INTERNAL AUDIT AND IT AUDIT SERIES

Implementing Cybersecurity

A Guide to the National Institute of Standards and Technology Risk Management Framework

Anne Kohnke • Ken Sigler • Dan Shoemaker

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Implementing Cybersecurity

Internal Audit and IT Audit

Series Editor: Dan Swanson

A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)
Dan Shoemaker, Anne Kohnke, and Ken Sigler
ISBN 978-1-4987-3996-2

A Practical Guide to Performing Fraud Risk Assessments
Mary Breslin
ISBN 978-1-4987-4251-1

Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program
Sean Lyons
ISBN 978-1-4987-4228-3

Data Analytics for Internal Auditors
Richard E. Cascarino
ISBN 978-1-4987-3714-2

Fighting Corruption in a Global Marketplace: How Culture, Geography, Language and Economics Impact Audit and Fraud Investigations around the World
Mary Breslin
ISBN 978-1-4987-3733-3

Investigations and the CAE: The Design and Maintenance of an Investigative Function within Internal Audit
Kevin L. Sisemore
ISBN 978-1-4987-4411-9

Internal Audit Practice from A to Z
Patrick Onwura Nzechukwu
ISBN 978-1-4987-4205-4

Leading the Internal Audit Function
Lynn Fountain
ISBN 978-1-4987-3042-6

Mastering the Five Tiers of Audit Competency: The Essence of Effective Auditing
Ann Butera
ISBN 978-1-4987-3849-1

Operational Assessment of IT
Steve Katzman
ISBN 978-1-4987-3768-5

Operational Auditing: Principles and Techniques for a Changing World
Hernan Murdock
ISBN 978-1-4987-4639-7

Securing an IT Organization through Governance,
Risk Management, and Audit
Ken E. Sigler and James L. Rainey, III
ISBN 978-1-4987-3731-9

Security and Auditing of Smart Devices: Managing Proliferation of
Confidential Data on Corporate and BYOD Devices
Sajay Rai and Philip Chuckwuma
ISBN 978-1-4987-3883-5

Software Quality Assurance: Integrating Testing, Security, and Audit
Abu Sayed Mahfuz
ISBN 978-1-4987-3553-7

The Complete Guide to Cybersecurity Risks and Controls
Anne Kohnke, Dan Shoemaker, and Ken E. Sigler
ISBN 978-1-4987-4054-8

Tracking the Digital Footprint of Breaches
James Bone
ISBN 978-1-4987-4981-7

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Implementing Cybersecurity

A Guide to the National Institute of Standards and Technology Risk Management Framework

By
Anne Kohnke, Ken Sigler, and Dan Shoemaker

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20170131

International Standard Book Number-13: 978-1-4987-8514-3 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Foreword

Effective risk management is at the heart of good cybersecurity practice. Adopting a risk-based approach allows managers to assess the relative strengths and weaknesses of different security decisions within the context of a complex operational environment where a maze of laws, policies, and directives, along with an evolving threat landscape, can stymie even the most experienced professionals.

In an emerging area like cybersecurity, where various governments and professional entities are racing to establish protocols of professional practice, standards—such as the National Institute of Standards and Technology (NIST) Risk Management Framework detailed in this book—can assist security professionals in navigating through the challenging environment. As I have observed through my years of identifying, developing, and implementing cybersecurity best practices, when done right, standards provide a common foundation upon which practitioners can build holistic security operations. Standard frameworks offer a structure to support the full range of activities needed to secure enterprise operations. Standards also define common terminology used to support communication within single organizations and collaboration across multiple entities. Through these frameworks, practitioners can improve the efficiency of critical processes and system integration activities. By identifying a clear set of desired outcomes for security operations and the methods needed to measure progress toward meeting those goals, standards can support the assessment of security tools, services, and practices.

While consistency is a desirable state, the role of standards is not to establish uniformity. On the contrary, properly articulated standards should not lead to monolithic structures. Rather, proper standards support the application of coordinated strategies by providing a roadmap to guide organizations toward areas of alignment and by allowing for enough flexibility that individual entities can adapt internal practices to meet specific environmental constraints. The importance of having both alignment and flexibility cannot be overstated, which is critical to establishing the resilience needed as organizations face a dynamic threat environment. To ensure that standard frameworks meet both of these objectives, the development process must be conducted at a time when the core knowledge of the field has developed sufficiently to serve as a stable foundation. In addition, the data gathering process should be broadly inclusive of stakeholders across the spectrum.

Public agencies and private business of all sizes and across sectors, ranging from critical infrastructure to entertainment, should be included in the requirements gathering phase. The synthesis of these disparate inputs should be no less comprehensive and must be performed with rigorous analysis and objective processes. This is setting a high bar—one that the NIST Risk Management Framework has met. The framework was developed through 4 years of intensive and coordinated efforts to gather and synthesize expert advice. The resulting framework provides a practical, easily applicable, and understandable approach to the management of risk in any organization. As such, it serves as a valuable resource for those charged with securing the enterprise.

This book provides general guidance on applying the NIST Risk Management Framework. The text walks the readers through the central concepts, relationships between steps, and general recommendations for application across a variety of organizational types. The authors have vast experience in translating federal cybersecurity standards for both the lay reader and the seasoned professional. As with their prior efforts, see *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*, the authors construct a detailed picture that will bolster the reader's ability to use the standards. Structured as a common sense guide that addresses each component of the Risk Management Framework, managers ranging from strategic to operational levels will gain practical insights from this book.

Diana L. Burley, PhD
Professor, Human and Organizational Learning
Executive Director, Institute for Information Infrastructure Protection
The George Washington University

Preface

This book will help the reader to understand and apply the federal risk management framework (RMF). The RMF was developed and promulgated by the National Institute of Standards and Technology (NIST) in 2014. Its aim is to define a detailed and practical end-to-end process and provide an explicit methodology to manage the risk to information and communication technology (ICT) systems. The RMF is specifically oriented toward the compliance requirements of the 2002 Federal Information Security Management Act (FISMA). Thus, it provides a strategy and operational steps for installing the controls called out by Federal Information Processing Standards (FIPS) 199 and 200. The controls themselves are specified in NIST SP 800-53, Revision 4. Given the comprehensive risk management focus of the NIST RMF, the recommendations that are contained in this book will support any form of organizational risk management process.

Using the NIST RMF, it is possible for an entity to define and implement persistent day-to-day organization-wide policy–based strategic risk management control over its operations. So, the attendant stages and associated specifications of the model comprise a collection of commonly accepted, practical, and easy to implement steps to ensure systematic risk management. Thus, the NIST RMF can be seen as the detailed roadmap for implementing practical risk management in any setting. More importantly, the real-world realization of the NIST RMF's recommendations can also establish coordinated risk management across a range of organizations, which will help to ensure a robust and properly coordinated approach to the overall problem of risk management nationally.

In addition to the overall architecture of the substantive risk management process, this model also specifies an approach for creating the control set. These controls are necessary to ensure best-practice risk mitigation. The contextual control framework generated by the standard underwrites the comprehensive risk management program and it will mitigate and manage organizational risk specifically as it applies to information.

The NIST RMF framework is generally considered to be authoritative because it was prepared through a broadly inclusive, 7-year, highly rigorous process spearheaded by the federal government through NIST. However, it involved a number of other constituencies including industry and academia. The ability to put the general shape of the risk management process into an explicit and commonly accepted frame of reference underwrites the practical management of across-the-board risk. Additionally, it underwrites the standardization of the risk management process throughout all sectors of the economy.

Why the NIST RMF Is Important

The NIST RMF is a key component of the general compliance requirements of the Federal Information Management Act (2002). The aim of the NIST RMF project was to develop a strategic, risk-based approach to the deployment of real-world cybersecurity controls, which are appropriate to address latent and active risks within a given ICT situation. As a result, the NIST RMF comprises a major national influence on the overall state of cybersecurity practice. In addition to the effectiveness of its general application, the NIST RMF is the first fully sanctioned specification of a complete cybersecurity risk management process.

Comprehensive risk management is a key element in the planning, design, and implementation of any organization's operational cybersecurity program—not just that of the federal government's. This is because the unequivocal understanding of the risk environment serves as the starting point for the selection of an appropriate set of corporate security behaviors. These behaviors are always needed to protect the users and the information assets of any ICT system.

Given its intended national role, the NIST RMF initiative is understandably very ambitious in scope. To provide a comprehensive demonstration of the recommendations of the framework, we have adopted a presentation model that is based around discussions of how to embed each of the standard elements of the NIST RMF process in a tailored cybersecurity risk management process for any organization. Accordingly, this text will focus on *how* the relevant aspects of risk management will interact together to ensure suitable control selection in a practical setting.

Practical Benefits of Implementing the Risk Management Model

The NIST RMF provides a carefully researched specification of each element of the risk management process. It embodies the steps required to identify and evaluate cybersecurity risk. Thus, the time and effort that NIST expended in developing the framework comprises an all-source picture of the accepted principles of the practice of risk management. And as such cybersecurity risk management practice can be improved by building a detailed picture of the NIST RMF process and tailoring it to a specific setting. The level of detail that NIST provided for each of the steps in the RMF implementation process makes it possible to structure either a single tailored application for a given setting or an entire organization-wide strategic framework. Thus using the NIST RMF, managers and even academics can be brought to a common understanding of risk management.

The government-wide scope of the NIST RMF is necessary because compliance with information assurance best practice is mandated for all governmental entities by law. So in essence, this is a survey book. It will provide the complete strategic understanding requisite to allow a person to create and use the NIST RMF process along with recommendations for risk management. This will be the case both for applications of the NIST RMF in practical corporate situations, as well as for any individual who wants to obtain specialized knowledge in organizational risk management.

The NIST RMF is by necessity generally applicable, and therefore an initial all-in-one book seems like the most practical way to introduce the concepts of the model. In effect, what we are providing is an end-to-end explication of the six primary stages of the process. In each stage, we will introduce the central concepts and the underlying relationships with each of the steps in the prior stages, and itemize the standard process performance and task recommendations for each step. The focus of this book is to explain how to use the framework in a general organizational application rather than illustrate how it applies in an explicit sector.

Who Should Read This Book

The knowledge that is contained in this book would support managers at both the strategic as well as the project management level. It would also help to ensure specific control compliance in support of the FISMA requirements. FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger–Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security.

The management responsibilities presume that responsible executives understand the risks and other factors that could adversely affect their organization's mission. Moreover, these managers must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems and must be guided by informed judgments that appropriately mitigate risk to an acceptable level.

This book is designed to give the reader a comprehensive understanding of the risk management process for all organizations. Its recommendations are relevant to every type of organization and the recommended approach must be tailored to the application. Nevertheless, it is recommended that tailoring should take place within a common framework. Therefore, the NIST RMF is also potentially applicable to risk management in all corporate settings. Thus, this book can serve as a roadmap of sorts, aimed at the practical understanding and implementation of the risk management process as an ordinary entity in the business process.

NIST is authoritative, both in the standard knowledge requirements that it specifies, as well as in terms of the definition of the specific elements of the organizational risk management process for a particular organizational application. This book is a comprehensive explication of the topic of risk management and it will allow a person to understand the application and uses of the RMF content. This also holds true for application of this book in education and training situations. The people who would benefit from this knowledge range from managers to all types of technical workers and specialists.

Organization of This Text

The chapters follow the model in a logical fashion. Some of the content of these chapters touch on concepts that are brand new; however, the general structure and approach of this model have been well established over time. And because of the extensive vetting process that was conducted by NIST in its preparation, the correctness of the approach is difficult to question. Accordingly, this book is based on nine chapters and an appendix.

Chapter 1: Introduction to Organizational Security Risk Management

This chapter presents an overview of organizational risk management through an exploration of the types of organizational risks that senior leaders must identify, the necessity and benefits of managing those risks, and the information security regulation that senior leaders must consider as they manage risk. The discussion continues with an overview of security risk management. Finally, the chapter provides an introduction to the NIST RMF.

Chapter 2: Survey of Existing Risk Management Models

This chapter briefly breaks away from the main objective of the book in order to discuss various models that can be used to implement the NIST RMF. The goal is to provide a comparative assessment of existing models and demonstrate how the NIST framework sets itself apart from other models. The models discussed include: ISO 13335, *Information Technology—Security; Techniques—Management of Information and Communications Technology Security*; HITRUST, AS/NZS, ISO 31000:2009, *Standard: Risk Management—Principles and Guidelines*; and NIST SP 800-30, *Guide for Conducting Risk Assessments*, and NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* This discussion will serve as the basis for the ideas that will be presented in the next seven chapters.

Chapter 3: Step 1—Categorize Information and Information Systems

This chapter begins with a definition of security impact analysis. CNSSI 1253 *Security Categorization and Control Selection for National Security Systems* and FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* are explored, compared, and contrasted as a source of guidelines for organizations to perform the information system categorization process. The major focus of this chapter centers around understanding the tables available in NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems*; the security categories; and utilizing FIPS 199 as a means of implementing the security categorization; and the information classification process of the NIST RMF.

Chapter 4: Step 2—Select Security Controls

This chapter begins with an introduction of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. Further, this guideline is used to provide a basis for discussion of establishing security boundaries and the identification of minimum security requirements. This chapter also provides a discussion related to the contents of the security plan, and continuous monitoring strategy (which are two of the underlying outputs of the control selection process).

Chapter 5: Step 3—Implement Security Controls

This chapter starts with a review of the system development life cycle (SDLC) using ISO 12207:2008 as a basis for discussion of when activities and tasks associated with security control implementation get performed. Emphasis is placed on the standards development and acquisition processes as a means for providing details related to the development of an organizational information security architecture while at the same time integrating it into the organization's enterprise architecture.

Detailed discussion is also provided about the types of security controls (i.e., common, hybrid) together with the proper approaches to allocation of each type. This chapter concludes with a discussion of the proper procedures for documenting control implementation at the functional level and within the existing security plan.

Chapter 6: Step 4—Assess Security Controls

This chapter begins by using NIST 800-30, *Guide for Conducting Risk Assessments*, as a directive for a discussion of the process of security risk assessment. Through this discussion, the reader will understand that security risk assessment and security control assessment are not only different processes but also complimentary in nature. The major focus of this chapter is on how to use NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and*

Organizations—Building Effective Assessment Plans. This serves as a basis for discussing the approach toward development of a security control assessment plan. An underlying objective of this chapter is to demonstrate that through security control assessment based on an established plan, the reader will be able to identify and further disclose security risks that may exist within the organization.

Chapter 7: Step 5—Authorize Information Systems

The first major component of this chapter provides a detailed discussion of the creation and dissemination of the security authorization package (security plan, security assessment report, and plan of action and milestones). This chapter begins with a discussion of the criteria included and creation of a plan of action and milestones. The reader will appreciate that the plan provides the strategies for how the organization will correct security weaknesses or deficiencies identified through security control assessment. The second major component that is discussed is the use of NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, as a basis for risk determination and risk acceptance.

Chapter 8: Step 6—Monitor Security State

This chapter starts by using ISO 12207:2008 as a basis for discussion of the operations and maintenance phases of the SDLC. The thrust of this discussion is on the activities associated with monitoring the security state during these two life cycle phases.

This chapter emphasizes the strategies associated with the ongoing security control assessments, remediation action strategies, procedures for implementing documentation and plan updates, implementing security status reporting procedures, strategies associated with ongoing risk determination and acceptance, and secure procedures for information system removal and decommission.

Chapter 9: Practical Application of the NIST RMF

This chapter provides specific examples of the implementation process for small-, medium-, and large-scale organizational applications. This is in the form of case studies that will be presented as model representations of the practical advantages and pitfalls of implementing the RMF as an end-to-end process. The aim of this final chapter is to give readers a concrete understanding of the real-world issues associated with enterprise risk management, as well as to suggest pragmatic strategies for implementation of the RMF within a range of settings.

Appendix: (ISC)^2 Certified Authorization Professional (CAP) Certification

The discussions that take place within this book have a direct relationship to the five domains of the (ISC)^2 CAP certification. The appendix will provide a brief introduction to (ISC)^2 followed by a discussion of the CAP domains, the value of this certification, its relationship to DoD 8570 standard, and the requirements to obtain certification for Information Assurance Manager Levels I and II.

Authors

Anne Kohnke, PhD, is an assistant professor of IT at Lawrence Technological University, Southfield, Michigan, and teaches courses in both the information technology and organization development/change management disciplines at the bachelor through doctorate levels. Anne started as an adjunct professor in 2002 and joined the faculty full time in 2011. Her research focus is in the areas of cybersecurity, risk management, and IT governance. Anne started her IT career in the mid-1980s on a help desk, and over the years developed technical proficiency as a database administrator, network administrator, systems analyst, and technical project manager. After a decade, Anne was promoted to management and worked as an IT Director, Vice President of IT, and Chief Information Security Officer (CISO). Anne earned her PhD from Benedictine University, Lisle, Illinois.

Ken Sigler is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills campus of Oakland Community College in Michigan. His primary research is in the areas of software management, software assurance, and cloud computing. He developed the college's CIS program option entitled "Information Technologies for Homeland Security." Until 2007, Ken served as the liaison between the college and the International Cybersecurity Education Coalition (ICSEC), of which he is one of three founding members. Ken is a member of IEEE, the Distributed Management Task Force (DMTF), and the Association for Information Systems (AIS).

Dan Shoemaker, PhD, is the principal investigator and a senior research scientist at the University of Detroit Mercy's (UDM) Center for Cyber Security and Intelligence Studies in Detroit, Michigan. Dan has served for 30 years as a professor at UDM with 25 of those years as department chair. He served as a cochair for both the Workforce Training and Education and the Software and Supply Chain Assurance Initiatives for the Department of Homeland Security, and was a subject matter expert for NICE Workforce Framework 2.0. Dan has coauthored six books in the field of cybersecurity and has authored over one hundred journal publications. Dan earned his PhD from the University of Michigan, Ann Arbor, Michigan.

Chapter 1

Introduction to Organizational Security Risk Management

At the conclusion of this chapter, the reader will understand:

- The role and importance of risk management in the cybersecurity process
- The issues associated with risk and generic risk management
- The form and content of the risk management process
- The general structure and intent of risk-oriented frameworks
- The general application and development of a risk-based strategy
- The generic elements of the risk management process

1.1 Introduction to the Book

The goal of this book is to provide a comprehensive understanding of the strategic risk management process as well as the underlying principles and a standard risk management framework. Risk management entails a formal set of steps that are carried out to protect an organization's assets from harm that may be caused by inadvertent or deliberate acts of destruction. Risk management involves a systematic architecture comprising all the necessary controls to prevent unauthorized use, loss, damage, disclosure, or modification of organizational information. Specifically, this chapter discusses the formal processes for identifying, managing, and mitigating risk as prescribed by the National Institute of Standards and Technology's (NIST) risk management framework (RMF). In this chapter, we also discuss the general uses for the framework and the contexts in which it applies.

In some respects, this book is as much about standardization as it is about risk management. Hence, Chapters 2 and 3 present an overview of the role of the standardization process in ensuring a consistent response to a given issue of importance. This includes a discussion of why information assets are difficult to protect as well as the part in which commonly acknowledged best practices apply in ensuring an informed response. The discussion will also center on how to use the NIST's RMF as a standard means of deploying an appropriate set of information technology security controls. We lay out the issues involved in implementing a standard process, including the benefits that derive from it, as well as potential pitfalls. We also try to give you an understanding of the implementation process, which is best demonstrated by applying the RMF to a specific context.

1.2 Risk Is Inevitable

Risk is a fundamental element of human life in the sense that risk is always a factor in any situation where the outcome is not precisely known (Figure 1.1). In addition, the necessary calculations that we make about the probability of some form of harm resulting from an action that we take are generally a given in our decision processes. Whether the risk assessment involves decisions about a major corporate

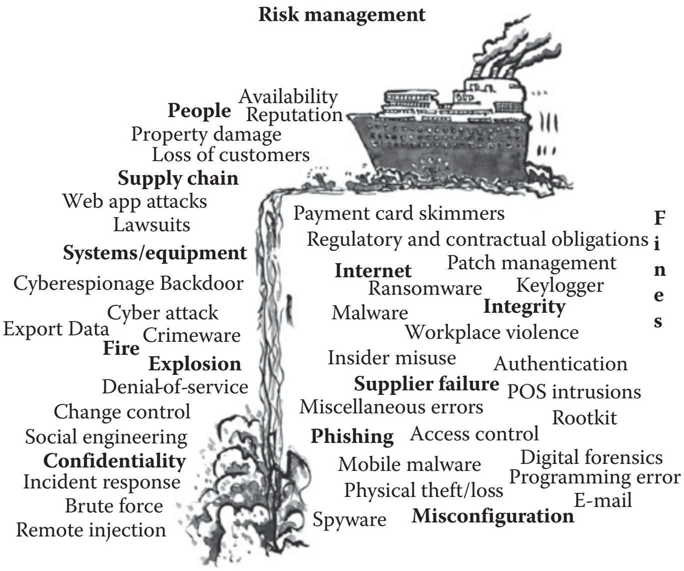

Figure 1.1 Security risk management.

initiative or just making the decision to walk down the street, we are always anticipating, identifying, and evaluating the potential risks involved. In that respect, we can be said to be constantly managing risk in everything we do.

The reason why risk management is a particularly important aspect of the cybersecurity body of knowledge (BOK) is that information and communication technology (ICT) and information assets are more difficult to account for and control than most conventional physical assets, because ICT involves the production and management of virtual, highly dynamic products, which makes it difficult to identify what to secure, let alone how to do it. That puts risk management center stage in the consideration of how to establish and maintain a secure ICT environment.

By definition, ICT assets are something of value to the business. The risk management process specifically ensures the assurance of three generic protection criteria, as shown in Figure 1.2. These three criteria assure against meaningful loss of *confidentiality*, loss of *integrity*, and loss of *availability* (CIA).

From a security standpoint, the most logical generic criterion might be assurance against a loss of confidentiality. *Confidentiality* is a security principle that encompasses an organization's requirement to restrict access to any sensitive information or data that it keeps. Obviously, if the organization's data and information could be made public without risk, there would not be a need for this attribute; however, this is rarely the case.

From an operational point of view, confidentiality is founded on establishing and adequately enforcing access control. Data and information are essential to the business operation. And in many information-intensive organizations, it might be the only real asset that is kept. For instance, most financial data within a company is sensitive and

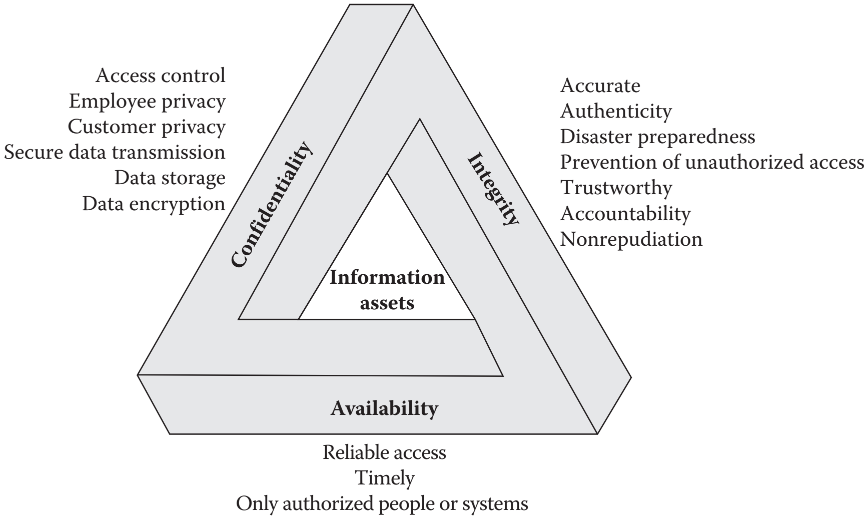

Figure 1.2 The confidentiality, integrity, and availability (CIA) triad.

access is almost always rigorously safeguarded. So, one way to view the monetary value of confidentiality is to imagine how much competitors might pay to have access to the data and information of a company or the cost of litigation if a legal requirement was violated. Thus, in that respect, the organization has a legal and ethical requirement to protect its sensitive business information as well as employee and customer privacy.

The second characteristic is *integrity*. The integrity of data or its attended processes is determined based on how authentic, accurate, and complete the data is. It is easy to appreciate the value of integrity in the context of financial business transactions. For example, if a bank could not depend on its account balances, it could potentially sustain a large loss by disbursing checks not covered by actual funds. In an inventory system, there is the potential to lose expensive materials if the counts were inaccurate due to faulty data. Or publically, the release of unreliable data that is used as background for a damaging story might expose a newspaper to legal action.

The third characteristic, *availability*, ensures that information is provided to an authorized user when it is required. The best way to understand the value of availability is to ask, "What would happen if the information was not available to support a given action or decision?" For example, what would happen if the business' payroll data were erased on payday? If the payroll program were suddenly inoperative, no one in the organization would be paid as expected. Imagine the chaos in a company the size of General Motors or IBM if they were unable to pay their employees or suppliers when they needed to. Given the potential harm that each of these principles might represent, all of the meaningful risks in each of these areas must be rationally managed.

Because every organization is unique and implements security differently, the actual process to identify, evaluate, and ensure that the meaningful risks in each of the CIA areas are properly managed generally involves the same eight requirements, which are as follows (Figure 1.3):

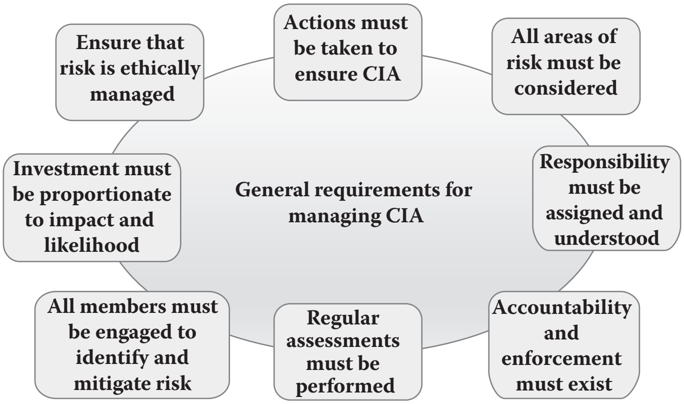
Actions must be taken to ensure CIA
All areas of risk must be considered
Responsibility must be assigned and understood
Accountability and enforcement must exist
Regular assessments must be performed
All members must be engaged to identify and mitigate risk
Investment must be proportionate to impact and likelihood
Ensure that risk is ethically managed
General requirements for managing CIA

Figure 1.3 General requirements for meaningfully managing CIA.

1. Identifiable actions must be taken to ensure correct, confidential, and available information.
2. All relevant areas of risk must be considered in any given solution.
3. The responsibility for risk management must be explicitly assigned to individuals and understood.
4. A system of accountability and enforcement for risk control must exist and be documented.
5. Regular and systematic assessments of risk status must be performed.
6. All members of the organization must understand the importance of and work to identify and mitigate risk.
7. Investment in risk management must be kept proportionate to the impact and likelihood of the risk occurrence.
8. The organization must ensure that risk is ethically managed.

In practice, organizations should design, implement, and follow a systematic process to establish a persistent operational risk management process. This design and management process is a strategic activity in that it involves short- and long-range considerations. Thus, planning for strategic risk management is necessary in order to ensure continuous risk assurance. And a formal strategic planning process is necessary to implement an organization-wide risk management process. Risk management itself must incorporate all of the elements of the business within its scope and the process should reach to the boundaries of the organization.

The outcome of the implementation of a risk management process is a concrete organization-wide risk management scheme that is documented. The risk management scheme will balance the aims of a long-term risk control policy with real-world conditions and constraints. The atomic-level components of the risk management process are a set of substantive security controls that ensure the requisite level of assurance against loss. These security controls should be traceable directly to the individual policies that defined their need. This is a closed-loop process in that the ongoing alignment of risk security controls to individual policies fine-tunes the evolution of the substantive risk management process and ensures its effectiveness in the operational setting.

One problem is that the term "risk management" is rather nebulous. So, the overall process itself requires a definition of what risk management means. A concise statement and commitment to the work is needed in order to make the practice standard. Standardization is important because a lack of effective, coordinated implementation and execution of the process has made overall risk management efforts ineffective. Worse yet, employees might feel the effort is the "flavor of the day" and not take it seriously. One does not need to look any further than the increasing number of incidents in cyberspace to confirm that.

The lack of coordinated action has been so pervasive that a logical response is the formulation of a comprehensive and coherent specification of the commonly accepted best practices for risk management. The specification could then be used to guide the creation of an effective risk management scheme for all organizations. In that respect, steps were taken by the federal government to formally research and develop a standard and comprehensive risk management process.

The specification of commonly accepted standard processes is the role of the NIST, the U.S. government's standards making body. Of specific interest here, the NIST has developed and published a formal reference model for the management of risk simply called the RMF, as shown in Figure 1.4.

This large-scale standard model serves as both the specification of a fundamental process for understanding the risks involved in assuring information and ICT organizations and the foundation for deploying the common control mechanisms required to manage the risks that exist within them. It has the additional advantage of providing the umbrella definition of the processes for achieving Federal Information Security Management Act (FISMA) and NIST certifications.

An important justification for this standard is that the RMF also defines the basis for a comprehensive strategic governance approach to risk. A governance rather than a technical approach is a highly advantageous strategy because, notwithstanding the issue of whether the cybersecurity function itself can ever fully embrace all of the issues associated with assurance, a governance-based solution is more easily understood and acceptable to the managers and nontechnical people who comprise the majority of the organization.

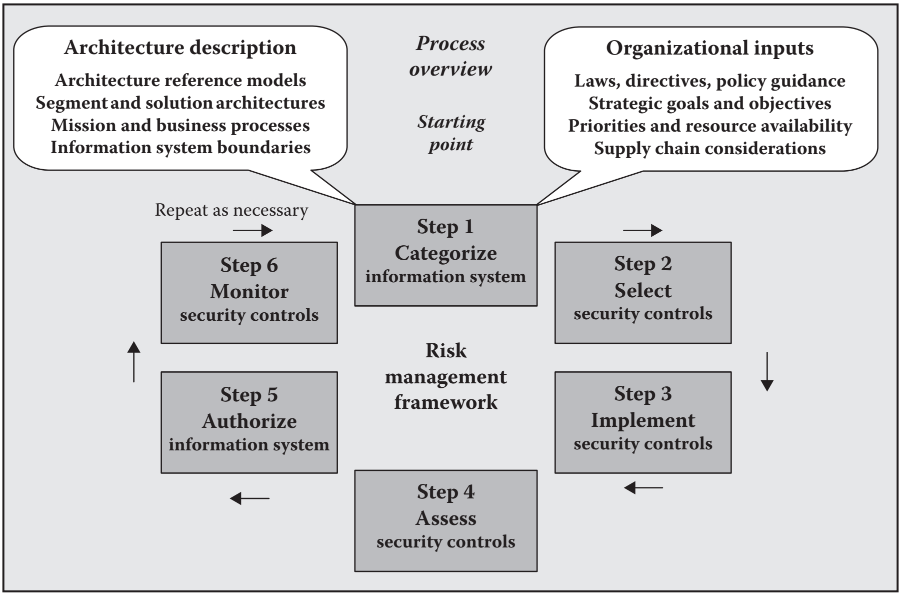
Architecture description
Architecture reference models
Segment and solution architectures
Mission and business processes
Information system boundaries
Process overview
Starting point
Organizational inputs
Laws, directives, policy guidance
Strategic goals and objectives
Priorities and resource availability
Supply chain considerations
Repeat as necessary
Step 1 Categorize information system
Step 2 Select security controls
Step 3 Implement security controls
Step 4 Assess security controls
Step 5 Authorize information system
Step 6 Monitor security controls
Risk management framework

Figure 1.4 The National Institute of Standards and Technology's risk management process overview.

A governance approach is appropriate for any organizational setting. In essence, a generic governance model constitutes a flexible top-down organizational process for establishing persistent risk management actions and the formal selection and maintenance of appropriate security controls. Moreover, since the RMF is founded on an established policy and procedure approach, it is able to capture and communicate the nature of the specific risks that an organization may encounter. And finally, since the framework itself is built and maintained through a comprehensive identification and assessment process, it can assist in rationally and systematically identifying changes in the threat environment as they occur.

1.3 Strategic Governance and Risk Management

Starting from the assumption that a standardized risk management process should be applied organization-wide (which is what we believe), risk management is a strategic issue, rather than a narrow technical concern. The reason to adopt an organization-wide risk management approach is to avoid the dysfunctional effects of a typical piecemeal solution where every department is managed by its own commonly accepted business practices. These are often based on an individual unit or manager's ideas about the proper way to accomplish a particular organizational goal. And regardless of whether they are universally standard or documented, these become the corporate way of doing business. One problem is that those approaches are often not coordinated effectively in the operational environment. In some cases, they can actually cause dysfunctional conflicts. And corporate risk management has often evolved this way. Organizations develop specific one-at-a-time responses as risks present themselves, rather than addressing them by employing a single, coordinated management strategy. Moreover, as new risks appear in the corporate threatscape that have not been seen before, they are not incorporated into any specific management techniques that the organization employs to mitigate and contain them.

The alternative approach to piecemeal risk management is a formally defined and instantiated architecture of comprehensive risk management best practices, which are specifically aimed at optimizing risk controls within the company. As with any complex system, formal risk management practice can only be implemented through a rational and explicit planning process. The planning activity fits the strategic purposes and responsibilities of standards-based risk management to the security needs of the organization. From the standpoint of the rest of this text, it is the creation of that strategic risk management capability, which the RMF leverages, that will drive the presentation and discussion of the framework.

Risk management is basically built around information. In effect, risk management gathers and utilizes information from all sources, in order to decrease the possibility of future risks. The information-gathering activity is aided by a set of formal processes and technologies. And, at its core a successful risk management function relies on the ability to assure that the processes, practices, knowledge, and skills of risk management are incorporated as quickly and efficiently as possible into the organization's substantive decision-making processes.

In addition to providing the information that helps guide strategic decision-making about risks, the risk management process also makes certain that a commonly accepted and systematic set of policies and procedures are in place to handle known risks. That responsibility is operationalized through a standard set of operating procedures. Those procedures ensure that the risk planning, analysis, response, and process management function are always directly aligned to the goals of the business operation. Nevertheless, the primary purpose of risk management is to ensure a disciplined and systematic response to the risks that the organization considers a priority.

1.4 Elements of Risk Management

In simple terms, the risk management process assesses the likelihood that any given action will adversely impact something of value to any given entity. That includes things of personal value such as money, health, or even life. Once those risks are known, the risk management process deploys all of the measures that are necessary to ensure that consequent harm does not occur.

Some organizations manage risk in a highly quantified and data-driven way, for example, corporations that require high levels of integrity in their products as well as the segments of the critical infrastructure where the potential failure of a crucial system could result in a set of highly unwelcome consequences. Others tend to spend less on risk management and spending levels are influenced by the nature of the threat environment and the value and sensitivity of the assets that are being protected.

Because identification and understanding are such important aspects of risk management, assessment provides the fundamental focus of the process. Risk management is operationalized by a continuous process of assessing the organizational environment aimed at identifying and understanding all of the potential threats and the negative impacts that might affect the business. Once these have been identified and characterized, specific steps are then devised and implemented to mitigate any adverse outcomes.

Given its focus on the support of substantive decision-making, an important underlying factor in risk evaluation is the uncertainty principle. Uncertainty is a key element in assessing threats because risk entails future consequences. In essence, the outcomes of any given threat have to be fully understood in order for an intelligent decision to be made about the way forward in addressing it. However, there are usually a number of unknown, and therefore unevaluated, factors that might be associated with a given threat. Thus, the institution of standard and persistent identification, understanding, and response practices becomes an important element in the risk management process.

It goes without saying that it is easier to identify and evaluate risk in less complex environments. Yet, every aspect of cyberspace is abstract and complex. Therefore, risk management for cybersecurity requires a much different approach to the understanding and evaluation of risk. The process in the virtual world has to touch on factors than would normally not be part of the decision-making processes in the conventional physical world—such as how to authorize the acceptance of an invisible product. Accordingly, the sheer virtuality of ICT environments alone poses a threat.

The issue of threat management is important to our existence as a nation because ICT is the platform on which our modern society rests. Consequently, the huge increase in the number of strategic threats to computers and networks is a compelling danger to our modern way of life. The generic areas of threat have been variously categorized into terms such as "cyber-crime," cyber-terrorism, and "cyber-war." And in response to all of this turmoil, the past 15 years have witnessed the creation and evolution of a specialized new profession that is dedicated to addressing the many novel risks of the virtual world. The aim of that profession is to assure that ICT systems and the information that they contain, process, and communicate are protected against all logical forms of unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction. That profession is presently termed "cybersecurity."

Cybersecurity evolved out of the practices and procedures of the older discipline of information assurance. One aspect of the original discipline was the responsibility to manage all risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Cybersecurity incorporates a holistic approach to protection in that all aspects of risk mitigation in virtual and physical space have to be included in the protection scheme. This includes the creation and deployment of a complete and appropriate set of electronic and behavioral countermeasures.

This requirement is not simply a computer science challenge. It requires knowledge and practices from a wide range of traditional security fields, such as continuity management, forensics, audit, management science, software, and systems engineering, and even fields such as law and criminology. Consequently, what is required to manage cybersecurity risks is a complete and provably effective framework that ensures the proper coordination and use of all appropriate methods in the execution of the process. The framework should be expected to consolidate provably correct approaches into a single logical and coherent model of operation. The model contains all of the commonly accepted security best practices necessary to provide effective mitigation and management of all known risks to individuals, operations, and assets of the organization.

The key concept is "commonly accepted." A commonly accepted model of best practice establishes a standard point of reference. A unified vision is necessary to establish coordinated actions in the management of risk. Comprehensive coordination is a necessity because *all* potential risks must be identified, assessed, and