INTERNAL AUDIT AND IT AUDIT SERIES

Securing an IT Organization through Governance, Risk Management, and Audit

Ken Sigler • Dr. James L. Rainey, III

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Securing an IT Organization through Governance, Risk Management, and Audit

Internal Audit and IT Audit

Series Editor: Dan Swanson

PUBLISHED

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

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

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

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

FORTHCOMING

Practical Techniques for Effective Risk-Based Process Auditing
by Ann Butera
ISBN: 978-1-4987-3849-1

The Complete Guide to CyberSecurity Risks and Controls
by Anne Kohnke, Daniel Shoemaker, and Ken E. Sigler
ISBN: 978-1-4987-4054-8

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

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

Securing an IT Organization through Governance, Risk Management, and Audit

Ken Sigler • Dr. James L. Rainey, III

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

Version Date: 20151027

International Standard Book Number-13: 978-1-4987-3732-6 (eBook - PDF)

Contents

Foreword

I am both honored and humbled to have been selected to write the foreword to *Securing an IT Organization through Governance, Risk Management, and Audit*.

This seminal work is long overdue. It offers practical solutions to a complex and expensive challenge facing our nation's critical infrastructure in both the public and private sectors. I do not say this lightly.

I have been actively involved professionally in the cybersecurity discipline for almost 20 years. My first big success was as the legal architect of the chairman of the Joint Chiefs of Staff–directed military exercise Eligible Receiver 97.

It was my first opportunity to brief the Department of Defense General Counsel and subsequently the Attorney General of the United States on the legal and policy implications and the technological challenges implicated in cybersecurity. It was also their first introduction to, and appreciation of, the proper role of technical means of verification via system penetration testing in order to evaluate the efficacy of the Department of Defense's cybersecurity defenses.

Eligible Receiver 97 was a watershed event. The "white hat" hackers, referred to ironically as the Red Team, successfully gained complete access to mission-critical computer systems at highly sensitive although unclassified levels. What was even more remarkable was that

the tools and techniques used were downloaded from the Internet. In other words, these were tools that your common hacker could and did use to attack government and commercial systems connected to the Internet.

The success of Eligible Receiver 97 changed the way senior military and civilian leadership viewed the emerging discipline of cybersecurity. Resources were redirected from more traditional military programs to cybersecurity but the necessary sense of urgency never gained a lasting foothold. The cyberalarms went off but we all too often simply hit the reset button, hoping the problem would simply go away. Hope is not a strategy. It is not even a plan to make a plan!

I am of the strong view that the key individual in helping our nation appreciate the seriousness of the growing cyberthreat to our critical infrastructures was Richard A. Clarke. He was the National Coordinator for Security, Infrastructure Protection, and Counterterrorism under President Bill Clinton and subsequently served President Bush as the Special Advisor to the President on Cybersecurity. Many of the programs he advocated during his tenure, had they not suffered from being "over-coordinated," would have resulted in our national cybersecurity programs being more robust. I must say the same about Melissa Hathaway's efforts with the Comprehensive National Cybersecurity Initiative.

Where does that leave us today? I take little comfort in recalling the history of the Internet. The architects designing this information railroad of Internet commerce were "connections"—the engineer was "features"—and riding in the caboose that was left at the station was the flagman—"security."

Threat actors of the 1970s were largely mischief makers and pranksters. They transitioned a decade later from individual brigands with destructive intent to present-day brigades of hackers working in concert for profit. All too often, we learn that they are acting at the behest and under the protection of nation states.

We also are challenged by malicious insiders. They are like vicious rapacious moths gulping gaping holes in the thin fabric of security that was installed like a decorative curtain as a clever afterthought.

As a result, every day we learn of some new computer security failure brought about by known and unknown computer exploits. What can we do to reduce the risk?

I suggest that risk has three elements: threat actors operating in the threat environment; uncorrected system vulnerabilities; and unexpected consequences. Each leg of the risk triad must be reduced to more manageable levels. There are no silver bullet solutions but there are intelligent choices that can be implemented.

One such intelligent choice is *Securing an IT Organization through Governance, Risk Management, and Audit*. This book offers an implementable, realistic, cost-effective, and workable methodology to help mitigate the risk triad previously mentioned.

This is not a textbook, although it could certainly be used as one. The real value of this commendable work is to reduce the knowledge fog that frequently engulfs senior business management and results in the false conclusion that overseeing security controls for information systems is not a leadership role or responsibility but a technical management task. This is an example of arrogant hubris.

This book is better described as a manual that identifies and describes successful and reproducible business practices and processes directly related to governance, risk management, and audit. Drawing on the Cybersecurity Framework called for in Executive Order 13636 and developed by the National Institutes of Standards and Technology through a collaborative effort between industry and government, the framework identifies and describes standards, guidelines, and best practices designed to help mitigate cybersecurity risk.

The authors, recognizing that it is not enough to identify the most efficient standard from among the many from which we have to choose, take their scholarship to the next level by mapping the framework standards to a proven implementation methodology.

That methodology is described in detail in Control Objectives for Information and Related Technology, generally referred to as COBIT 5. The COBIT publications resulted from a series of studies done by the Information Systems Audit and Control Association, a nonprofit, independent association that advocates information security, assurance, risk management, and governance.

I encourage cybersecurity practitioners at all levels, as well as those in senior management, to carefully read, implement, and practice the techniques and methodologies set forth so clearly in this notable contribution to the field of cybersecurity. It is a book to read, study,

and implement. The return on your investment of time, human, and financial resources will benefit your organization ten times over.

Richard HL Marshall, Esq.
Former Director of Global Cyber Security Management
Department of Homeland Security
Former Associate General Counsel for Information Assurance
National Security Agency
Chief Executive Officer, X-SES Consultants, LLC

Preface

The implementation of appropriate security controls for an information system is an important task that can have major implications for the operations and assets of an organization. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective in their application?

An effective IT security program should include

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.

It is of paramount importance that responsible individuals within the organization understand the risks and other factors that could adversely affect their operations and assets. Moreover, these officials must understand the current status of their security programs and

the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated missions using defined processes of governance, risk management, and audits.

Information is a key resource for all organizations. The information and communications technologies (ICTs) that support information continue to advance at a rapid pace. They are also under increasing attack. Destructive security breaches against financial, retail, and energy providers indicate a need for defined management frameworks that address technology-related risk at an acceptable level. Many organizations recognize this challenge but need help charting a road map to protect valuable business assets. They need an approach that draws on the success of others through manageable processes and measurable improvement. This book describes proven practices to exploit opportunity through a better understanding of organizational risk and active management processes. This book enables the reader to implement Control Objectives for Information and Related Technology (COBIT) methods as an effective way to use the Cybersecurity Framework (described in the following paragraph). Application of these components enables communication about priorities and activities in business terms, turning potential organizational risk into competitive advantage.

In 2013, U.S. President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. The EO called for the development of a voluntary risk-based cybersecurity framework (the Cybersecurity Framework, or CSF) that is "prioritized, flexible, repeatable, performance-based, and cost-effective." The CSF was developed through an international partnership of small and large organizations, including owners and operators of the nation's critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST). The CSF provides a risk-based approach that enables rapid success and steps to increasingly improve cybersecurity maturity. Because these values closely mirror the governance and management principles provided in COBIT, those practices were used in the CSF as an implementation road map.

This book provides details of the CSF with emphasis on the processes directly related to governance, risk management, and audit. Additionally, the book maps to each of the CSF steps and activities the methods defined in COBIT 5, which resulted in an extension of the CSF objectives with practical and measurable activities. Achieving CSF objectives using COBIT 5 methods helps to leverage operational risk understanding in a business context, allowing the ICT organization to be proactive and competitive. This approach, in turn, enables proactive value to the ICT organization's stakeholders, converting high-level enterprise goals into manageable, specific goals rather than an unintegrated checklist model.

While the CSF was originally intended to support critical infrastructure providers, it is applicable to any organization that wishes to better manage and reduce cybersecurity risk. Nearly all organizations, in some way, are part of critical infrastructure. Each is connected to critical functions as a consumer through the global economy, through telecommunication services and in many other ways. Improved risk management by each member of this ecosystem will, ultimately, reduce cybersecurity risk globally.

Acknowledgments

A book of this magnitude could not have come to successful completion without the assistance of many people. First and foremost, we would like to thank our family and friends for their continued patience and support. In particular, much thanks to Ken's wife Tricia, who once again demonstrated the admirable qualities of the usual rock upon which his efforts are founded.

The months when this book was written were challenging times for James. During that period, he lost his grandfather. Three months later his grandmother passed. A short time after that, one of his brightest students lost his life to senseless violence. Each of these individuals played an instrumental role in molding James into the professional that he has become today.

Additional gratitude goes out to the originator of this effort, Dan Swanson, whose tremendous ideas helped bring the book to reality. We would also like to thank our acquisition editor, Rich O'Hanley, who has provided tremendous patience and understanding. Much thanks also go out to Bernadette McAllister, PhD, for the time and effort she put into providing content expert review and feedback. Finally, heartfelt thanks to our project team: project coordinator Hayley Ruggieri, copy editor Adel Rosario from MTC Publishing, and project editor Rachael Panthier. With the help of those three individuals, you are assured a quality reading experience.

Authors

Ken Sigler is a faculty member, since 2001, of the Computer Information Systems (CIS) program at the Auburn Hills, Michigan, campus of Oakland Community College and the chair of the Campus Senate. His primary research are in the areas of software management, software assurance, and cybersecurity. He has authored several books on the topic of cybersecurity ICT management, and to his credit, he developed the college's CIS program option Information Technologies for Homeland Security, which has a recognized relationship with the Committee on National Security Systems. Sigler serves as the liaison for the college as one of three founding members of the International Cybersecurity Education Coalition (ICSEC), which is now the Midwest chapter for CISSE. Throughout his entire tenure at the college, he has also served as postsecondary liaison to the articulations program with Oakland County, Michigan, secondary school districts. Through that role, he developed a 2 + 2 + 2 Information Security Education process leading students through information security coursework at the secondary level into a four-year articulated program leading to a career in information security at a federal agency. Sigler is a member of the Institute of Electrical and Electronics Engineers, the Distributed Management Task Force, and the Association for Information Systems.

James L. Rainey, III, DMIT, is an IT specialist with the U.S. government, where he works with a group of developers on modernizing systems. Dr. Rainey earned a BA degree from the University of Detroit Mercy in 1995 and an MS degree in computer and information systems in 1997 (where he studied under Dr. Daniel Shoemaker). He did a tour with the National Security Agency (Fort Meade, Maryland) in 1998 where he earned a citation for his work with one of their internal groups. Dr. Rainey also worked at GM's Tech Center in Warren, Michigan, while working for Electronic Data Systems (EDS) as a developer. Following his job with EDS, he worked at Comerica Bank's Data Center in Auburn Hills, Michigan, as a developer. He taught at the University of Detroit Mercy's Computer and Information Systems Department for 10 years as an adjunct professor. Prior to accepting this position, Dr. Rainey worked on a large-scale enterprise resource planning implementation as both a Systems Applications and Products (SAP) basis administrator and eventually being promoted as infrastructure architect. Dr. Rainey has been published in refereed IT security journals. In April of 2010, he successfully defended his dissertation at Lawrence Technological University, where Dr. Annette Lerine Steenkamp chaired his committee and Dr. Richard Bush served as a committee member. The research topic was "A Process Improvement Model for Improving Problem Resolution Tracking in Data Centers."

Organization of the Text

This book is divided into two parts. The first part is organized around the Framework for Improving Critical Infrastructure Cybersecurity. The framework is focused on using business drivers as a basis for guiding cybersecurity activities and emphasizing cybersecurity risk as a core component to an ICT organization's risk management processes. The framework is made up of three parts: the core, the profile, and the implementation tiers. Within the core is a set of cybersecurity activities, outcomes, and references that the framework prescribes as being common across all critical infrastructure sectors. At the profile level, the framework provides guidelines for an ICT organization to use in developing profiles. Through the individual profiles, the framework assists in aligning cybersecurity activities with business requirements, risk tolerance, and resources. The information resource level provides the link between the framework's defined processes to private and public sector standards that further define each process. It is through this linkage that COBIT serves as a primary resource for most of the processes defined in the framework. In general, the framework defines what needs to be done, and the provided resources (COBIT in the context of this book) detail how to do it. As a result, the goal of the first part of this book is to provide a comprehensive survey of all of the elements of the framework and how they work together to provide a mechanism for ICT organizations to clearly understand the characteristics of their

approach to managing cybersecurity risk to ensure defect-free software products. In addition, this part presents and discusses three new elements that are necessary to ensure a secure software process: risk understanding, secure coding, and security testing.

The second part of the book presents the COBIT Framework in detail, addressing the following components: assumptions, IT governance, audit guidelines, framework principles, and the framework model. The framework is then decomposed to examine its content at a granular level, focusing on its practical aspects. Next, the control objectives from COBIT are evaluated from a high level and also eventually decomposed to further address the framework's practical elements.

The second part of the book also examines the IT manager's perspective on how the framework should be used to factor in strategic IT decisions from the perspective of what questions are addressed through the framework itself. The Capability Maturity Model and its maturity levels are also compared to qualitative maturity descriptions which are embedded in COBIT.

Finally, the second part of the book provides a demonstration of the concept by showing how to accurately build an audit plan following COBIT.

Because the intent is to provide comprehensive advice about how to structure and improve secure system development through defined processes of governance, risk management, and audit, these two parts are designed to cross-reference each other. The first part presents the commonly agreed-on elements of the critical infrastructure cybersecurity and the second presents the COBIT standard from the perspective of managing cybersecurity governance, risk, and audit. To ensure a successful learning experience, the authors provide

- Insights—Supplemental material inserted directly within the chapters to provide further understanding of presented chapter content.
- Chapter Summary—A bulleted list providing a brief but complete summary of the chapter.
- Case Projects—Hypothetical scenarios designed to put the learner into the role of management or other organization decision makers. The projects are designed to reinforce one or more of the major topics presented in each chapter.

PART I

Cybersecurity Risk Management and the Framework for Improving Critical Infrastructure Cybersecurity

1

Cybersecurity Risk Management

After reading this chapter and completing the case project, you will

- Understand the definition of *cybersecurity* and how it fits into the overall scope of information and communications technology (ICT) organization management;
- Understand the importance of cybersecurity risk management as it relates to managing ICT life cycle processes;
- Understand the relationships between managing ICT governance, risk, and audit;
- Understand the best practices for using standards and frameworks to foster productivity in managing ICT governance, risk, and audit; and
- Understand the benefits of using standards and frameworks within ICT life cycle processes.

Cybersecurity

This book is based on a simple reality. The failure to include governance, risk management, and audit within the management structure of an information and communications technology (ICT) operation leads to unreliable and insecure products. Accordingly, this book describes an approach that lets ICT managers establish and sustain a logical and secure management process. The advice shared in the book is supported by a well-defined and standard set of management practices that have been proved to ensure trustworthy products.

A common cliché used by many ICT managers is, "if it isn't broke, why fix it?" The answer lies in the growing number of harmful effects of exploitation. As ICT systems continue to take advantage of the Internet and cloud computing technologies, those

systems continue to grow exponentially, connecting layer of software made up of trillions of lines of code. Those layers impact every aspect of the general public's way of life, from social networking and other forms of personal entertainment to national defense. A security attack in any of those layers could lead to personal tragedy or national disaster. How serious is the problem? Veracode, a major ICT security firm found that "58 percent of all software applications across supplier types [failed] to meet acceptable levels of security" (Veracode 2012).

Cybersecurity: A Definition

The field of cybersecurity has taken on a number of definitions over the years. However, the common body of knowledge throughout the ICT industry agrees that cybersecurity is concerned with creating and implementing processes that identify emerging threats in addition to providing cost-effective countermeasures to address those threats. The National Initiative for Cybersecurity Careers and Studies more formally defines *cybersecurity* as "strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (National Initiative for Cybersecurity Careers and Studies 2014). Cybersecurity as a discipline has grown quickly, most notably since the 9/11 attacks. Since that time, given the critical role that the Internet plays in our lives, a formalized discipline to study effective ways to ensure confidentiality, integrity, availability, authentication, and nonrepudiation of digital information has moved to the front of our national priority list.

Despite the national attention the field of cybersecurity has received since the beginning of the 21st century, there is still much debate about what mechanism provides the right set of actions to eliminate, or at least minimize, security attacks. Part of the reason for this debate is

that the field of cybersecurity consists of contributions from a number of different disciplines. These disciplines include the following:

- Traditional computer security and computer science studies, which provide the knowledge for safeguarding electronic information
- Networking studies, which supply the knowledge necessary to secure storage and transmission of data and information
- Software engineering, which adds process considerations, such as verification, validation, configuration management, and other forms of life cycle process security
- Business management, which provides the knowledge necessary to conduct project management, create and sustain security policy, and enforce contract and regulation compliance
- Legal studies, which contribute consideration of intellectual property, privacy rights, copyright protection, cyberlaw, and cyberlitigation

All of these disciplines provide a distinct contribution to the underlying effort of protecting an organization's data and information infrastructures. It is only through collaboration between all of these areas, working together toward goal, that significant organizational effectiveness can be achieved toward establishing best practices for cybersecurity. There is still an issue to resolve, however. Many ICT organizations still struggle with managing "who does what." There remains a lack of clear understanding regarding the scope of contribution each discipline serves within the cybersecurity initiative. Regardless of the management structure, common sense tells us that there are three vital components that need to exist within an organization in order for cybersecurity to be achieved: ICT governance, controls, and audit. In a later section of this chapter you will learn how implementing a framework based on those practices is vital to the success of cybersecurity initiatives in an organization.

INSIGHT Cybersecurity Myths That Small Companies Still Believe

High-profile breaches at Target (TGT), Home Depot (HD), and JPMorgan Chase (JPM) have put cybersecurity on the agenda for

companies large and small. But despite the ongoing media commentary and "best practices" memos, consultant Adam Epstein of Third Creek Advisors notes that board members of small-cap companies and those considering or preparing initial public offerings are still befuddled by persistent myths on this topic.

The confused companies include many in Silicon Valley, where one would expect to find more tech savvy, he says. I asked Epstein, the author of a how-to book for corporate boards, to bang out a primer on what directors think they know about cyber threats but really don't. Herewith, his free advice:

1. **Cyber breaches are preventable.** No, they're not. Breaches are a matter of when, not if. As security guru Tom Ridge recently noted in my interview with him in *Directorship* magazine, your networks have likely already been breached. If Fortune 50 companies with nine-digit annual cybersecurity budgets can't prevent breaches, neither can you. Effective cybersecurity is more about identifying corporate "crown jewels," making it as difficult as possible for them to leave the building, and having a thoughtful plan for post-breach resilience.
2. **The information technology (IT) team is on it.** No, probably not. Boardroom cybersecurity oversight generally consists of inviting the head of IT to make a periodic presentation on the company's firewalls and antivirus software. Lacking security experts, most boards collectively exhale on hearing the IT update. Unfortunately, cybersecurity is only partially an IT issue. It's also a matter of corporate culture, employee training, and physical security. You need to worry about disgruntled employees and your supply chain, not to mention that little company you just acquired. That's way beyond IT.
3. **Cyber theft is about credit cards.** In the past several months, I've consulted with several boards whose members said that because their businesses don't store or process credit card data, this area isn't a cause for concern. Wrong. Cyber thieves have disparate goals, ranging from semi-benign mayhem, to espionage, to misappropriation, to terrorism. Credit card information is certainly a target, but so is personal info, intellectual

property, strategy memos, customer lists, and other nonpublic information.

4. **Always disclose cyber incursions immediately.** While it's admirable to want to get out in front of breach incidents and voluntarily disclose them, this can sometimes put a board at a disadvantage. Consider the Target breach, where the size and nature of the crisis expanded substantively with each press release. Malware can morph after being detected and wreak further havoc. It's often unlikely that the first information received by the board about a breach will be accurate and comprehensive, so exercise caution not to complicate a crisis by voluntarily misrepresenting it.
5. **No worries, we've got insurance for this.** A lot of so-called cyber coverage results from a three-page application that barely addresses the quality and extent of your company's computer-network architecture, physical and data security protocols, and corporate risk culture. The resulting coverage usually comes up short. Scores of cyber policies exclude more than they cover. Make sure the policy is underwritten after extensive, informed security assessments of your company—not just a standardized form sent via e-mail.

Good luck. You'll need that, too. (Barrett 2014)

Cybersecurity Risk Management

Simply put, risk management is the practice of looking at what could go wrong and then deciding on ways to prevent or minimize potential problems. It encompasses four components: frame, assess respond, and monitor. We all carry out informal risk management numerous times in the course of a day without even realizing it. Every time we cross a street, we stop to weigh the risk of rushing in front of oncoming traffic, waiting for the light to change, using the crosswalk, etc. Our ability to analyze the consequences of each decision is risk assessment. What we decide to do after performing that quick analysis is risk response based on proper early training and our experience of crossing a road. We may decide to wait for the traffic light and use the crosswalk, which greatly reduces the potential risk; we may follow