

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

© 2016 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20151027

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

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.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

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

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

Contents

FOREWORD	xv
PREFACE	xix
ACKNOWLEDGMENTS	xxiii
AUTHORS	xxv
ORGANIZATION OF THE TEXT	xxvii

**PART I CYBERSECURITY RISK MANAGEMENT
AND THE FRAMEWORK FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY**

CHAPTER 1 CYBERSECURITY RISK MANAGEMENT	3
Cybersecurity	3
Cybersecurity: A Definition	4
Cybersecurity Risk Management	7
Risk Management Components	8
Risk Management Tiered Approach	12
Tier 1: Organizational Level	13
Tier 2: Mission/Business Process Level	14
Tier 3: Information System Level	15
Managing ICT Security Risk through Governance, Control, and Audit	18
Governance	19
Controls	21
Audits	22
Implementing Best Practices Using a Single Cybersecurity Framework	26

Chapter Summary	28
Case Project	29
CHAPTER 2 INTRODUCTION TO THE FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY	31
Overview of the Framework	32
Benefits of Adopting the Framework	34
Framework Core	37
Functions	38
Categories	38
Subcategories	39
Information Resources	40
Framework Implementation Tiers	43
Framework Profile	46
Framework Is Descriptive and Not Prescriptive	50
Structure of the Book's Presentation of the Framework	53
Chapter Summary	53
Case Project	54
CHAPTER 3 IDENTIFY FUNCTION	55
Identify Function Overview	57
Asset Management Category	59
ID.AM-1: Physical Devices and Systems within the Organization Are Inventoried	62
ID.AM-2: Software Platforms and Applications within the Organization Are Inventoried	63
ID.AM-3: Organizational Communication and Data Flows Are Mapped	64
ID.AM-4: External Information Systems Are Cataloged	65
ID.AM-5: Resources Are Prioritized Based on Their Classification, Criticality, and Business Value	66
ID.AM-6: Cybersecurity Roles and Responsibilities for the Entire Workforce and Third-Party Stakeholders Are Established	68
Business Environment Category	69
ID.BE-1: The Organization's Role in the Supply Chain Is Identified and Communicated	70
ID.BE-2: The Organization's Place in Critical Infrastructure and Its Industry Sector Is Identified and Communicated	71
ID.BE-3: Priorities for Organizational Mission, Objectives, and Activities Are Established and Communicated	72
ID.BE-4: Dependencies and Critical Functions for Delivery of Critical Services Are Established	73
ID.BE-5: Resilience Requirements to Support Delivery of Critical Services Are Established	74

Governance Category	76
ID.GV-1: Organizational Information Security Policy Is Established	77
ID.GV-2: Information Security Roles and Responsibilities Are Coordinated and Aligned with Internal Roles and External Partners	79
ID.GV-3: Legal and Regulatory Requirements Regarding Cybersecurity, including Privacy and Civil Liberties Obligations Are Understood and Managed	80
ID.GV-4: Governance and Risk Management Processes Address Cybersecurity Risks	81
Risk Assessment Category	84
ID.RA-1: Asset Vulnerabilities Are Identified and Documented	85
ID.RA-2: Threat and Vulnerability Information Is Received from Information Sharing Forums and Sources	88
ID.RA-3: Threats, Both Internal and External, Are Identified and Documented	88
ID.RA-4: Potential Business Impacts and Likelihoods Are Identified	90
ID.RA-5: Threats, Vulnerabilities, Likelihoods, and Impacts Are Used to Determine Risk	91
ID.RA-6: Risk Responses Are Identified and Prioritized	91
Risk Management Category	92
The Risk Management Plan	94
Implementing Risk Management	96
Risk Handling Strategies	97
Linking COBIT to the Identify Function	100
Chapter Summary	101
Case Project	101
CHAPTER 4 PROTECT FUNCTION	103
Protect Function Overview	104
Access Control Category	106
PR.AC-1: Identities and Credentials Are Managed for Authorized Devices and Users	107
PR.AC-2: Physical Access to Assets Is Managed and Protected	109
PR.AC-3: Remote Access Is Managed	110
PR.AC-4: Access Permissions Are Managed, Incorporating the Principles of Least Privilege and Separation of Duties	111
PR.AC-5: Network Integrity Is Protected, Incorporating Network Segregation Where Appropriate	112
Awareness and Training Category	113
PR.AT-1 through PR.AT-5: Awareness and Training Subcategories	115

Data Security Category	116
PR.DS-1: Data-at-Rest Are Protected	117
PR.DS-2: Data-in-Transit Are Protected	119
PR.DS-3: Assets Are Formally Managed throughout Removal, Transfers, and Disposition	120
PR.DS-4: Adequate Capacity to Ensure Availability Is Maintained	121
PR.DS-5: Protections against Data Leaks Are Implemented	121
PR.DS-6: Integrity Checking Mechanisms Are Used to Verify Software, Firmware, and Information Integrity	123
PR.DS-7: Development and Testing Environment(s) Are Separate from the Production Environment	123
Information Protection Processes and Procedures Category	127
PR.IP-1 and PR.IP-3: Configuration Management Baselines Are Established and Change Control Is Put into Place	128
PR.IP-2: A System Development Life Cycle to Manage Systems Is Implemented	135
PR.IP-4: Backups of Information Are Conducted, Maintained, and Tested Periodically	138
PR.IP-5: Policy and Regulations Regarding the Physical Operating Environment for Organizational Assets Are Met	139
PR.IP-6: Data Are Destroyed According to Policy	140
PR.IP-7: Protection Processes Are Continuously Improved	141
PR.IP-8: Effectiveness of Protection Technologies Is Shared with Appropriate Parties	142
PR.IP-9: Response Plans and Recovery Plans Are in Place and Managed	143
PR.IP-10: Response and Recovery Plans Are Tested	145
PR.IP-11: Cybersecurity Is Included in Human Resources Practices	146
PR.IP-12: A Vulnerability Management Plan Is Developed and Implemented	148
Maintenance	149
PR.MA-1: Maintenance and Repair of Organizational Assets Is Performed and Logged in a Timely Manner, with Approved and Controlled Tools	149
PR.MA-2: Remote Maintenance of Organizational Assets Is Approved, Logged, and Performed in a Manner That Prevents Unauthorized Access	151
Protective Technology	151
PR.PT-1: Audit/Log Records Are Determined, Documented, Implemented, and Reviewed in Accordance with Policy	152

PR.PT-2: Removable Media Is Protected and Its Use Restricted According to Policy	154
PR.PT-3: Access to Systems and Assets Is Controlled, Incorporating the Principle of Least Functionality	155
PR.PT-4: Communications and Control Networks Are Protected	156
Linking COBIT to the Protect Function	158
Chapter Summary	160
Case Project	161
CHAPTER 5 DETECT FUNCTION	163
Detect Function Overview	164
Anomalies and Events Category	168
DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and Systems Is Established and Managed	170
DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods	172
DE.AE-3: Event Data Are Aggregated and Correlated from Multiple Sources and Sensors	175
DE.AE-4: Impact of Events Is Determined	175
DE.AE-5: Incident Alert Thresholds Are Established	176
Security Continuous Monitoring Category	176
DE.CM-1: Network Is Monitored to Detect Potential Cybersecurity Events	177
DE.CM-2: Physical Environment Is Monitored to Detect Potential Cybersecurity Events	180
DE.CM-3: Personnel Activity Is Monitored to Detect Potential Cybersecurity Events	181
DE.CM-4: Malicious Code Is Detected	182
DE.CM-5: Unauthorized Mobile Code Is Detected	183
DE.CM-6: External Service Provider Activity Is Monitored to Detect Potential Cybersecurity Events	184
DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software Is Performed	185
DE.CM-8: Vulnerability Scans Are Performed	186
Detection Processes Category	187
DE.DP-1: Roles and Responsibilities for Detection Are Well Defined to Ensure Accountability	189
DE.DP-2: Detection Activities Comply with All Applicable Requirements	191
DE.DP-3: Detection Processes Are Tested	192
DE.DP-4: Event Detection Information Is Communicated to Appropriate Parties	192
DE.DP-5: Detection Processes Are Continuously Improved	193

Chapter Summary	195
Case Project	195
CHAPTER 6 RESPOND FUNCTION	197
Respond Function Overview	198
Response Planning Category	202
Communications Category	204
RS.CO-1: Personnel Know Their Roles and Order of Operations When a Response Is Needed	205
RS.CO-2: Events Are Reported Consistent with Established Criteria	206
RS.CO-3: Information Is Shared Consistent with Response Plans	207
RS.CO-4: Coordination with Stakeholders Occurs Consistent with Response Plans	208
RS.CO-5: Voluntary Information Sharing Occurs with External Stakeholders to Achieve Broader Cybersecurity Situational Awareness	208
Analysis Category	209
RS.AN-1: Notifications from Detection Systems Are Investigated	209
RS.AN-2: Impact of the Incident Is Understood	211
RS.AN-3: Forensics Are Performed	211
RS.AN-4: Incidents Are Categorized Consistent with Response Plans	212
Mitigation Category	214
RS.MI-1: Incidents Are Contained	215
RS.MI-2: Incidents Are Mitigated	216
RS.MI-3: Newly Identified Vulnerabilities Are Mitigated or Documented as Accepted Risks	217
Improvement Category	217
RS.IM-1: Response Plans Incorporate Lessons Learned	218
RS.IM-2: Response Strategies Are Updated	219
Chapter Summary	219
Case Project	220
CHAPTER 7 RECOVER FUNCTION	221
Distinguishing between Business Continuity and Disaster Recovery	222
Recover Function Overview	224
Recovery Planning Category	226
Activation Phase	227
Execution Phase	229
Reconstitution Phase	231
Improvement Category	231
RC.IM-1: Recovery Plans Incorporate Lessons Learned	232
RC.IM-2: Recovery Strategies Are Updated	233

Communications Category	233
RC.CO-1: Public Relations Are Managed	234
RC.CO-2: Reputation after an Event Is Repaired	235
RC.CO-3: Recovery Activities Are Communicated to Internal Stakeholders and Executive and Management Teams	235
Chapter Summary	235
Case Project	236

PART II CYBERSECURITY, GOVERNANCE, AUDIT, AND THE COBIT 5 FRAMEWORK

CHAPTER 8 THE COBIT FRAMEWORK	241
Assumptions	241
IT Governance	242
Framework Model	243
Practical Technical Scenarios (PTSs)	246
What Drives COBIT 5	249
Framework Principles	251
P1: Meeting Stakeholder Needs	251
P2: Covering the Enterprise End to End	255
P3: Applying a Single, Integrated Framework	258
P4: Enabling a Holistic Approach	258
Enabler 1: Principles, Policies, and Frameworks	258
Enabler 2: Processes	259
Enabler 3: Organizational Structures	260
Enabler 4: Culture, Ethics, and Behavior	261
Enabler 5: Information	261
Enabler 6: Services, Infrastructure, and Applications	262
Enabler 7: People, Skills, and Competencies	263
P5: Separating Governance from Management	263
Management	263
Governance	263
Other Governance Frameworks and Best Practices	263
COSO Internal Controls	264
Information Technology Infrastructure Library	264
Committee of Sponsoring Organizations Enterprise Risk Management	265
Chapter Summary	265
Case Project	266
 CHAPTER 9 DECOMPOSITION OF FRAMEWORK	 269
Framework Principles: Creation	269
Definition of Categories and Seven Enablers	269
Control Issue	273
Navigation Issue	274

Chapter Summary	275
Case Project	276
CHAPTER 10 FRAMEWORK STRUCTURE'S GENERIC DOMAINS	277
COBIT's Framework Structure	277
Planning and Organization	278
Acquisition and Implementation	283
Delivery and Support	284
Monitoring	287
Chapter Summary	288
Case Project	288
CHAPTER 11 DECOMPOSITION OF COBIT 5 PRINCIPLES	291
Purpose of COBIT Control Objectives and Principles	291
Principle 1: Installing the Integrated IT Architectural Framework	293
Principle 2: What Do Stakeholders Value?	294
Principle 3: The Business Context Focus	295
Principle 4: Managing Risk	296
Principle 5: Measuring Performance	296
Chapter Summary	297
Case Project	297
CHAPTER 12 COBIT MANAGEMENT GUIDELINES	299
Enterprise Management	299
Risk Management	300
Status of IT Systems	301
Continuous Improvement	302
Chapter Summary	304
Case Project	304
CHAPTER 13 COBIT MANAGEMENT DASHBOARD	307
Performance Measurement	307
IT Control Profiling	308
Awareness	308
Benchmarking	308
Chapter Summary	311
Case Project	311
CHAPTER 14 WHAT COBIT SETS OUT TO ACCOMPLISH	313
Adaptability to Existing Frameworks	313
Constituency of Governance for Finance	314
Constituency of Governance for IT	315
Chapter Summary	315
Case Project	316
CHAPTER 15 INTERNAL AUDITS	317
Purpose of Internal Audits	317
Roles That Potentially Use COBIT	318

CONTENTS

XIII

Approaches to Using COBIT in an Internal Audit	319
Types of Audits That Can Be Facilitated Using COBIT	319
Advantages of Using COBIT in Internal Audits	320
Chapter Summary	321
Case Project	321
CHAPTER 16 TYING IT ALL TOGETHER	323
COBIT Works with Sarbanes–Oxley (SOx)	323
GETIT Working Hand in Hand with COBIT	323
Process Assessment Model (PAM)	324
Chapter Summary	324
Case Project	325
BIBLIOGRAPHY	327

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

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