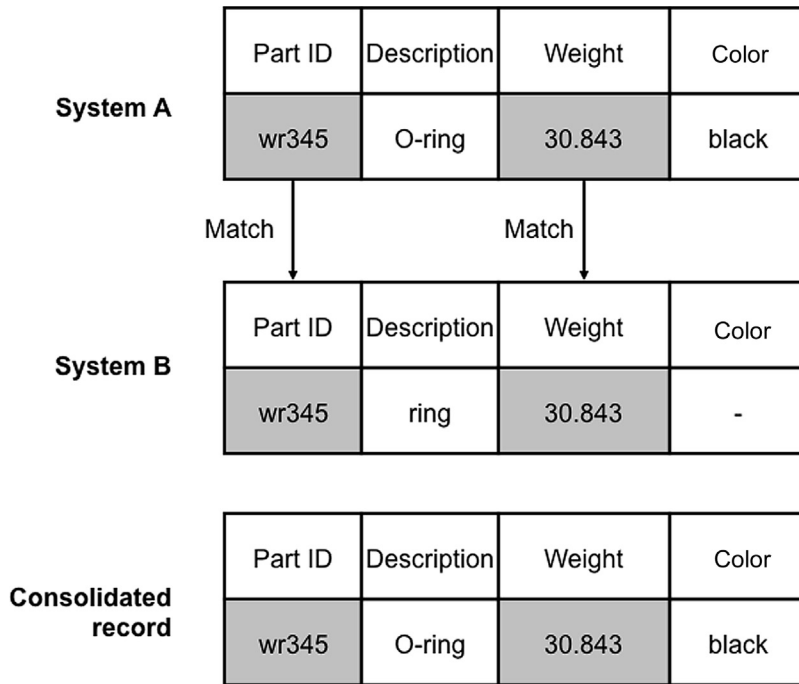
The problems arise when the data values in two different records are inconsistent and it is necessary to choose the correct data value for the new master record. Rules that govern what data is carried forward to the consolidated master record are called survivorship rules and these are part of the merge algorithms. Most of the time, records will be gathered from multiple systems and so the rules need to define exactly which data and which system are to be trusted to provide the best data. Some example rules include:

1. If the value exists in system A, then choose this value, rather than the value from system B.
2. If there is only one value available (the others are missing), then take this value.

As an example of applying survivorship rules, consider what happens when creating a consolidated master record from the data from the two systems in [Figure 12.11](#). With the “Part ID” and “Weight” values, there is no problem because they are consistent, and so these values can be taken and placed directly in the consolidated master record. For the “Color” field it is also relatively straightforward because the value in system B is missing and so the value from system A is chosen (in accordance with rule 2 above). For the description field there are two inconsistent values and this is the hardest case to cater for. Rule 1 states that system A is the authoritative source of reference, and so this value is taken to be included in the consolidated record. You can see how successful matching relies on developing strong rules that cater for the different scenarios that may arise.

Standardization

In the manufacturing company example, the records of parts are spread between various databases and therefore the attribute names may not always be the same. For example, an attribute could be labeled “part_description” in one database and “desc.” in another. MDM solutions help to map between these values to indicate which attributes are semantically equivalent. Note that semantically equivalent attribute values may also be different between systems. For example, date fields may be formatted dd/mm/yyyy in one system and mm/dd/yyyy in another system, which means that the values also need to be mapped. This is referred to as standardization, and it is often performed during the transform step of an ETL process in many MDM solutions (see the previous section on lexical analysis). Even within the same database, there may be differences between the values for a particular attribute.

**FIGURE 12.11**

Survivorship example.

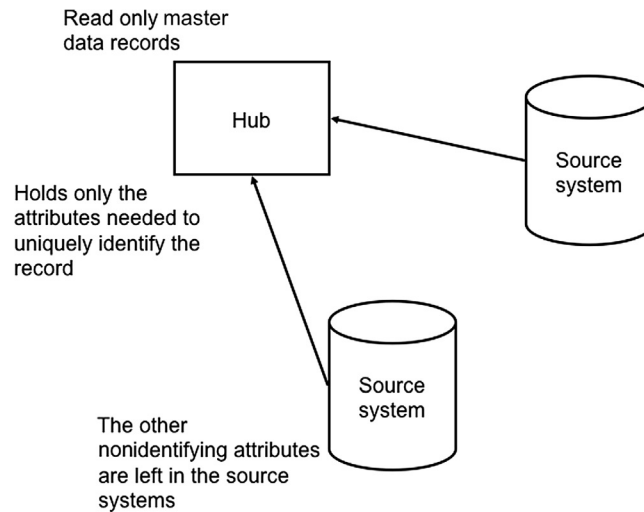
A common example is with free text fields such as addresses or part descriptions that contain different punctuation marks and a mixture of short abbreviations and more fully expanded abbreviations, etc. In this case, standardization could help to present a common value format to all users or to map between these if different users require different formats. For example, standardization could help map between the semantically equivalent values “pneumatic actuator” and “act. pneumatic” by changing one to the other.

Usually before applying record linkage algorithms it is beneficial to standardize values making them more consistent. The record linkage algorithms, therefore, stand a better chance of matching similar values and do not have to rely on approximate string matching algorithms.

Architectures for MDM

Depending on the manufacturing organization’s individual information systems and how they are arranged, there are different possible MDM architectures that could be used to consolidate the parts records and provide transaction support to create, read, update, and delete the parts records.

There are a few different architectures for implementing MDM and it is common for organizations to develop these incrementally from the simplest to the most complex. In practice, while there are many possible ways of implementing these and small differences exist between the architectures, here we describe only the main architectures to give a general overview.

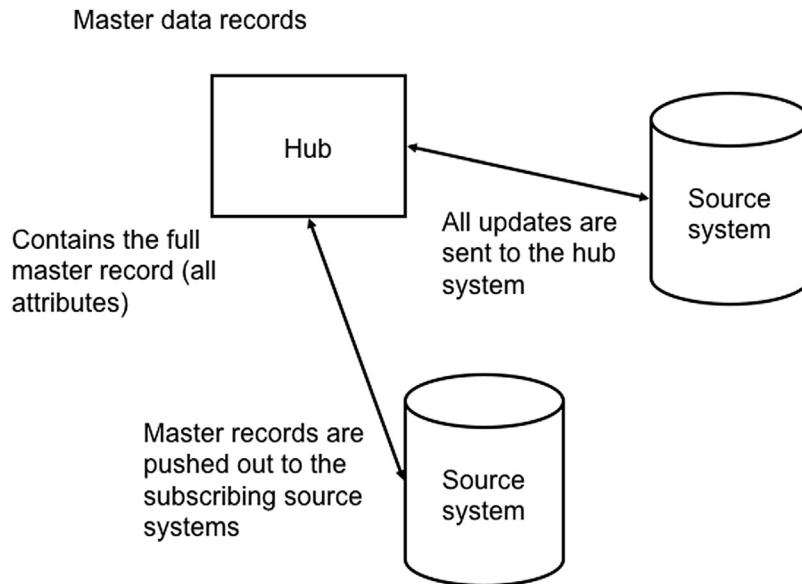
**FIGURE 12.12**

Registry MDM architecture.

The registry implementation style is the simplest architecture and consists of a central hub system that holds the key data that relates to the master record (Figure 12.12). It only holds the data that is essential to determine the unique identity of the record and all other data related to the record are left in the source systems. This avoids unnecessary movement of data between the systems, and allows the users at the source systems to change most of the data without the hub even needing to know. The hub creates a globally unique identifier for each master data record and also holds a reference (cross-reference keys) to the associated record in the source systems. Updates are published to the hub system, using this reference, from each source system. Usually, there are no mechanisms that allow updating at the hub system and propagation of these updates to the source systems, and therefore, this type of architecture is useful when only needing to read the data from the hub. Being the simplest architecture, it is the easiest to implement.

For the manufacturing organization that needs to consolidate parts, this architecture is an ideal starting point to give the users read-only access to the consolidated parts. The transactional systems that track parts' locations and usage can reference the master records for parts in the hub system as a single, reliable version of the truth. However, if the organization needs more than just read-only access to the master data, a new MDM architecture is required that builds on the registry architecture.

At the next level of complexity is the coexistence MDM architecture (Figure 12.13). In this architecture, the hub contains the full master record rather than only the uniquely identifying attributes (as in the registry architecture). Furthermore, not only are the updates from the source systems sent to the hub system, but also changes in the master record in the hub system are sent to subscribing source systems. This means that when an update to a record is made in the source system, the update is sent to the hub and then the update is sent out to all subscribing source systems. The difference in time between these updates means that the subscribing source systems may contain out-of-date information for the brief period before the synchronization is made.

**FIGURE 12.13**

Coexistence MDM architecture.

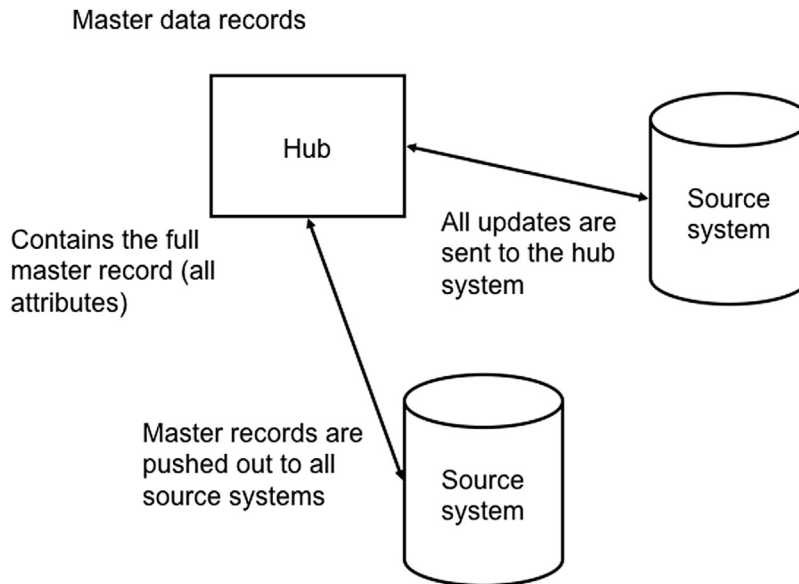
The manufacturing company could use this architecture to distribute the parts records to the relevant source systems where they could be updated, and these updates would be reflected in the other subscribing systems.

The next level of complexity of MDM architecture is when all source systems are updated with the correct master data, referred to as the transactional architecture (Figure 12.14). This is an advanced and complex architecture because it extends the coexistence architecture by synchronizing data to all systems. This is done once the hub has integrated the relevant master data records from all the systems and resolved any inconsistencies.

If the manufacturing organization implements this architecture, it can be sure that all parts records would be properly integrated and available at all systems. This is a complex architecture, and it means that additional effort needs to be expended to develop and maintain this system. The trade-off of whether to develop a system like this or stick with the simpler system should be based on the requirements of the organization, not the desire of IT or anyone else to have the “highest-level” architecture. For instance, if the manufacturing organization can fulfill its needs by using the registry architecture, then there is no need to develop this further.

**IMPORTANT**

The trade-off of whether to develop a system like this or stick with the simpler architecture should be based on the requirements of the organization, not the desire of IT or anyone else to have the “highest-level” architecture.

**FIGURE 12.14**

Transactional MDM architecture.

Note that the hub system referred to in all of the MDM architectures could be a new system or an adaption of one of the existing source systems. If there is one source system that contains the most authoritative list of master records and has good data integration capabilities, then this is a good candidate for the hub. The advantage is that it may already contain a lot of the master records, existing ETL operations to integrate the data, configured data cleansing capabilities, etc. The problem is that

**ACTION TIP**

Consider whether to use an existing source system as the hub, but be wary about how this could negatively affect the operational use of this system.

it would be necessary to ensure that the operational use of this system is not interrupted by making it the MDM hub. It would be easy to overlook the performance requirements of this system, which could be drastically affected if it turns into a transactional MDM architecture that requires the system to synchronize all updates to all source systems.

Summary

With the use of track and trace technologies to automate the reliable capture of information and MDM solutions to ensure that differences in terminology can be automatically unified, there are many options to mitigate information risks with minimal human intervention. For many manufacturing organizations that need to keep track of the state of millions of consumable parts, these solutions are a necessity to address, otherwise they could lead to intractable problems that humans would quickly be overwhelmed by.

CONCLUSION

With the massive data sets used by today's leading organizations, manual methods of correcting information quality problems and analyzing the data are no longer feasible nor wise to apply without support. Automated methods for processing this data are essential and they are becoming increasingly necessary to use for all data-related tasks. Not only are these methods necessary to deal with a significant volume of data that organizations collect daily, but also the speed at which it is necessary to make decisions places new constraints on how the data needs to be managed and analyzed.

Organizations now face customers who will take their business elsewhere if their needs and preferences are not immediately and properly addressed, or the information held about them is incorrect; it is no longer acceptable to take weeks to process data and obtain the results. In many of today's applications, speed is of the highest importance, and reducing the time between the event, data analysis, and decision is paramount to commercial success. This relies heavily on keeping the information free of quality problems before being able to perform speedy analysis to obtain valid results.

Existing software tools and architectural approaches that can help automate information quality assessment and improvement provide the answer to cope with these speed and volume requirements. This chapter has introduced the different ways in which the stages of the TIRM process can be automated, as well as how automated information management technologies can be employed to address different problems in different data types.

REFERENCE

- Gao, J., Koronios, A., Kennett, S., & Scott, H. (2010). Business Rule Discovery through Data Mining Methods. In J. E. Amadi-Echendu, K. Brown, R. Willett & J. Mathew (Eds.), *Definitions, Concepts, and Scope of Engineering Asset Management* (pp. 159–172). London: Springer.

Establishing Organizational Support and Employee Engagement for TIRM

WHAT YOU WILL LEARN IN THIS CHAPTER:

- How to overcome organizational resistance during TIRM implementation
- The reasons for organizational resistance
- How to change organizational culture
- How to engage employees in information risk management

INTRODUCTION

TIRM is multidisciplinary and it should involve *everyone in the organization* rather than be the responsibility of a few key individuals. Not everyone will love your TIRM initiative from day one. There will be some people in every organization who feel threatened by the rising role of data and information assets and might do everything to stop you from succeeding. By involving people from the outset and making them feel that their contributions are valued, engagement and buy-in to the (new) processes will be easier to achieve. This chapter reviews techniques for managing change, how to overcome resistance, and how to engage employees to ensure the successful management of information risks.

ESTABLISH ORGANIZATIONAL SUPPORT AND CHANGING ORGANIZATIONAL CULTURE

Implementing a TIRM program within an organization will require changes that without doubt will create organizational resistance. Resistance to change is not uncommon, and those responsible for the implementation of change programs and procedures may have to work hard to overcome that resistance.

STRATEGIES FOR OVERCOMING ORGANIZATIONAL RESISTANCE

One model for reducing resistance to change is offered by [Kotter and Schlesinger \(1979\)](#). It has been well documented in the literature and has stood the test of time. They consider that people (employees) resist change for the following main reasons:

- *Parochial self-interest*—some people are concerned with the implication of the change for themselves. They think they will lose something of value as a result. People focus on their own best interests rather than considering the effects for the success of the business.

STRATEGIES FOR OVERCOMING ORGANIZATIONAL RESISTANCE—cont'd

- *Misunderstanding and lack of trust*—people resist change when they do not understand its implications. They perceive that they have more to lose rather than gain from the change. This often occurs when trust is lacking between those implementing change and the employees.
- *Different assessments of the situation*—employees assess the situation differently from the initiators of change. Initiators (i.e., change managers) assume that employees have all the relevant information, however, they may not, and as a consequence some

employees may disagree on the reasons for the change and the advantages of the change process.

- *Low tolerance to change*—some people are very keen on security and stability in their work and they prefer the status quo—that is, for things to remain as they are. Even when intellectually they understand that change is good, emotionally they are unable to make the transition.

Kotter and Schlesinger set out six approaches to deal with resistance to change shown in [Table 13.1](#).

Table 13.1 Methods of Reducing Resistance to Change

Approach	Situational Use	Advantages	Drawbacks
Education and communication	Where there is a lack of information or inaccurate information about the change	Once persuaded, people often will help with the implementation of the change	Can be very time consuming if many people are involved
Participation and involvement	Where the initiators do not have all the information they need to design change, and where employees have considerable power to resist	People who participate will be committed to implementing change, and any relevant information they have will be integrated into the change plan	Can be very time consuming if participators design an inappropriate change
Facilitation and support	Where people are resisting because of adjustment problems	No other approach works as well with adjustment problems	Can be time consuming, expensive, and still fail
Negotiation and agreement	Where someone or some group will clearly lose out because of change, and where that person/group has considerable power to resist	Sometimes it is a relatively easy way to avoid major resistance	Can be too expensive for others to negotiate for compliance
Manipulation and cooptation	Where other tactics will not work or are too expensive	It can be a relatively quick and inexpensive solution to resistance problems	Can lead to future problems if people feel manipulated
Explicit and implicit coercion	Where speed is essential, and the change initiators possess considerable power	It is speedy and can overcome any kind of resistance	Can be risky if it leaves initiators discredited

Source: *Kotter and Schlesinger, 1979*.

Organizational culture is a critical success factor in the roll out of any new initiative and TIRM will only succeed if the culture supports it. Developing the right cultural environment where TIRM could become embedded in organizational processes may be one of the biggest challenges that organizations could face. Establishing the desired organizational culture in which employees do the (right) things

expected of them is critical in terms of making the most of your TIRM initiative. Some senior managers do not always appreciate or understand the impact of organizational culture and incorrectly assume that employees will behave in particular ways. Stories about the failure of new initiatives abound, and it is often due to the absence of prioritizing the work that needs to be done to create the right cultural characteristics. Even when an organization publishes its vision, mission, and articulates its values, the right behaviors need to be reinforced if these beliefs and practices are to become reality. This must be done through the development of a culture that underpins such standards and behaviors. Integrating TIRM and ensuring everyone in the organization adheres to the standards expected is only possible by developing and maintaining the right cultural environment.



THEORETICAL EXCURSION: SCHOLARS OF ORGANIZATIONAL CULTURE

The term *culture* has its theoretical roots within social anthropology and was first introduced into the English language by Edward B. Tylor in 1871. He defined it as “that complex whole which includes knowledge, beliefs, art, morals, law customs and any other capabilities and habits acquired by man as a member of society” (Tylor, 1871). Since Tylor’s original conception of culture there have been many researchers who have built on his work and redefined his definition. In the late 1970s we began to see organizational culture and management appearing in the mainstream literature on organizational theory. Interest in organizational culture grew in the 1980s as researchers began to explore the factors underpinning Japan’s successful economic performance. Authors like Pascale and Athos (1981), Deal and Kennedy (1982), and Peters and Waterman (1982) moved attention away from national culture to organizational culture and wrote extensively about how organizations that had deeply embedded some shared values were far more successful than those that had not.

Hofstede (1980; Hofstede et al., 1990) and Trompenaars (Trompenaars and Prud’homme, 2009) are two of the leading authorities on managing organizational culture. Hofstede defines culture as ‘*mental programming*’ and Trompenaars defines it as

the pattern by which a company connects different value orientations (for instance, rules versus exceptions or a people focus versus a focus on goals) in such a way that they work together in a mutually enhancing manner. The corporate culture pattern shapes a shared identity which helps to make corporate

life meaningful for the members of the organization and contributes to their intrinsic motivation for doing the company’s work.

Another well-regarded author, Schein (1985) defines culture as

the shared values, beliefs and practices of people in the organization. It is reflected in the visible aspects of the organization, such as its mission statement and espoused values. However, culture exists at a deeper level and is embedded in the way that people act, what they expect of each other, and how they make sense of each other’s actions. Culture is rooted in the organization’s core values and assumptions; often these are not only unarticulated but so taken for granted that they are hard to articulate and invisible to organizational members.

Organizational culture is shaped by a combination of explicit and implicit messages. Johnson (1992) suggests that organizations have a cultural paradigm that defines how they view themselves and their environment. The paradigm evolves over time and shapes strategy: managers draw on frames of reference that have been built up over time and are especially important at a collective organizational level. The notion of the paradigm lies within a cultural web and is represented in Figure 13.1.

The cultural web is a tool that enables a cultural audit to be undertaken. By considering the beliefs and assumptions represented by the six outer circles, you can assess the current culture.

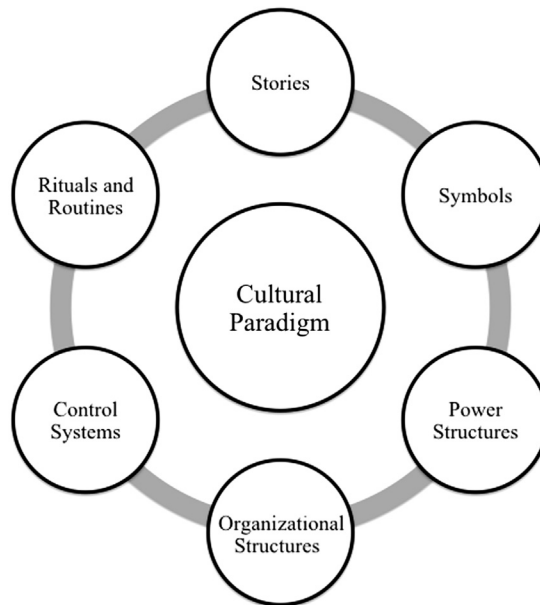


FIGURE 13.1
Cultural web.

So, how can an organization create the right culture, one that supports the wider organizational goals and risk appetite? Does the culture need to change? Changing the culture may not be a matter of discarding the existing culture and implementing a new one, but rather building on what currently supports an initiative like TIRM and fine-tuning those aspects that currently hinder TIRM's integration into day-to-day practices. An approach for a cultural change program has been proposed by Trompenaars and Prud'homme (see following box).

CORPORATE CULTURE CHANGE PROGRAM

Trompenaars and Prud'homme (2009) state that "the dilemma of change needs to be reconciled by 'dynamic stability' or 'continuity through renewal.'" Despite the pressures for achieving change, it is important to ensure the strengths of current corporate culture do not get lost. A meaningful corporate culture is a mix of existing core values and new, aspirational ones. Therefore, it is necessary to know your existing culture and what you want to retain from it before embarking on a change

project. Trompenaars and Prud'homme propose the following schedule for a corporate culture change program:

1. Assess current culture (through questionnaires, document analysis, interviews, focus groups).
2. Create input for future corporate culture and core values (including obtaining commitment from the top).

CORPORATE CULTURE CHANGE PROGRAM—cont'd

- | | |
|---|--|
| <ol style="list-style-type: none"> 3. Discuss in organization (involving people at different levels, and working on business and organizational dilemmas). 4. Finalize definition of desired culture and target corporate values (including action plan to support implementation). | <ol style="list-style-type: none"> 5. Implementation (embedding the corporate culture in processes and instruments and working on organizational/behavior change). 6. Monitor (live the corporate culture and learn from day-to-day experiences in the new culture). |
|---|--|

Having assessed the current culture, the next step is to envisage what the ideal culture should look like. Define the ideal and ensure those aspects that are required to underpin the TIRM initiative are included. Finalize the ideal state; build a picture of what the future should look like. What are the main cultural characteristics that need to be embedded within the organization? How do you want employees to behave? How do you want them to manage information risk?

- Implementation should be led from the top; involve everyone and ensure that there are open lines of communication so that there is clarity about expectations.
- Consider using “culture champions” to promote and embed new ways of working.
- Provide training, coaching, and mentoring, and help people abandon the behaviors associated with poor or inadequate risk management processes. Often the greatest challenge in changing behavior is not getting people to behave in new ways but getting them to stop behaving in established ways.
- Consider reward and recognition strategies to incentivize the right behaviors.
- Consider too what penalties or sanctions might be appropriate for behaviors that compromise risk management processes.

Do not forget to monitor the progress. Track how effectively the new culture is evolving and how it is facilitating TIRM and take corrective action if required. Changing organizational culture and embedding new ways of working and behaving will take time. It may be difficult and indeed uncomfortable but it can be done.

EMPLOYEE ENGAGEMENT IN TIRM

Employee engagement plays a significant role for the success of TIRM. Information is quite rightly seen as the lifeblood of many organizations, and it is vital that all employees see their role as one that encompasses the proper management of information risk. How then does an organization achieve this? How do all employees come to regard information risk management as an integral component of their day-to-day activities?

A report by [PriceWaterhouseCoopers \(PwC\) \(2009\)](#) suggests that there are four key steps that, if followed, will ensure that risk management (and by definition, information risk management) is part

of the daily activities of everyone in the organization. Following these four steps will help improve employee engagement.

The four key steps are:

1. Focus on personal accountability.
2. Hold your business units accountable.
3. Lead from the front.
4. Refocus your risk management function.

Focus on personal accountability

- Clarify responsibility, authority, and accountability. Before asking people to do something, make sure you have given them the authority they need to complete the task and make it clear how they will be held accountable. It is not at all unusual to see employees being asked to do something without being given the necessary resources with which to achieve those tasks. Neither is it unusual to see employees failing to understand the repercussions they could face if a task or tasks are not carried out successfully. Clear communication and a full appreciation of one's role are the keys here.
- Encourage staff to question the allocation of responsibility. Is your organization the type in which employees take responsibility for tasks even though the resources they need are not made available to them? Alternatively, is your organization one where staff shy away from taking responsibility because they are fearful of possible consequences? A free and open dialog is needed in both cases with employees knowing exactly what they are responsible for and the consequences of noncompliance.
- Watch out for blind spots. Encourage staff to speak out and challenge the status quo and the identification of any shortcomings in the risk management processes. Establish a "no-blame" culture so that employees are comfortable sharing their failures openly. This helps the organization learn quickly how to manage vulnerabilities and address risk incidents.
- Keep the door open. Invite employees to speak out if they suspect that something is wrong. You need employees to be comfortable in speaking up before a situation escalates to a position where it is not recoverable and does lasting damage to the organization.
- Reward the right behavior. Show that you value employees who behave responsibly and honestly by recognizing the contribution they make. There is a natural reticence to report errors for fear of misconduct proceedings being instigated and/or being seen as an informer. The danger is that when problems go unreported, the same mistakes get made repeatedly and are never addressed nor rectified. Reward employees who manage risks appropriately. It is unhealthy and indeed unwise to believe all risks are detrimental to the organization. The nature of business means that properly calculated risks should be taken, and where these lead to successful outcomes, employees should be rewarded. It may be that an incentive program would help ensure that the right behavior is rewarded.

Hold your business units accountable

- Make your business units measure the maturity of their risk processes. Many organizations do not manage their information risks as well as they should because the underlying risk management

processes are not well established (nor understood). Each business unit manager should assess the maturity of their risk management processes, identify any issues and shortcomings, then take steps to address these matters so that the unit (and the organization) is no longer vulnerable to risk/loss.

- Get your managers to sign on the line. Insist that business unit managers sign off on the risks they have assumed. Regular reviews should be undertaken, with action plans devised and implemented to address identified risks. There should be open lines of communication with senior management who should be made aware of any new risks that have been identified.
- Create robust controls. Each business unit should have controls in place that reflect the organization's risk appetite, taking into consideration the legal and regulatory frameworks within the industry. Remain alive as well to changes in legislation and regulatory regime.
- In the report a model for measuring the maturity of an organization's risk management process is offered as a starting point, shown in [Table 13.2](#).

Lead from the front

- Make your presence felt. Show business unit managers that the organization is serious about information risks by reviewing on a regular basis how they address information risks.
- Look at the big picture. Ask business unit managers which processes can be simplified or safely eliminated. Many large organizations have grown through mergers and acquisitions; they comprise a complex web of people, business practices, and IT systems that have never been fully integrated. This complexity may be supported by good business reasons, but it also adds to the information risks organizations face.
- Capitalize on technology. Encourage business units to adopt new tools (e.g., data-mining software, scenario-planning software) to keep track of what is happening. Most business units collect a good deal of information, and such tools can help make better sense of the data and what additional information they need to know.
- Keep things consistent. Ensure that the information each business unit gives to senior management is consistent. Different business unit managers may have different risk appetites and different perceptions of risk. A consistent reporting framework will assist here.
- Dig down to the roots. Insist that any breakdown in a core process or breach of an internal code of practice is analyzed in depth to identify the root cause and correct it. Individuals who are responsible must be held accountable.

Refocus your risk management function

- Clarify the TIRM function's role. Once the business units are in control of the risks they are taking, the risk management function can concentrate on what it should be doing—namely, providing information, advice, and assurance. Its remit should ensure that it is not continuing to assume the responsibilities the operational managers should be handling.
- Listen and learn. The TIRM function's first task is to identify and interpret any changes in the external environment including changes in the expectations of external stakeholders. Ensure that it keeps abreast of all new developments.

Table 13.2 Model for Measuring the Maturity of an Organization's Risk Management Processes

Level of Maturity	Framework	Commitment	Ownership	Processes	Communication and Training	Measurement	HR Support	Oversight
Ad-hoc	No structured approach	Risk management seen as an unnecessary expense	No interest in using risk management	No tracking of risk management	No formal risk management training	No risk assessment performed	No HR support	No standard reporting
Initial	Policy/process defined	Rules-based approach	Partially defined roles	Risk management champion drives implementation	Risk management material circulated	One-off requirements announced	New staff trained	Monitored by exception
Repeatable	Practical guidance provided	Proactive approach	Clearly defined roles	Managers drive implementation	Coordinated training provided	Repeat measurements reported	Risk management integrated into all training	Business units monitor own risks
Managed	Managers confirm compliance	Risk management embedded	Center of excellence model	Business units drive implementation	Business units drive tailored training	Risks measured consistently	Risk management ability impacts hire/promote decisions	Single view of risk across organization
Excellence	Risk management central to decision making	Risk management used for strategic advantage	Managers pursue risk unconsciously	Board and CEO drive risk agenda	Training focuses on best practice	Risk-adjusted performance measures used	Risk management seamlessly integrated into HR	Business driven with key risk indicators

- Assess and advise. The TIRM function also has a key role to play in developing an information risk framework by giving the business units feedback on the effectiveness of the controls they are using and helping them to modify those controls where necessary. The risk management function should assess how the risk management processes the business units have established are performing. What progress have they made? What gaps remain and how should they be closed?
- Tell the truth—be honest about risk; do not bury bad news. The TIRM function's final duty is to check that the business units are doing what they claim and let you know what is really happening. That, in turn, means ensuring it has sufficient authority and mandate to talk to senior management on an equal footing and challenge the existing order where necessary.
- Get it right. Putting information risk management back where it belongs—with business units and individual employees—enables the organization to create a lean information risk management function with lower overheads. More importantly, it helps to build a business that is as unsusceptible to risk as it can possibly be—that is, a business that is effective and efficient.
- Never forget the importance of culture. What is promulgated above will not succeed unless the right organizational culture is in place.

By following the four steps outlined in the report, an organization will be ensuring that accountability for information risk exists throughout the various different business units. Recognize that all employees have an important role to play, an important contribution to make, and that they are fully engaged in embedding TIRM in the organization.

SUMMARY

As with all initiatives that require a change of mindset and thinking in organizations, the introduction of the TIRM process will face organizational resistance from different stakeholders within your organization. Overcoming individual and cultural resistance is probably the biggest challenge you will face when implementing the TIRM process. This chapter presented established strategies to overcome organizational resistance and increase employee support for TIRM.

REFERENCES

- Deal, T. E., & Kennedy, A. A. (1982). *Corporate Cultures: The Rites and Rituals of Corporate Life*. Reading, MA: Addison-Wesley.
- Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-related Values*. Beverly Hills, CA: Sage Publications.
- Hofstede, G., Neuijen, B., Ohayv, D., & Sanders, G. (1990). Measuring Organizational Cultures: A Qualitative Study across Twenty Cases. *Administrative Science Quarterly*, 35, 386–396.
- Johnson, G. (1992). Managing Strategic Change—Strategy, Culture and Action. *Long Range Planning*, 25(1), 28–36.
- Kotter, J. P., & Schlesinger, L. A. (1979). Choosing Strategies for Change. *Harvard Business Review*, 57(2), 106–114.
- Pascale, R. T., & Athos, A. G. (1981). *The Art of Japanese Management*. New York: Warner.
- Peters, T. J., & Waterman, R. H. (1982). *In Search of Excellence: Lessons from America's Best-run Companies*. London: Harper and Row.
- PriceWaterhouseCoopers. (2009). *Hands Up! Who's Responsible for Risk Management?* Available at, www.pwc.com/getuptospeed.
- Schein, E. H. (1985). *Organizational Culture and Leadership*. San Francisco: Jossey Bass.
- Trompenaars, F., & Prud'homme, P. (2009). *Managing Change across Corporate Cultures*. London: Capstone.
- Taylor, E. B. 1871. Cited in Brown, A. (1998). *Organizational Culture*, 2nd ed. London: Financial Times Management.

Conclusions and Outlook

This book provides the tools for organizations to investigate and understand how poor data and information quality adversely impacts the achievement of business goals, and shows how to improve the quality of data and information assets to maximize their business value.

We started our work on TIRM in 2009, before Big Data became the huge thing it is now. Many industrial practitioners who we collaborated with approached us at that time with a similar problem: “We know that our business success depends so much on data quality, but we have such a depth of data that we don’t know where to start! How can we find out where to focus our data quality improvement efforts to create the biggest value for our business?”

We realized quickly that, to address the problem, the key would be to find a way for measuring the effect that poor data and information quality has on the business objectives of an organization. Understanding which data and information quality problems have the highest impact would give managers a tool to gear their information quality improvement programs toward real business value. It also would help managers to build a more convincing business case for information quality improvement, and to better utilize the sleeping data and information treasures that they sit on.

But why should we reinvent the wheel? The impact of an adverse event on business objectives can be best measured and managed by using risk management. Risk management is an old discipline that can offer many established concepts and, literally, hundreds of best practices, tools, and techniques. We just needed to find a way to “tap” into this wisdom by finding the right ways to integrate data and information management with the risk management discipline. Some approaches from information security served as role models.

We developed a holistic solution: the concepts, process, model, and various techniques and tools presented in this book that we summarize under the umbrella of Total Information Risk Management. TIRM has been of value in many different organizations from many industrial sectors in which it was applied as part of our research. The book has essentially been designed to progress gradually from the theory to the practice of TIRM—that is, it starts with an explanation of key concepts about data and information assets, enterprise information management, and risk management, and moves through a description of the TIRM process to examples of where the approach has been used to address real-life problems, and continues with a demonstration of how existing risk techniques can be integrated with TIRM, how to best employ software tools to automate some of the TIRM processes, and finally how to establish organizational support and employee engagement for a new initiative.

Within organizations, a good starting point for a TIRM initiative would be to get a few people to familiarize themselves with the concepts of TIRM by reading this book. In the first few chapters, we

presented some background knowledge that is a prerequisite for understanding the process. As with any change management initiative, involving key stakeholders from the beginning will help to increase engagement within the organization.

Implementing the TIRM process is done on a stage-by-stage basis. Initially, the context needs to be established; this is followed by an assessment of the information risks after which the causes of information risks are identified with appropriate (risk) treatments being selected. The treatments are chosen with due regard being given to the costs and benefits of implementation.

After implementation, the TIRM process needs to be monitored and reviewed on a regular basis. The learnings from the first cycle of any TIRM initiative should be applied to realize even greater benefits during the second cycle and so on. Throughout the process there are opportunities to integrate well-known risk management tools and techniques with TIRM as well as using software applications to automate some of the processes. Finally, as with any new initiative, you will face resistance from those who prefer the “status quo” and we encourage you to consider ways in which to overcome resistance and gain employee engagement by using the methods described in Chapter 13.

While the target audience for this book is managers with organizational responsibility for data and information quality, we also believe that those studying for professional qualifications and Master’s degrees in information studies as well as MBA students will find this book a suitable text. There has been a clear movement in postgraduate studies to provide students with material that is theoretical yet pragmatic so that theories can be easily applied in organizational contexts. We believe that this text fulfills this criterion.

Without any doubts, the era of the information worker is here and that calls for all organizations to understand what drives success in the Information Age. Having good data and information quality will help an organization to thrive in today’s fast-paced global economy. Managing information and, perhaps even more importantly, managing risks associated with information use are clearly rising to the top of many organizational agendas.

During the past few decades, information management has established itself as a key discipline in its own right and the processes we now propose in this book consider a dimension that, to the best of our knowledge, has not been widely discussed in the literature. We are seeking to help organizations not only face the risks inherent in trying to work with poor-quality data and information, but also to consider how best to manage and mitigate those risks.

A good information management strategy should be at the heart of organizational activity, not as a stand-alone initiative, but as an activity that underpins the overall business strategy and assists with the achievement of organizational goals. TIRM opens up new territory for both information management and risk management. It is therefore seen as a key component of both information strategy and risk strategy. We believe that the practices discussed in this book are applications that are worthy of pursuit for most of today’s organizations. Bringing together people from disparate parts of an organization to collaborate with each other, share their expertise and knowledge, form strong alliances, and work with similar goals in mind will surely reap success. The TIRM process provides the necessary structure to facilitate this type of effective collaboration.

In broad terms, the TIRM process represents a new way of thinking about the impact of data and information quality. We trust that it will appeal to all organizations, whatever size, in whatever sector, whether private, public, or nonprofit, and help them maximize the value of their data and information holdings. TIRM will empower organizations to find their way through the jungle of data and information and utilize them to create tangible business value and lasting competitive advantage.

Index

Note: Page numbers with “*f*” denote figures; “*t*” tables; and “*b*” boxes.

A

- Accessibility information quality category 13b
- Apple 83
- Application of TIRM
 - process 167–214
 - context, establishment of 167–172
 - information risk
 - assessment 173–202
 - information risk treatment 203–214
- Approximate string matching
 - algorithms 249, 265
- Association rule mining 259–260
- Automated methods for TIRM 237
 - information environment step, investigation of 238–244
 - information quality problems
 - identification 244–250
 - information risks, detection and treatment of 256–268
 - risk analysis tool covering stage B 250–256
- Automated track and trace technologies 262–263

B

- Big Data 4–5, 31, 33–35
- Bow-tie diagrams 232–233
- Brainstorming 83, 218–220
- Business intelligence and analytics 31–32
- Business metadata 7t, 241
- Business model 85–86, 169
- Business network processes 87b
- Business objectives 89–93, 170–171
- Business process 59–60
 - identification of 86–88
 - types of 87b
 - representatives 80b, 159–160

C

- Change management 33
- Checklists 222
- Chief risk officer (CRO) 54
- Clarification data 239–240
- Column analysis 244–246
- Communication plan 151t
- Competitive environment, investigation of 85
- Context, establishment of 167–172
 - business objectives
 - identification 170–171
 - defining the context 169
 - external environment
 - establishment 169
 - goals, defining 168
 - information
 - environment 171–172
 - information management processes 172
 - information quality issues, list of 172
- IT systems and databases 171–172
- measurement units 170–171
- motivation formulation 167–168
- organization analysis 169–170
 - business model, identification of 169
 - business processes, identification of 169–170
 - organizational culture, identification of 170
 - organizational structure, identification of 170
- potential information management and information quality issues, investigation of 172
- relevant information management processes 172

- relevant IT systems and databases 171–172
- responsibilities, defining 168–169
- risk criteria 170–171
- scope, defining 168. *See also* Stage A, of TIRM process.
- Context definition of TIRM process 81
- Contextual information quality category 13b
- Core processes 87b
- Corporate culture change program 274b–275b
- Corporate governance 163
- Cross-domain analysis 246–247
- Cultural web 274f
- Culture, defined 273b
- Customer relationship management (CRM) 36
- Customers, demands for 35–36

D

- Data and information assets 1–22
 - assessment of 14–15
 - decision making, influencing 17
 - different dimensions of 12–14
 - improvement of 15
 - life cycle of 10–11
 - organizational costs and impacts of 18–20
 - organizational success, influencing 15–20
 - poor, sources of 14
 - quality of 11–15
 - raw data’s transformation into information products 9–10
 - in 21st century 4–5
 - understanding and measuring the impact of 20
 - unique characteristics of 8–9

Data and information quality 11–12
 Data cleaning 250
 Data lineage 241–242
 Data profiling 240–241, 244
 Delphi method 221–222
 Detection algorithms 247–248
 Deterministic algorithms 248
 Domain analysis 246

E

Economic environment, investigation of 84
 English, Larry 18
 Enterprise architecture 95b
 Enterprise information management (EIM) 23–33
 Big Data 33–35
 challenges for 35–38
 burden of legacy data and systems 36
 customers becoming more demanding 35–36
 globalization as a challenge and driver for better EIM 35
 growing complexity in enterprise information architectures 36
 Internet of things 37
 leveraging it for enterprise-wide transformation 37
 movement toward analytical and fact-driven enterprise 37–38
 poor alignment of business and IT 37
 social networks and media 36
 governance 24–26
 key components for 24f
 strategy 26
 business intelligence and analytics 31–32
 change management 33
 information architecture management 28–29
 information integration management 29–30
 information process management 26–27
 information quality management (IQM) 27–28
 information security management 32–33
 master data management 30
 metadata management 30–31

 technology portfolio management 33
 relationship between TIRM and 161–162
 information governance and corporate governance 163
 information policy and implementation strategy 162–163
 specific EIM projects 164–165
 Enterprise risk management (ERM) 165
 relationship between TIRM and 165
 TIRM integration with 165
 Enterprise-wide transformation 37
 Establishing the context. *See also* Stage A, of TIRM process.
 External environment, establishment of 82–85, 169
 competitive environment, investigation of 85
 economic environment, investigation of 84
 financial environment, investigation of 84
 legal environment, investigation of 83–84
 natural environment, investigation of 84
 political environment, investigation of 83–84
 regulatory environment, investigation of 83–84
 social and cultural environment, investigation of 83
 technological environment, investigation of 84
 Extract, transform, and load (ETL) operations 30, 241

F

Failure mode effect criticality analysis (FMECA) 229–230
 Fault-tree analysis (FTA) 230–232, 232f
 Financial environment, investigating 84
 Fishbone diagrams. *See* Ishikawa diagrams
 FN curves 226–227
 Force-field analysis 88–89
 Foxconn 83
 Fuzzy matching 249

G

Geographic information system (GIS) 256–258
 Goals
 defining 168
 determination, of TIRM process 77–78
 Governance codes 163

H

Historical data, defined 7t

I

IBM 4–5
 Implementation strategy 162–163
 Incident investments process
 finalized refined model of resolve incident task in 183f
 probability and impact of each consequence in 181f–182f
 risk controls in 180f–181f
 Incident management 173–184, 174f
 affected business objectives in 179f
 analyzing tasks in each business process 173–174
 consequences in 177f–178f
 estimating likelihood and impact of each con 180–182
 examining information needed for each task 174–175
 existing risk controls, examining 180
 identifying consequences of information quality problems 177–178
 identifying for each consequence the affected business objectives 178
 identifying information quality problems during task execution 175–177
 information needs for 174f–175f
 information quality problems in 176f
 refining numbers and verifying results 182–184
 InfoRAS risk tool 250–252, 250f, 256
 Information Age 4–5
 Information architecture management 28–29

- Information environment 94–100, 171–172
 - information management and information quality issues 99–100
 - processes 96–98
 - IT systems and databases 94–96
 - Information environment step, investigation of 238–244
 - information flow
 - discovery 242–244
 - master and transactional data 238–239
 - metadata 241–242
 - reference data 239–241
 - Information flow 242
 - discovery 242–244
 - flow diagram 141f, 172f
 - for call center 98f
 - example of 96f
 - Information governance and corporate governance, relationship between 163
 - Information integration
 - management 29–30
 - Information management and information quality
 - issues 99–100
 - maturity models 97b
 - processes 96–98, 172
 - strategy 284
 - Information manufacturing system 9
 - Information policy 162–163
 - Information process
 - management 26–27
 - Information quality
 - business impacts, classification of 19t
 - dimensions 79t, 114t
 - problems 244–250
 - analyze causes of 137–140
 - column analysis 244–246
 - cross-domain analysis 246–247
 - domain analysis 246
 - identify causes of 137–138
 - lexical analysis and validation 247
 - matching algorithms 247–249
 - primary and foreign key analysis (PK/FK analysis) 247
 - rank causes of 138–140
 - semantic profiling 249
 - Information quality management (IQM) 27–28
 - Information risks 40–42
 - analysis 103
 - anatomy of 40f
 - assessment 173–202
 - incident management. *See* Incident management
 - infrastructure investments. *See* Infrastructure investments
 - new connections *see* New connections. *See also* Stage B of TIRM process.
 - case for quantifying 44–45
 - defined 39
 - evaluation 103
 - identification 103, 218–220
 - ineffective information management 41
 - lowered business process performance 42
 - management process 59–60
 - poor information quality, consequence of 41–42
 - risk management and information management 45–46
 - sources of 43
 - treatment 203–214
 - benefits of 147t
 - communicating results to stakeholders 210–211
 - costs, benefits, and risks, estimation of 146–147, 146t, 205–208
 - development 136
 - effectiveness verification 213–214
 - evaluation and selection of 136, 148–150, 209–210
 - identifying and describing 140–145, 204
 - implementation plan for 153t
 - implementation risks of 147–148, 148t
 - information quality problems, causes of 204
 - investment analysis of 149t
 - plans development 151–153, 211
 - plans implementation 153–154, 212
 - project status report for 154t
 - verifying effectiveness of 154–156. *See also* Stage C, of TIRM process.
 - upside of 44
 - ways to mitigate 43–44. *See also* Risk.
 - Information risks, detection and treatment of 256–268
 - engineering asset management (example) 256–261
 - addressing the problem for new data entering the system 258–259
 - association rule mining 259–260
 - improving the existing information 259–261
 - semantic profiling 260–261
 - managing spares and consumables (example) 261–268
 - automated track and trace technologies 262–263
 - master data
 - management 263–268
 - records, detecting and merging 264
 - standardization 264–265
- Information scrap costs 18
- Information security
 - management 32–33
- Information technology (IT) 4
- Infrastructure investments 192–202
 - affected business objectives in 197f
 - analyzing tasks in each business process 192
 - estimating likelihood and impact of each consequence 200, 200f–201f
 - evaluation and ranking 202
 - examining information needed for each task 192, 193f
 - existing risk controls, examining 198, 199f
 - identification for each consequence the affected business objectives 196–198
 - identifying consequences of information quality problems 196, 196f
 - identifying information quality problems during task execution 194
 - information quality problems in 195f
 - refining numbers and verifying results 200–202, 201f

Integrating TIRM process within organization 157–166
 Intermediate consequences, identification of 119, 125–126
 International Organization of Standards (ISO) 240
 ISO 31000 65, 157–158
 ISO.IEC 31010:2009 217–218
 “Internet of things” 37
 Interval scale 91t
 Intrinsic information quality category 13b
 IS/IT business value chain 16–17
 Ishikawa diagrams 228f
 IT systems and databases 80b, 94–96, 160, 171–172

K

Kodak 84

L

Ladley, John 25
 Large organizations, advice for 161
 Legacy data and systems, burden of 36
 Legal environment, investigating 83–84
 Lewin’s force-field analysis 88–89
 Lexical analysis 247
 LightBulbEnergy 167
 Loshin, David 18–20, 137

M

Management processes 87b
 Managing committee 160–161
 Mandatory access control 32
 Marco, David 23
 Master data 6, 7t, 238–239
 Master data management (MDM) 30, 247–248, 263–268
 architectures for 265–268
 transactional architecture 267
 Matching algorithms 247–249, 264
 Maturity models, of information management 97b
 Measurement metrics, types of 91t
 Measurement units, identifying 90–93, 170–171
 Metadata 6, 241–242
 business metadata 7t, 241
 management 30–31
 operational metadata 7t, 241
 structural metadata 241

technical metadata 7t, 241
 Monte Carlo simulation 222–223
 Motivation formulation for TIRM process 76–77, 167–168

N

Natural environment, investigation of 84
 New connections 184–190, 184f
 affected business objectives in 188f
 affected business objectives, identification of 188
 consequences in 187f
 consequences of information quality problems, identification of 185
 existing risk controls, examination of 189
 finalized refined model of the evaluate request task in 191f
 information needs for 185f
 examination of 184–185
 information quality problems in 186f
 during task execution, identification of 185
 likelihood estimation and impact of each consequence 190
 probability and impact of each consequence in 190f–191f
 refining numbers and verifying results 190
 risk controls in 189f
 tasks analysis in each business process 184
 “No-blame” culture 276
 Nominal/categorical scale 91t

O

Operational metadata 7t, 241
 Optimal asset management 167–168
 Ordinal scale 91t
 Organization analysis 85–89
 business model, identification of 85–86, 169
 business processes, identification of 86–88, 169–170
 organizational culture, identification of 88–89, 170
 organizational structure, identification of 170

Organizational culture 272–273, 273b
 changing 271–275
 identifying 88–89
 Organizational resistance, overcoming 271b–272b
 Organizational structure, identification of 88
 Organizational support, establishment of 271–275

P

Palmer, Michael 5
 Parochial self-interest 271b–272b
 Personal accountability 276
 Planned versus realized benefits 155t
 Political environment, investigation of 83–84
 Poor information quality, consequence of 41–42
 Potential information management and information quality issues, investigating 172
 Potential information risk treatment options 144t
 evaluation of 149t–150t
 identification of, 143t
 Preventive controls 232
 PriceWaterhouseCoopers (PwC) 275–276
 Primary and foreign key analysis (PK/FK analysis) 247
 Probabilistic algorithms 248–249
 Process failure costs 18
 Program implementation 161
 Program leadership 160
 Program management 160–161

Q

Quality management 11

R

Radio-frequency identification (RFID) 4, 262
 Ratio scale 92t
 Recovery preparedness 232
 Redman, Tom 18
 Reference data 6, 7t, 239–241
 Regulatory environment, investigation of 83–84
 Relationship of TIRM to EIM strategy and governance 161–162

- information governance and corporate governance 163
 - information policy and implementation strategy 162–163
 - specific EIM projects 164–165
 - Representational information quality category 13b
 - Resistance to change, methods of reducing 272t
 - Responsibilities for TIRM process, defining 168–169
 - Responsibilities identification for TIRM process 80–81
 - Rework costs 18
 - Right behavior, rewarding 276
 - Risk 48–50
 - analysis of 51, 250–256
 - assessment of 51–52
 - evaluation 51, 232
 - identification 51
 - indices 223–224
 - management 47–58, 82–83, 157–158, 217–218, 283
 - generic process 50–51
 - function 277–279
 - and information management 45–46
 - processes 278t
 - matrix 233–235
 - risk appetite 52–53
 - risk criteria 52–53, 170–171
 - defining 93
 - treatment of 53–54. *See also* Information risks.
 - Role-based access control model 32
 - Roles and responsibilities for TIRM 157–161
 - large organizations, advice for 161
 - responsible committees 160–161
 - managing committee 160–161
 - steering council 160
 - workgroups 161
 - small- and medium-size organizations, advice for 161
 - specific roles 158–160
 - business process representative 159–160
 - IT system and database representatives 160
 - TIRM process facilitators 159
 - TIRM process manager 159
 - TIRM process sponsor 159
 - Root-cause analysis (RCA) 137, 139f, 227–229
 - Rotella, Perry 5
- ## S
- Samsung 83
 - Scenario analysis 225–226
 - Scope definition of TIRM process 78–80, 168
 - Semantic profiling 249, 260–261
 - Semi-structured and structured interviews 220–221
 - Semi-structured data 7
 - Senior leadership 75b
 - Sensors 4
 - Shell Scenarios 225–226
 - Situation, assessments of 271b–272b
 - Small- and medium-size organizations, advice for 161
 - Social and cultural environment, investigating 83
 - Social networks and media 36
 - Software tools 114–115. *See also* Automated methods for TIRM.
 - Stage A, of TIRM process 73–101, 74f
 - business objectives, identification of 89–93
 - context definition of TIRM process 81
 - external environment, establishment of 82–85
 - competitive environment, investigation of 85
 - economic environment, investigation of 84
 - financial environment, investigation of 84
 - legal environment, investigation of 83–84
 - natural environment, investigation of 84
 - political environment, investigation of 83–84
 - regulatory environment, investigation of 83–84
 - social and cultural environment, investigation of 83
 - technological environment, investigation of 84
 - goals determination of TIRM process 77–78
 - implementing 75–76
 - information environment, understanding 94–100
 - information management and information quality issues 99–100
 - information management processes 96–98
 - IT systems and databases 94–96
 - measurement units, identification of 90–93
 - motivation and goals for 73
 - motivation formulation for TIRM process 76–77
 - organization analysis 85–89
 - output of 75
 - overview of 74–75
 - responsibilities identification for TIRM process 80–81
 - risk criteria, defining 93
 - scope definition of TIRM process 78–80
 - Stage B, of TIRM process 103–134
 - affected business objectives for each consequence, identification of 121
 - tasks in each business process, analysis of 105–107
 - defining tasks in business process 105–106
 - describing tasks 106–107
 - frequency of task execution, estimation of 107
 - data and information assets needed for task description of 110–112
 - identification of 108–110
 - likelihood, estimation of 112–113
 - existing risk controls, examination of 122–124
 - impact of each direct and intermediate consequence, estimation of 126–127
 - impact on business objective for each consequence, explaining 121–122
 - information quality problems, consequences of 118–120
 - description of 119–120
 - direct consequences, identification of 118–119
 - intermediate consequences, identification of 119

Stage B, of TIRM process (*Continued*)
 information quality problems
 during task execution 113–118
 identification and description 116–117
 likelihood, estimation of 117–118
 quality of data and information assets, evaluation of 113–116
 information risks
 evaluation using risk criteria 131–132
 ranking 132–133
 likelihood of each direct and intermediate consequence, estimation of 125–126
 motivation and goals for 103–104
 organizing 104–105
 output of 104
 overview of 104
 refinement of numbers and verifying results 127–128
 total risk figures for each information quality problem, calculating 129–131
 Stage C, of TIRM process 135–156, 136f
 communicating the results to stakeholders 150–151
 information quality problems
 causes analysis 137–140
 causes identification 137–138
 causes rank 138–140
 information risk treatment options
 description 144–145
 benefits estimation 147
 costs estimation 146–147
 identification of 140–144
 implementation risks
 identification 147–148

information risk treatment plans
 development of 151–153
 implementation of 153–154
 information risk treatments, effectiveness verification 154–156
 motivation and goals for 135–137
 output of 136–137
 overview of 135–136
 treatment options, evaluation and selection 148–150
 Stakeholder
 analysis of 88–89
 communicating the results to 150–151
 Standardization 264–265
 Steering council 160
 Structural metadata 241
 Structured (electronic) data 6
 Structured “what if” technique (SWIFT) 224–225
 Supporting processes 87b
 Survivorship rules 264

T

Technical metadata 7t, 241
 Techniques for TIRM 217–218, 219t
 bow-tie diagrams 232–233
 brainstorming 218–220
 checklists 222
 Delphi method 221–222
 failure mode effect criticality analysis (FMECA) 229–230
 fault-tree analysis (FTA) 230–232
 FN curves 226–227
 Monte Carlo simulation 222–223
 risk indices 223–224
 risk matrix 233–235
 root-cause analysis (RCA) 227–229
 scenario analysis 225–226
 semi-structured and structured interviews 220–221

structured “what if” technique (SWIFT) 224–225
 Technological environment, investigating 84
 Technology portfolio management 33
 Temporary data 7t
 Thorp, Jer 5
 TIRM model 68–69, 69f
 and TIRM process. *See* TIRM process
 providing estimates for 70
 quantifying information risk 65
 TIRM process 59–72, 61f
 communicating and consulting with relevant stakeholders 63
 information stakeholders, identification of 63–64
 stakeholders in stage A 64
 stakeholders in stage B 64
 stakeholders in stage C 64–65
 facilitator 80b, 159
 manager 80b, 159
 monitoring and reviewing 65
 risk appetite determination 70–71
 sponsor 80b, 159
 stages of. *See* specific entries. *See* also individual entries
 Total Data Quality Management (TDQM) 27–28
 Transactional data 6, 7t, 238–239

U

Undesired effect 230

W

Wal-Mart 4–5
 “Warehouse” field 249
 Workgroups 161