

“All-in-One Is All You Need.”

ALL-IN-ONE

CRISCTM

Certified in Risk and
Information Systems ControlTM

E X A M G U I D E

*Complete coverage of all
exam domains*

*Ideal as both a study tool
and an on-the-job reference*

*Filled with practice
questions, tips, and
in-depth explanations*



Electronic content includes:

- Customizable exam engine
- PDF copy of the book

BOBBY E. ROGERS, CISSP-ISSEP®, CEH™
DAWN DUNKERLEY, Ph.D., CISSP®

ALL ■ IN ■ ONE

CRISCTM

Certified in Risk and
Information Systems ControlTM

EXAM GUIDE

This page intentionally left blank

ALL ■ IN ■ ONE

CRISC™

Certified in Risk and
Information Systems Control™

EXAM GUIDE

Bobby E. Rogers
Dawn Dunkerley



New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

McGraw-Hill Education is an independent entity from ISACA® and is not affiliated with ISACA in any manner. This study/training guide and/or material is not sponsored by, endorsed by, or affiliated with ISACA in any manner. This publication and digital content may be used in assisting students to prepare for the Certified in Risk and Information Systems Control™ (CRISC™) exam. Neither ISACA nor McGraw-Hill Education warrants that use of this publication and digital content will ensure passing any exam. Certified in Risk and Information Systems Control and CRISC are trademarks of ISACA in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Copyright © 2016 by McGraw-Hill Education. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN: 978-0-07-184714-8

MHID: 0-07-184714-6

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-184711-7,
MHID: 0-07-184711-1.

eBook conversion by codeMantra
Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." McGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

I'd like to dedicate this book to my family, who was very understanding and patient with me while I wrote this book. To my wife Barbara; my children Greg, Sarah, and AJ; and my grandchildren, Sam and Ben: you guys are the world to me.

—Bobby E. Rogers

I dedicate my work to my children, Lauren and Max, and my (as of the date to be published!) husband Thomas. I am so fortunate to have a beautiful, growing family who puts up with my grouchiness when I write all evening. Thank you for being you.

—Dawn Dunkerley

This page intentionally left blank

ABOUT THE AUTHORS

Bobby E. Rogers is an information security engineer working as a contractor for Department of Defense agencies, helping to secure, certify, and accredit their information systems. His duties include information system security engineering, risk management, and certification and accreditation efforts. He retired after 21 years in the U.S. Air Force, serving as a network security engineer and instructor, and has secured networks all over the world. Bobby has a master's degree in information assurance (IA) and is pursuing a doctoral degree in cybersecurity from Capitol Technology University in Maryland. His many certifications include CISSP-ISSEP, CEH, and MCSE: Security, as well as the CompTIA A+, Network+, Security+, and Mobility+ certifications.

Dawn Dunkerley received a Ph.D. in information systems from Nova Southeastern University in 2011 with a doctoral focus on information security success within organizations. Her research interests include cyberwarfare, cybersecurity, and the success and measurement of organizational cybersecurity initiatives. Dr. Dunkerley holds a number of professional certifications, including CRISC, CISSP-ISSAP, CISSP-ISSEP, CISSP-ISSMP, CSSLP, and PMP certifications.

About the Technical Editor

B. Kelly Sparks is the directorate of test information system security manager (ISSM) for the U.S. Missile Defense Agency and has more than 30 years of experience in the cybersecurity field. Kelly's experience includes 20 years in the U.S. Air Force specializing in electronic systems security assessment, information operations, electronic warfare training, and operations security. Prior to joining Missile Defense Agency, he served as the senior principle cybersecurity analyst with Dynetics, Inc., for nine years; he specialized in information assurance, certification and accreditation, network vulnerability assessment, and penetration testing and provided service to multiple Department of Defense and commercial technology clients. He has more than eight years of teaching experience as an adjunct faculty member at University of Alabama in Huntsville, the U.S. Air Force Information Operations School, and the U.S. Navy Network Security and Vulnerability technician course. Kelly has an A.S. degree in intelligence analysis from the Community College of the Air Force, a B.S. degree in computer science from Park University, and an M.S. degree in network security from Capitol College. Kelly holds the CRISC, CISSP, and CEH certifications, as well as graduate certificates in security management and network protection.

This page intentionally left blank

CONTENTS AT A GLANCE

Chapter 1	Risk Concepts.....	1
Chapter 2	Threats and Vulnerabilities in the Enterprise.....	37
Chapter 3	Identifying and Managing Risk Scenarios.....	69
Chapter 4	Risk Assessment and Analysis	91
Chapter 5	Risk Response and Mitigation.....	125
Chapter 6	Control and Risk Monitoring	159
Chapter 7	Information Systems Control Concepts	181
Chapter 8	Designing and Implementing Controls	209
Chapter 9	Measuring Risk and Control Effectiveness	239
Appendix A	The NIST Risk Management Framework	267
Appendix B	ISACA's Risk IT Framework	275
Appendix C	About the Download.....	285
	Glossary	287
	Index.....	295

This page intentionally left blank

CONTENTS

Acknowledgments	xv
Introduction	xvii
Chapter 1 Risk Concepts	1
Basic Security Concepts	2
Goals of Information Security	2
Supporting Security Goals	3
Risk Management Concepts	7
Risk Terms and Definitions	8
Standards, Frameworks, and Best Practices	12
Business Perspective of IT Risk Management	19
Business Goals and Objectives	19
Business Information Criteria	20
Organizational Structures	21
Information Systems Architecture	22
Managing Risk Ownership	24
Risk Ownership	25
Risk Awareness	26
Legal and Governance	28
Chapter Review	30
Review Questions	31
Answers	35
Chapter 2 Threats and Vulnerabilities in the Enterprise	37
Threats and Vulnerabilities	38
Identifying Threats and Vulnerabilities in the Enterprise	38
Business Processes and Initiatives	42
Environmental Risk Factors	42
Threats	43
Vulnerabilities	44
Project and Program Management	44
Third-Party Management	47
Systems Development Life Cycle	49
Emerging Technologies	53
Management of IT Operations	54
Data Management	56
Business Continuity and Disaster Recovery Management	58
Chapter Review	62
Review Questions	62
Answers	66

Chapter 3	Identifying and Managing Risk Scenarios	69
Developing and Managing Risk Scenarios	69
Risk Identification and Classification	70
Risk Scenarios	71
Developing Risk Scenarios	75
Analyzing Risk Scenarios	80
Risk Register	82
Chapter Review	84
Review Questions	84
Answers	88
Chapter 4	Risk Assessment and Analysis	91
Risk Assessment Processes	92
NIST RMF	92
OCTAVE Methodology	93
ISO/IEC Standards	95
ISACA's Risk IT Framework	96
Performing a Risk Assessment	98
Quantitative and Qualitative Techniques	103
Quantitative	104
Qualitative	106
Combining Quantitative and Qualitative Techniques	107
Other Analysis Techniques	108
Risk Analysis	110
Control Analysis	111
Reporting Risk Assessment Results	116
Chapter Review	119
Review Questions	119
Answers	123
Chapter 5	Risk Response and Mitigation	125
Risk Response	126
Risk Response Standards and Frameworks	127
Understanding Risk Response Options	131
Evaluating Risk Response Options	131
Selecting Risk Response	133
Prioritizing Risk Responses	134
Risk Mitigation	137
Risk Response Action Plans	137
Control Development	138
System Development Life Cycle	146
Project Management	148
Project Management Frameworks	148

Chapter Review	152
Review Questions	153
Answers	156
Chapter 6 Control and Risk Monitoring	159
Control Monitoring	160
Control Testing and Assessment	160
Indicators	166
Chapter Review	174
Review Questions	175
Answers	178
Chapter 7 Information Systems Control Concepts	181
Information Security Control Concepts	182
Control Classification	184
Control Selection	185
Control Frameworks	186
NIST	186
COBIT	190
Val IT	192
PCI-DSS	193
Other Control Frameworks	195
Chapter Review	201
Review Questions	203
Answers	206
Chapter 8 Designing and Implementing Controls	209
Business Perspectives of Controls	210
Business Cases for Controls	210
Regulatory Guidance and Controls	213
Business Functions and Controls	216
Information System Security Engineering	218
Design Considerations	224
Control Selection	227
Implementing Controls	228
Chapter Review	233
Review Questions	234
Answers	237
Chapter 9 Measuring Risk and Control Effectiveness	239
Applying Key Performance Indicators	239
Key Performance Indicator Review	240
Key Performance Indicator Development	240
Chapter Review	263
Review Questions	263
Answers	265

Appendix A	The NIST Risk Management Framework	267
Overview		268
Tiered Approach		268
Applicability		268
Publications		269
RMF Steps		270
Step 1: Categorize Information Systems		270
Step 2: Select Security Controls		270
Step 3: Implement Security Controls		272
Step 4: Assess Security Controls		273
Step 5: Authorize Information Systems		273
Step 6: Monitor Security Controls		274
Appendix B	ISACA's Risk IT Framework	275
Overview		275
Applicability		277
Publications		277
Framework Focus Areas		279
Risk Governance		279
RG1: Establish and Maintain a Common Risk View		280
RG2: Integrate with ERM		280
RG3: Make Risk-Aware Business Decisions		280
Risk Evaluation		280
RE1: Collect Data		281
RE2: Analyze Risk		281
RE3: Maintain Risk Profile		281
Risk Response		282
RR1: Articulate Risk		282
RR2: Manage Risk		283
RR3: React to Events		283
Appendix C	About the Download	285
System Requirements		285
Downloading Total Tester Premium Practice Exam Software		285
Total Tester Premium Practice Exam Software		285
Installing and Running Total Tester		286
Technical Support		286
Total Seminars Technical Support		286
McGraw-Hill Education Content Support		286
Glossary		287
Index		295

ACKNOWLEDGMENTS

From Bobby:

First, we'd like to thank all the good folks at McGraw-Hill Education and their associates for guiding us throughout this book, helping us to ensure a quality product. Meghan Manfre, Amy Stonebraker, and Tim Green were awesome to work with, making sure we stayed on track and doing everything they could to make this a wonderful experience. We're very grateful to them for giving us the chance to write this book and believing in us every step of the way.

Dawn Dunkerley has been one of my best friends for several years now, and I also consider her one of the smartest folks in our profession, so I was doubly happy to have her accept my invitation to coauthor this book. She's added some fantastic insight and knowledge to this book; I couldn't have done it without her. Thanks much, Dawn!

Kelly Sparks deserves some special thanks because, as the technical editor, he had a difficult job, which was to make sure that we stayed reasonable and technically accurate throughout the book. It's hard to be critical of someone else's work when you're also good friends with the writers, so I know it must have been a challenge for Kelly to be critical, truthful, and diplomatic at the same time, but he pulled it off just perfectly anyway. Kelly knows this field extremely well. He didn't pull any punches and was hard on us when he needed to be, and that's why I'm happy to have him on board as the technical editor. Kelly definitely contributed to the clarity, understanding, and technical accuracy of the text. Thanks for all your help, Kelly; this book is a direct testament to your extraordinary competence and professionalism.

Finally, and most importantly, I'd like to thank my family, who endured a lot of time without me at the dinner table, on family outings, and on a daily basis to give me the time to write this book. For my wife Barbara, who went to bed without me many nights while I stayed up writing to meet a deadline, as well as doing my share of the housework so I could write, I give my deepest thanks and love. For my children, Greg, Sarah, and AJ, thanks for being great kids. I'm very proud of the adults you three have become. I'd also like to thank my two grandsons, Sam and Ben, who had to learn to play quietly in the house while I wrote.

From Dawn:

I absolutely must start by acknowledging the best author and friend I could have asked to work with, Bobby Rogers. Bobby not only has a work ethic that scares me (when *does* he sleep?) but has always been ready with a kind word, a joke, or a willing hand. Thank you for your exceptional service to our field. I would also like to thank Barbara Rogers for putting up with Bobby and his aforementioned work ethic. I am so glad to call you both friends.

Meghan Manfre, Amy Stonebraker, and Tim Green continue to be both excellent editors and excellent people; we could not have pulled off this project without you and your consistent support.

A big thank you to our technical editor, Kelly Sparks. You did a great job keeping us on our toes. You were great to work with, and I have a renewed appreciation for your skills.

Finally, I heartily acknowledge the contribution of my family and friends who have supported me throughout my various crazy endeavors. I could not ask for more than the love and encouragement I receive every day toward pursuing my goals. Thank you all.

INTRODUCTION

Welcome to the All-in-One exam guide for ISACA's Certified in Risk and Information Systems Control™ (CRISC™) exam! This book will help you study for, and successfully pass, one of ISACA's premier certification exams, the CRISC exam. This exam is designed to test your knowledge of a wide variety of topics related to the risk management and information systems controls. The exam focuses on business and IT risk management in an enterprise infrastructure, as well as how to design and implement IT security controls to mitigate risk.

Every day, it seems, data is breached at some of the largest organizations in the world. Recently we've seen breaches in the U.S. government, in the healthcare industry, and even at entertainment giants such as Sony. No organization, no matter what size, is immune to the threat of data breaches or, for that matter, data theft or loss. Effective risk management, however, can reduce the possibility of data breaches, as well as strengthen IT infrastructures and even contribute to their efficient use. Information system controls serve to reduce the likelihood of negative events having a significant impact on the organization and should be carefully planned for and considered.

This book covers topics that include basic risk concepts, risk assessments, standards and frameworks, and information security control design and implementation. We also cover the essential concepts, terminology, and definitions that risk management practitioners and security professionals need to be effective in this area. In the book's nine chapters, we cover all four of the top-level domains, as well as the task and knowledge statements listed in the official ISACA exam objectives.

While you don't have to already be an expert in all of the areas we discuss, of course having experience in some of these areas, such as risk concepts, helps. A good, broad background of experience and knowledge in information security will give you an advantage in your studies for this exam. Of course, you'll get a good background in all of these subjects throughout the book. Chapters 1 through 6 cover risk management basic concepts, assessments, and risk response. The remaining chapters (Chapters 7 through 9) discuss how to design and implement information security controls, integrating them with an effective risk management program.

Passing the CRISC exam not only places you in a class of professionals recognized for their experience and expertise in this field but also serves to quantify and validate your knowledge of advanced risk management and security topics. After passing this exam, you'll be able to show that not only are you qualified but you are certified in these areas. This book is designed to help get you there.

How to Use This Book

This book covers everything you'll need to know for ISACA's CRISC certification examination. Each chapter covers specific objectives and details for the exam, as defined by ISACA in its job practice areas. We've arranged these objectives in a manner that makes fairly logical sense from a learning perspective, and we think you'll find that arrangement will help you in learning the material.

Each chapter has several components designed to effectively communicate the information you'll need for the exam.

- The topics covered in each chapter are listed in the first section to help you to map out your study.
- **Tips** are included in each chapter that offer great information on how concepts you'll study apply in a place that we like to call "the real world." Often, they may give you a bit more information on a topic covered in the text.
- **Exam Tips** are included to point out an area you need to focus on for the exam. Note that they won't give you any exam answers, but they do help you by letting you know about important topics that you may see on the test.
- **Notes** may be included in a chapter as well. These are bits of information that are relevant to the discussion and that point out extra information.
- Some chapters have **exercises** designed to provide hands-on experience and to reinforce the chapter information. As your organization and circumstances are no doubt different from ours, these may, from time to time, need a little adjustment on your end.

The Examination

As we have several years of experience in taking certification examinations, let's say that both of us would love for this to be your one-stop shopping source for exam material to help you study for and pass the exam. Unfortunately, as with any sort of certification exam, there's probably no single source of information to study for the test. This is because different materials offer different perspectives, depth of information, and explanations that people process and learn from differently. Having said that, we believe that there's more than enough information in this book for you to both pass the exam and be successful in real life as an ISACA-certified CRISC professional. The other thing you'll need, which in our minds is just as important as good study material, is experience. There's no substitute for practical, hands-on experience, and you should make every effort to get experience on all aspects of the ISACA CRISC exam material that we discuss in this book.

In terms of prerequisites and experience, ISACA requires that you have three years of experience, in at least two of the domains, and of those, one of those two must be in Domain 1 or Domain 2 in order to take this exam and earn the certification. There is no

prerequisite certification exam that you must pass, although having other advanced-level certifications, such as the CISSP or CISM, certainly will also help you gauge the level of knowledge you need for this exam.

Speaking of the exam, here are the specifics: The exam consists of 150 questions, covering the four domains of the job practice areas. Each domain covers a specific topic and is broken down into task and knowledge statements. Because domain objectives can change at ISACA's discretion, the best source for you to get up-to-date information on the domains and objectives is ISACA's website (www.isaca.org), where the most current exam information will be posted. While we've made every effort to ensure that we have the most current exam information in the book (as of the June 2015 exam session), remember to check ISACA's site for any exam or objective changes before, and during, your study effort and definitely before you take the exam.

As you might imagine, the four domains are broken out over the 150 questions, but there is not an equal percentage of questions. If you take a look at the most current version of the ISACA objectives on the site, you'll see that some domains may have more questions than others, based upon how important the topic is to the exam. For example, Domain 1.0, IT Risk Identification, comprises 27 percent of the questions on the exam, per the exam information from ISACA. This domain is broken down into topics such as identifying threats and vulnerabilities, developing risk scenarios, and so on. So, out of 150 questions, you should expect to get about 40 of them from this particular domain. Of course, this is just an estimate because ISACA can alter the exam and its objectives as it desires. But you can pretty much bet that this is a fair estimate. Other domains have differing percentages of questions on the exam as well. One test-taking strategy that has served countless students is to make sure that you know an area you're comfortable with very well, especially if it has a higher percentage of exam questions, but you should also try to focus most of your studying on the areas you are unsure about, of course. You won't be able to pass the test by just being very good at one particular domain, so you should make every effort to learn the domains that you may not know as well.

Finally, you should know that you have a maximum of four hours to take the exam. The exam has a passing score of 450, on a scale of 200 to 800. ISACA, like many certification bodies, uses a type of scale scoring system, so it may be difficult at first to determine exactly how well you did based upon the score you get. As it's still a paper-based exam (as of this writing), scoring the exam and receiving your results can take up to eight weeks. When you pass the exam, you'll get a breakdown of your scores on each of the domains, as well as an overall passing score.

Practice Area Map

The following map has been constructed to allow you to cross-reference the official job practice areas with the job practice areas as they are presented and covered in this book. References have been provided for the job practice areas exactly as the exam vendor presents it, the section of the exam guide that covers that job practice area, and a chapter and page reference.

CRISC Exam Effective 2015

Official Job Practice Areas	All-in-One Coverage	Chapter No.	Page No.
Domain 1: Risk Identification			
1.1 Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization's business objectives and operations	Business Processes and Initiatives	2	42
1.2 Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk analysis	Threats and Vulnerabilities	2	38
1.3 Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations	Developing and Managing Risk Scenarios	3	69
1.4 Identify key stakeholders for IT risk scenarios to help establish accountability	Risk Scenario Stakeholders	3	79
1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile	Risk Register	3	82
1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives	Risk Culture, Appetite, and Tolerance	1	12
1.7 Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.	Risk Awareness	1	26
Domain 2: IT Risk Assessment			
2.1 Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk	Analyzing Risk Scenarios	3	80
2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation	Control Analysis Evaluating Existing Control Effectiveness	4 8	102 229
2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment	Control Gaps Adjusting Controls Based on Mitigation Requirements and Control Gaps	4 8	113 230

Official Job Practice Areas	All-in-One Coverage	Chapter No.	Page No.
2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability	Considering Risk and Control Ownership	4	116
2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making	Reporting Risk Assessment Results	4	116
2.6 Update the risk register with the results of the risk assessment.	Updating the Risk Register	4	118
Domain 3: Risk Response and Mitigation			
3.1 Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions	Risk Response	5	126
3.2 Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date)	Risk Response	5	126
3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level	Designing Effective Controls Information Security Control Concepts Designing Considerations Control Selection	5 7 8 8	140 182 224 227
3.4 Ensure that control ownership is assigned to establish clear lines of accountability	Risk Mitigation Managing Control Ownership and Risk	5 8	131 232
3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution	Risk Mitigation Documenting Controls	5 8	131 232
3.6 Update the risk register to reflect changes in risk and management's risk response	Documentation	5	143
3.7 Validate that risk responses have been executed according to the risk action plans	Risk Response	5	126
Domain 4: Risk and Control Monitoring and Reporting			
4.1 Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk	Defining Key Risk Indicators	6	171
4.2 Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile	Collecting and Analyzing Data Key Performance Indicator Review	6 9	172 240

Official Job Practice Areas	All-in-One Coverage	Chapter No.	Page No.
4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making	Collecting and Analyzing Data	6	172
	Key Performance Indicator Review	9	240
4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance	Defining Key Performance Indicators	6	166
	Key Performance Indicator Development	9	240
4.5 Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls	Defining Key Performance Indicators	6	166
	Key Performance Indicator Review	9	240
4.6 Review the results of control assessments to determine the effectiveness of the control environment	Control Testing and Assessment	6	160
	Key Performance Indicator Development	9	240
4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making	Collecting and Analyzing Data	6	172
	Key Performance Indicator Review	9	240

Risk Concepts

In this chapter, you will:

- Review basic security concepts
- Learn about standards, frameworks, and best practices related to risk identification, assessment, and evaluation
- Learn to describe how business goals, information criteria, and organizational structures affect risk
- Determine how information systems architecture presents risk to the organization
- Learn about risk ownership and awareness
- Recognize legal, regulatory, and contractual requirements for risk management within the organization

This chapter will review a large portion of Certified in Risk and Information Systems Control (CRISC) Domain 1: Risk Identification with coverage of fundamental information security and risk management concepts. We'll cover a good deal of the terminology associated with risk management and many of the core concepts you'll need to be familiar with for the exam, but we will go into more depth on many of these concepts in later chapters.

The CRISC exam topics that we cover in this chapter are as follows and include the following domain objectives and knowledge statements:

- 1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives
- 1.7 Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture



NOTE Throughout the book, the task and knowledge statements are listed in the order they are described in the CRISC Job Practice areas, not necessarily how they are presented in the chapter.

Basic Security Concepts

To successfully sit for the CRISC exam, you should be familiar with some basic security concepts. You can't be expected to know how to manage risk in a security environment if you don't understand the basics of security. We'll assume you have some level of experience already as a security professional since risk management is a significant portion of (and a logical career progression from) the information security profession. You may also have had some level of experience in specific risk management processes during your career. As such, we won't go into detail on the basic security concepts in the upcoming sections; this chapter will just serve as a quick refresher to remind you of certain security concepts.

The CRISC exam is not a technical exam; it is more of a process- and management-oriented exam, so we won't delve into firewall configuration rules, protocol filtering, encryption, or any of the other fun stuff that security professionals do. We will, however, discuss a couple of other security concepts that are important to know for the exam since risk affects all of these concepts in different ways.

Goals of Information Security

Traditional security doctrine, as well as fundamental security knowledge you may learn from various training courses and on-the-job experience over the years, teaches that there are three fundamental security goals. These goals are what we're striving for as security professionals; they are *confidentiality*, *integrity*, and *availability*. You'll sometimes see these three terms strung together as an acronym, such as the CIA triad or, occasionally, as the AIC triad, depending upon the different security literature you read. In any event, these three goals are what you want to achieve for all of your information systems and data. They are also characteristics that you want all of your systems, processes, procedures, methods, and technologies to have. We will discuss these three items in the next few sections and why they are important to the security profession. We'll also briefly describe some of the risks associated with these three goals.

Confidentiality

The goal of confidentiality is to keep information systems and data from being accessed by people who do not have the authorization, need-to-know, or security clearance to access that information. In other words, confidentiality means that only authorized individuals and entities should be able to access information and systems. Confidentiality can be achieved through a number of security protection mechanisms, such as rights, privileges, permissions, encryption, authentication, and other access controls. If the confidentiality of data or information systems is breached, you get the opposite of confidentiality, which is unauthorized disclosure. Unauthorized disclosure is a risk to data and information systems and one that we as security professionals struggle hard to protect against.

Integrity

Integrity is the characteristic of data that means the data has not been subject to unauthorized modification or alteration. In other words, it means data is left in the same state as it was when it was stored or transmitted. So, when it is accessed again or received, it should be identical to the data that was originally stored or transmitted. Integrity is

achieved in several ways, by using checksums, message digests, and other verification methods. Data alteration is the opposite of integrity, particularly when the modification has not been authorized by the data owner. Data modification or alteration can happen accidentally, such as when it may be inadvertently changed because of human error or faulty transmission media. It can also happen intentionally (which is usually malicious in nature when this modification is unauthorized) by direct interaction with data during storage or transmission, such as during an attack, for example. This risk to data affects whether the data can be trusted as authentic or true, whether it can be read as intended, and whether it is corrupt.

Availability

Availability is when data and systems are accessible to authorized users at any time or under any circumstances. Even if data is kept confidential and its integrity remains intact, that does you no good if you can't access it when you need it to perform critical business functions. Availability ensures you have this data (and the information systems that process it) at your fingertips. Just as confidentiality and integrity have their opposites, data destruction or denial of service is the opposite of availability. This risk to your information systems could prevent authorized consumers of that data or users of that information system from performing their jobs, thus severely impacting your business operations. Figure 1-1 shows the relationships of the three information security goals to one another.



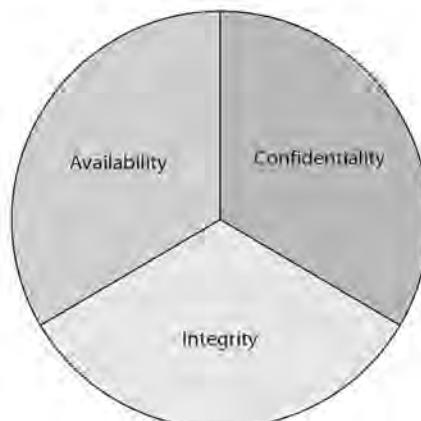
EXAM TIP You will need to understand the definitions of the goals of information security well for the exam. Almost everything in information risk management supports these three goals, either directly or indirectly.

Supporting Security Goals

Popular security theory sets forth the three overarching security goals but also provides for auxiliary elements that support these goals in various ways. These are concepts that, both individually and combined, help you as a security professional to maintain data

Figure 1-1

The three goals of information security



confidentiality, integrity, and availability, as well as protect your systems from unauthorized use or misuse. We'll discuss these different security elements and other concepts, as well as how they support the three primary goals of security, in the next few sections.

Access Control

As a security professional, you probably already know that a *security control* is a security measure or protection applied to data, systems, people, facilities, and other resources to protect them from adverse events. Security controls can be broken down and categorized in several ways. *Access controls* directly support the confidentiality and integrity goals of security and indirectly support the goal of availability. An access control essentially means that you will proactively ensure that only authorized personnel are able to access data or the information systems that process that data. Access controls ensure that only authorized personnel can read, write to, modify, add to, or delete data. They also ensure that only the same authorized personnel can access the different information systems and equipment used to store, process, transmit, and receive sensitive data.

There are several different types of access controls, including identification and authentication methods, encryption, object permissions, and so on. Remember that access controls can be administrative, technical, or physical in nature. Administrative controls are those that are implemented as policies, procedures, rules and regulations, and other types of directives or governance. For example, personnel policies are usually administrative access controls. Technical controls are those that are most often associated with security professionals, such as firewalls, proxy servers, virtual private network (VPN) concentrators, encryption techniques, file and folder permissions, and so on. Physical controls are those used to protect people, equipment, and facilities. Examples of physical controls include fences, closed-circuit television cameras, guards, gates, and restricted areas.

In addition to classifying controls in terms of administrative, technical, and physical, you can also classify access controls in terms of their functions. These functions include preventative controls, detective controls, corrective or remedial controls, deterrent controls, and compensating controls. All of the different controls can be classified as one or more of these different types of functions, depending upon the context and the circumstances in which they are being used.

Data Sensitivity and Classification

Asset is a general, all-encompassing term that could include anything of value to an organization. The term *asset* can be applied to data, systems, capabilities, people, equipment, facilities, processes, proprietary methods, and so on; it is anything the organization values and desires to protect. Organizations normally determine how important their assets are to them and how much protection should be afforded to those assets. For example, intellectual property is an extremely valuable asset to the organization and is normally well protected. This is really the basic fundamental concept of risk management—how much security or protection a particular system or piece of data requires, based upon how likely it is that something bad will happen to it, balanced with what the organization can really afford to spend on the protection for that asset. To make reasonable decisions on how much security an asset needs, the organization has to decide how much the asset is worth to it. We'll discuss worth in terms of dollars a bit later in the chapter, but for now let's

look at it from a perspective of asset sensitivity. In terms of sensitivity, you'll usually see the term *data sensitivity* in particular, but you could also broadly consider sensitivity for any asset in an organization.

Data (or other asset) sensitivity refers to how much protection the organization feels a particular system or piece of data requires, based upon its value to the organization and the impact if it were lost, stolen, or destroyed. For example, information published on the organization's public website or in the company newsletter is public knowledge and is usually easily retrievable if, for some reason, the hard disk containing that data fails or is erased. Since the data is public, you may not consider that data to be very sensitive in nature and require little protection for it. On the other hand, customer order data is extremely important to the organization simply because its business operations depend upon that data in order to function and turn a profit. So, it makes reasonable sense that the organization would spend a little bit more time, money, and effort in protecting that particular data. Therefore, its sensitivity, or *classification level*, would be considered somewhat higher than public data. Generally, the higher the sensitivity of the data, the more protection it is given.

In basic security classes, you typically learn about the different classifications of data found in both commercial organizations and government ones. In commercial organizations, typical data sensitivity labels include Private, Company Sensitive, Proprietary, and so on. In the U.S. government, data sensitivity levels include Confidential, Secret, and Top Secret, and they are classified based upon the level of damage to the security of the United States that could be incurred if data at these various classification levels were disclosed or lost. Remember that data sensitivity is driven by the value of the data to the organization and by the impact if it is lost, stolen, or destroyed, and it is balanced by the commitment of resources the organization is willing to provide to protect that data. Data sensitivity and classification policies specify the different formal levels of sensitivity in the organization and what those levels require in terms of protection.

Identification and Authentication

Identification and authentication are often misunderstood terms. They are related, to be sure, but they are not the same thing and really shouldn't be used interchangeably by a knowledgeable security professional. Identification refers to the act of an individual or entity presenting valid credentials to a security system in order to assert that they are a specific entity. When you enter a username or password into a system, for example, or insert a debit card into an automated teller machine and enter a personal identification number (PIN), you are identifying yourself. Authentication is the second part of that process, where your identity is verified with a centralized database containing your authentication credentials. If the credentials you have presented match those in the authentication database, you are authenticated and allowed access to the network or resource. If they do not match, you are not authenticated and are denied access.

There are several methods of identification and authentication, including single factor (such as username and password, for example) and multifactor, which consists of two or more of the following: something you *know* (knowledge factor), something you *have* (possession factor), or something you *are* (biometric or inherence factor). Authentication also uses a wide variety of methods and technologies, such as Kerberos and 802.1X, for example.

Authorization

Authentication to a resource doesn't automatically guarantee you have full, unrestricted access to a resource. Once you are authenticated, the system or resource defines what actions you are authorized to take on a resource and how you are allowed to interact with that resource. *Authorization* is what happens once you've successfully identified yourself and been authenticated to the network. Authorization dictates what you can or can't do on the network, in a system, or with a resource. This is usually where permissions, rights, and privileges come in. In keeping with the concept of *least privilege*, users should be authorized to perform only the minimum actions they need in order to fulfill their position responsibilities. Authorization has a few different components. First, there is *need to know*. This means there must be a valid reason or need for an individual to access a resource, and only to a certain degree. Second, an individual may have to be trusted, or *cleared*, to access a resource. This may be accomplished through a security clearance process or nondisclosure agreement, for example.



EXAM TIP Understand the differences between identification, authentication, and authorization. Remember that identification is simply presenting credentials, while authentication is verifying them. Authorization dictates what actions an individual can take on a system.

Accountability

Accountability means that a person is going to be held responsible for their actions on a system or with regard to their interaction with data. Accountability is essentially the traceability of a particular action to a particular user. Users must be held responsible for their actions, and there are different ways to do this; it is usually assured through *auditing*. First, there must be a unique identifier that is tied only to a particular user. This way, the identity of the user who performs an action or accesses a resource can be positively established. Second, auditing must be properly configured and implemented on the system or resource. What you are auditing is a user's actions on a system or interactions with a resource. For example, if a user named Sam deletes a file on a network share, you want to be able to positively identify which user performed that action, as well as the circumstances surrounding the action (such as the time, date, from which workstation, and so on). This can be accomplished only if you have auditing configured correctly and you take the time to review the audit logs to establish accountability.



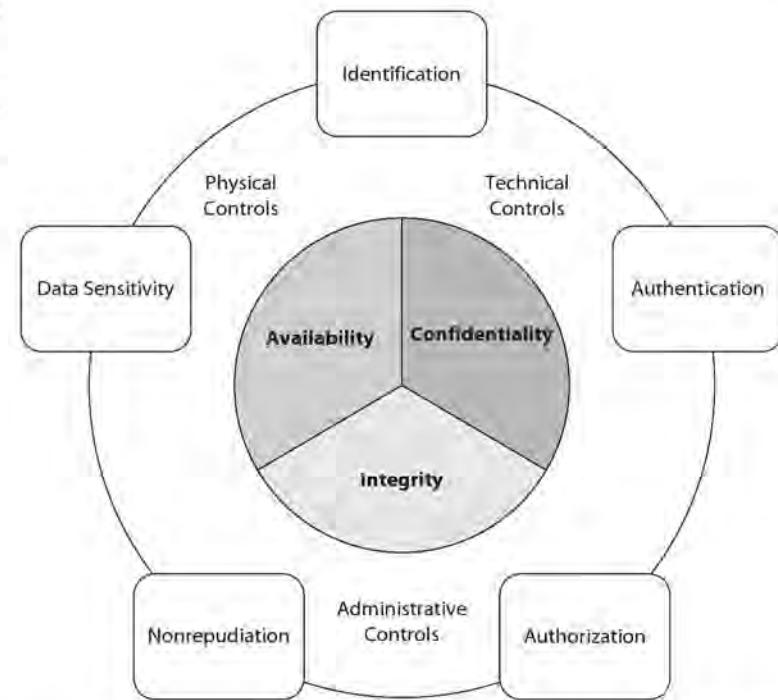
NOTE Although related, accountability is not the same thing as auditing. Accountability uses auditing as just one method to ensure that the actions of users can be traced to them and that they are held responsible for those actions. Other methods, such as nonrepudiation, are used as well.

Nonrepudiation

Nonrepudiation is closely related to accountability. Nonrepudiation ensures that the user cannot deny that they took an action simply because the system is set up such that no

Figure 1-2

How access controls support security elements and information security goals



one else could have performed the action. The classic example of nonrepudiation is given as the proper use of public key cryptography. If a user sends an e-mail that is digitally signed using their private key, then they cannot later deny that they sent the e-mail, since only they are supposed to have access to the private key. In this case, the user can be held accountable for sending the e-mail, and nonrepudiation is assured.

Figure 1-2 summarizes the relationships between access controls, the supporting elements of information security, and the three information security goals. Note that there is no hard-and-fast rule about mapping security elements and access controls to security goals; all of these elements and controls can support any one or even more than one goal at a time. For example, encryption, a technical access control, can support both confidentiality and data integrity at the same time.



NOTE Although other books may describe the supporting elements of the security goals differently, the basic ones we've described here are common and directly support the three goals of confidentiality, integrity, and availability.

Risk Management Concepts

Now that we have framed some of the important information security concepts, such as the security goals and supporting elements, we will explain the basics of how risk is managed with relation to these concepts. As this chapter covers the foundational concepts

associated with risk, we'll cover the different terms you need to know for risk management. Risk management is the overall process of developing a strategy for addressing risk throughout its life cycle and includes several components. These include risk identification, assessment, analysis, evaluation, and response. We'll talk about each of these different processes later in the chapter, as well as throughout this book. For the exam, you'll need to know how these basic processes work, and as you proceed through this book, you will learn how to perform each of these risk management steps.

Risk Terms and Definitions

To fully appreciate the overall concepts of risk management and prepare for the exam, you need to be familiar with several key terms and concepts. In the next few sections, we'll explain several of these key terms and concepts. Understand, however, that risk can be a complex body of knowledge to comprehend, so these are explained only at the basic level during this chapter. We will go far more in-depth on each of these terms and concepts throughout the remainder of this book, including how the terms relate to each other in the overall risk management process.

Vulnerabilities

Vulnerabilities are weaknesses in a system, operation, or facility that would make these resources susceptible to being exploited by a threat. Vulnerabilities can exist in the way a system processes, transmits, or stores data; they can also exist in the technologies that make up a system or even in its design. Even people can have vulnerabilities; one such weakness that affects the people in an organization is complacency. This weakness might prevent them from always following security practices, for example, and allow a security threat to take advantage of that weakness. Facility vulnerabilities could include a lack of physical security controls, a “blind spot” near a doorway to a secure area where an intruder may hide, and so on. One of the first steps in managing risk is to identify all of the vulnerabilities that exist within a system or facility so they can be adequately addressed. This is usually accomplished by conducting a vulnerability assessment, which attempts to thoroughly identify any and all vulnerabilities inherent to a system and its people, operations, policies, procedures, and facilities. We'll discuss vulnerability assessments more in Chapter 2, but for now keep in mind that while a vulnerability assessment can be conducted as a stand-alone type of assessment, it really doesn't have as much value unless it is part of a larger risk assessment, where it can be brought into context with other important elements of risk.

Threats and Threat Agents

A *threat* is a danger of harm that can be enacted on an asset. The asset has to be in danger from this threat and, theoretically, if there is no danger, then there is no threat. Threats exploit specific vulnerabilities. A threat must have a matching weakness in a system that it can exploit, or act upon, if it is to be an effective threat. An example of a threat and vulnerability pairing might be the use of a weak encryption algorithm in a system (a vulnerability) and a cryptographic attack against that algorithm (the threat). If the system used a much stronger algorithm, then the vulnerability would not exist, and that particular

Threat Agent	Threat	Vulnerability	Type of Threat
Fire	Destruction of data-processing facilities	Faulty fire detection or suppression equipment	Physical
Unauthorized user	Accidental unauthorized access to sensitive data	Lack of data sensitivity policy	Administrative
Malicious insider	Data theft	Lack of adequate access controls on data	Technical/physical
Careless user	Information spillage	Lack of protective controls for sensitive information	Technical

Table 1-1 Examples of Threats, Vulnerabilities, and Threat Agents

threat would not be a danger or risk to the system for that specific instance. A *threat agent* is something that causes or initiates a threat against a vulnerability. In the example given previously, a hacker or malicious actor would be the threat agent that exercises the cryptographic attack (threat) against the weak algorithm (vulnerability). Table 1-1 gives some other examples of threats, vulnerabilities, and threat agents to further emphasize these concepts.

As you can see from Table 1-1, a threat is only the presence of something that can exploit a vulnerability; the vulnerability can be a concrete weakness or even the *absence* of a security control within the system (such as a lack of backup power or data destruction policy, for example) that creates a weakness or vulnerability. The presence of both of these conditions at the same time creates the potential for danger or harm to a system, its data, the people, or the facilities. This potential danger is defined as *risk*, but we will present a more comprehensive definition of that term in the next few sections. From the table you can also see that both vulnerabilities and threats directly affect the three primary goals of security (confidentiality, integrity, and availability). Both threats and vulnerabilities can also be different combinations of administrative, technical, physical, and operational in nature.

Threat assessments are often conducted to identify matching threat and vulnerability pairings, as well as the threat agents that could exercise a threat. Like a vulnerability assessment, the assessment does not have to necessarily be part of but can definitely support risk management. Threat assessments are conducted using a wide variety of data, including historical trends, statistical analysis, industry data, and other information from sources including the government, vendors, and even the organization.

Impact

Impact is what happens to the organization or to the business when a weakness or vulnerability is exploited by a threat. Impact can be expressed as a level of damage to an asset or the organization itself. It can be seen as how the business or operations of an organization are affected by a threat that exercises a vulnerability. Impact can also be cumulative; several smaller impacts that affect different systems within an organization can be additive and

create a much larger impact on an organization than any one of them would. Impact can be expressed in terms of revenue lost based upon a complete or partial loss of an asset or process. It can also be expressed in terms of other concrete numbers or, even in subjective terms, based upon how serious the organization determines the effect of the event to be.

Likelihood

Likelihood is the probability of a threat exploiting a particular vulnerability. During threat and vulnerability assessment processes, the organization will normally determine the seriousness of a threat in terms of its impact if it occurs, based upon a certain level of weakness in the system. The organization also routinely determines the likelihood of these threats, given existing security controls and protections for an asset in the organization. For example, the likelihood of an intruder that breaks into an extremely secure facility that has gates, guards, and guns surrounding it, as well as high security fences, might be extremely low. A different facility without all of these security protections might incur a much higher likelihood of the same threat. In addition to security controls protecting an asset, other environmental factors might come into play, such as the facility residing in a “bad” neighborhood, distance from police and other emergency services, motivation of the threat agent, and so on. All of these different factors, which are really unique to the operational environment and asset in question, should be considered when determining the likelihood that a threat could occur. As with impact, likelihood could be measured in statistical percentages or subjective terms.

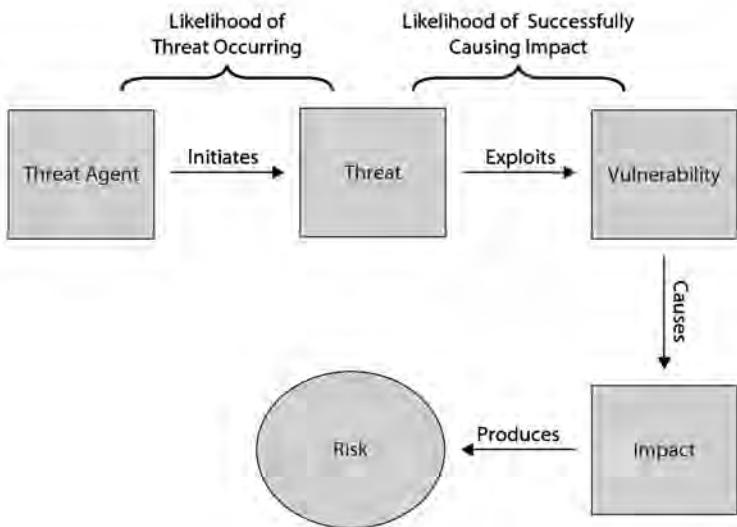
Risk

The four elements just described—vulnerabilities, threats and threat agents, impact, and likelihood—combine to make up the fundamental parts of risk. Risk is sometimes a difficult concept to get your arms around because it can be explained with different definitions, especially within the security community. On one hand, risk is a relative level of danger or harm to an asset. It's also sometimes defined as the likelihood of a negative event happening to an organization and impacting its business operations. Another way of saying it might be the likelihood of a threat exploiting a vulnerability, causing an impact to an asset.

In any event, risk is a combination of these four factors, and it is a value that can be relatively measured using these factors. For example, impact can be expressed in lost revenue (dollars), lost productivity (labor hours), or even loss of market share (a drop in sales). Likelihood can be measured as a statistical probability (a percentage, for example) or even a subjective measurement, such as high, medium, or low. Threats and vulnerabilities can be a little bit more difficult to assign concrete values to; usually these values are also subjective, such as high, medium, or low designations. Later in this chapter, we'll discuss how these values can be measured and risk can be expressed, using either quantitative (expressed as numbers) or qualitative (expressed using subjective values) methods. Figure 1-3 attempts to bring together all of these factors to illustrate their relationships, helping you to better grasp the concept of risk.

Figure 1-3

Threats,
vulnerabilities,
likelihood, and
impact



Two terms associated with risk that we will briefly describe here include *inherent risk* and *residual risk*. Inherent risk is associated with any endeavor, including risk associated with technologies, business processes, markets, and so on. All endeavors that businesses embark on contain some inherent risk that may be both unique to the particular endeavor and common to a technology or process. Residual risk, which we'll discuss in depth later in the book, is the risk that remains after we have taken steps to respond to risk, either by reducing it or by mitigating it. It is a commonly accepted fact within the risk management community that risk can never be entirely eliminated; it can only be reduced to a manageable or acceptable level. Residual risk is normally the amount of risk left over after you've taken these steps, which must then be accepted. We'll discuss more about risk response in Chapter 5.

It's worth mentioning here that organizations typically maintain data associated with risk, including identified threats and vulnerabilities, as well as their likelihood and impact determinations, in what is known as an *enterprise risk management* (ERM) program. In addition to being a system that records and assists in analyzing risk management data, ERM is also the formal management program, including processes and methodologies, that the organization uses to manage risk throughout its entire life cycle.



EXAM TIP Understand the differences and relationships between the four risk elements of threats, vulnerabilities, likelihood, and impact. Threats exploit vulnerabilities, and the level of risk is based upon the likelihood of the threat exploiting a given vulnerability and the impact to the system if it occurs.

Risk Culture, Appetite, and Tolerance

An organization normally has a *risk culture*, which is essentially how the organization as an entity feels about and deals with risk. This culture is developed from several sources. First, it can come from the organization's leadership, based upon their business and management philosophies, attitudes, education, and experience. It can also come from the organization's governance. Remember that governance is essentially the rules and regulations imposed either by external entities (in the form of laws, for example) or internally by organization.

In any case, the culture of the organization really defines how the organization feels about risk and how it treats risk over time. As part of the organization's risk culture, there are its *risk appetite* and *risk tolerance*. These are different terms you also need to know to understand risk. Risk appetite is, in effect, how much risk an organization is willing to deal with in any given endeavor. This is the general level of risk that an organization is willing to accept in the course of its business. An organization's risk appetite is driven by the corporate risk culture, in other words, by the environment the organization exists in (market, regulation, and other external factors).

Risk tolerance, on the other hand, is the acceptable level of deviation in risk for a particular endeavor or business pursuit. Risk tolerance is how much variation from the expected level of risk the organization is willing to put up with. There's a certain amount of risk in every business enterprise or pursuit; however, the organization may not be able or willing to tolerate large deviations from what it considers is its acceptable level of risk on an endeavor.



EXAM TIP Know the differences between risk appetite and risk tolerance; risk appetite involves how much risk the organization is willing to endure, and risk tolerance is how much variation from that amount is acceptable to the business for a particular venture. Risk culture drives both of these factors.

Standards, Frameworks, and Best Practices

Managing risk is not an ad hoc process. It can be a complex effort and involves establishing a formal program with responsible people leading it. It requires developing procedures and processes that are defined, repeatable, and defendable. Fortunately, you don't have to reinvent the wheel; most of this work has already been done for you in the form of established frameworks, methods, standards, and practices. One of the first things you'll want to do when establishing a risk program is to understand what type of framework, processes, standards, and practices you will use since there is a variety to choose from. You must try to use the one that fits your organization the best, and you can't do that unless you have at least a basic understanding of the more defined, standardized ones used in the industry. Let's take a moment and discuss the difference between frameworks, standards, and practices.

A *framework* is a generally overarching methodology for a set of activities or processes. It may not get into the detailed processes and procedures; instead, it provides for a 500-foot view of the general direction and steps used to build a more detailed

program or process. A framework is used as an overall architecture for a larger effort. A framework has characteristics that include defined steps and repeatability and can be tailored based upon the organization's needs. In terms of a risk management framework, you may have a set of general steps defining how to approach risk management, including listing the processes and activities necessary to build such a program or effort. You would then break down these larger steps into specific supporting procedures for this effort based on the needs of your organization and based on standards (described in a moment). Frameworks are typically selected and adopted at the strategic level of corporate management and governance.

A *standard* is a mandatory set of procedures or processes used by the organization, and standards usually fit into an overall framework. Standards often define more detailed processes or activities used to perform a specific set of tasks. Standards are used for compliance reasons and made mandatory by an organization or its governance. The National Institute for Standards and Technology (NIST) standards are mandatory for use by the U.S. federal government, for instance, but are published as an option for private organizations and industries to adopt if they so choose. If an organization adopts the NIST standards for risk management, for example, then the organization may make them mandatory for use by its personnel. Then all processes and activities for a given effort within the organization would have to use and meet those standards. Some standards define the level of depth or implementation of a security control or measure. The Federal Information Processing Standards (FIPS) for cryptography and encryption are an example of this; they set forth the different levels of encryption strength for various cryptography applications that may be required in certain circumstances. So, if you create security policies and procedures for implementing cryptography within the organization, the FIPS standard could tell you to what level those policies and procedures must be implemented.

A *practice* is a normalized process that has been tried and proven as generally acceptable within a larger community of practice. Practices could also be developed by a standards organization or a recognized authority regarding a particular subject or particular process. Professional industry organizations or vendors often develop practices documents. You might also see "best practices" promulgated by various industries or organizations, for example. Practices are not usually mandatory but could be made mandatory by the corporate management or other governance if they were so inclined.

The next few sections give more detailed examples of some of the formal frameworks and standards you should be familiar with for the exam and in real life as a risk management professional. We recommend you pay particular attention to the ones developed and published by ISACA; these are listed in the exam task and knowledge statements and will likely be present in some form on the exam. Of course, in this book, we will give only a brief overview of each, so you should take the time to review the actual standards and frameworks in-depth before you sit the exam.

NIST Risk Management Framework

The NIST Risk Management Framework (RMF) is a six-step methodology that provides for risk management all the way through the information systems life cycle. The steps for the RMF are briefly described in the following sections.

Step 1: Categorize Information Systems This step involves inventorying the types of information on target systems and assigning categorization levels to that information based upon the level of impact based upon if the security goals of confidentiality, integrity, and availability were affected or compromised for that particular information on the system. This step uses subjective values of high, medium, and low to assign values to each of the three goals for a particular type of information. Types of information processed on the system could include business-sensitive information, financial information, protected health information, and so on. FIPS 199, as well as NIST Special Publication 800-60, provides detailed guidance on categorizing information systems.

Step 2: Select Security Controls Based upon these individual values, as well as an aggregate of them, step 2 involves choosing the applicable security controls you would assign to each information system. This step provides baselines of security controls based upon the high, medium, and low values assigned during step 1. If the aggregate value of information or a system has been rated as high, for example, then the high baseline of security controls is employed for that system. Once the security control baseline has been established, the organization has the latitude and flexibility to add or subtract security controls from the baseline as it sees fit based upon different factors including the applicability of some controls, the environment the system operates within, and so on. You can find the selected controls in the supporting NIST Special Publication 800-53, revision 4, which contains a catalog of all of the NIST controls.

Step 3: Implement Security Controls In this step, the selected controls are applied to the information systems, and data is processed on those systems. This in itself is a large process that can cover a good deal of the life cycle of the system in question, and it may take significant time and resources. In this step, the organization is essentially securing the information system against any validated threats and protecting identified vulnerabilities.

Step 4: Assess Security Controls This step is where a lot of security professionals who manage certification and accreditation activities or perform risk assessments come into the picture. During this step, the controls that the organization selects for the information system are formally assessed, verifying that they implement them correctly and validating that they perform as they were designed. They are assessed based upon their effectiveness in protecting against the threats they were implemented to protect against. During this step, the system is assessed in its current state, with all existing controls and mitigations in place. Based upon the assessment, there may be recommendations for further controls and mitigations, as well as alterations to existing security posture for the system. In this step, the level of risk to the system and its data is normally analyzed and determined.

Step 5: Authorize Information Systems Step 5 involves the decision from the entity with the power to authorize a system to be implemented and put into operation. This decision is based upon various factors, including the level of risk assessed during step 4, the risk appetite the organization has settled on, and the tolerance for risk that

the organization is willing to accept. The decision to authorize a system for use may also come with caveats, including conditional authorization based upon the continued mitigation and reduction of risk by the system or data owner. This authorization is a formal authority for the system to operate, made by someone with the legal authority to make that decision. It is typically in writing and valid for only a specified period of time, after which the system must be reassessed for risk and control compliance.

Step 6: Monitor Security Controls Continuous monitoring of security controls defines step 6 in the RMF; just because an authorization decision is rendered doesn't mean that the system will now be operated forever without continually monitoring its security posture for new or increased risks. Existing controls will be monitored for continued compliance and effectiveness against identified threats, new risks will be occasionally discovered for the system as new threats and vulnerabilities are identified, and the system will have to be reauthorized after a certain period of time. Note that the RMF is a cyclical process; all these steps will be re-accomplished for each system at various times over the system life cycle. Figure 1-4 summarizes and illustrates the NIST Risk Management Framework.

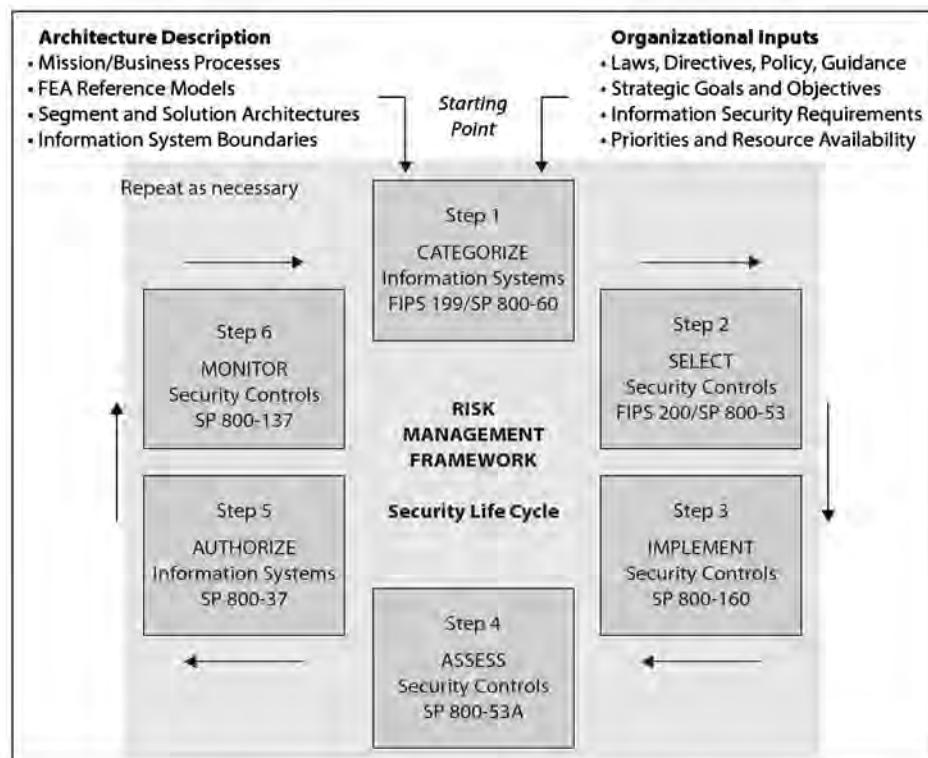


Figure 1-4 The NIST Risk Management Framework (courtesy of NIST, from Special Publication 800-53, revision 4)

As you can see from Figure 1-4, each step of the RMF has associated NIST publications that provide guidance on performing that particular step. Additionally, however, there are also NIST publications that help you manage the overall risk process within the organization. These publications support the RMF by providing more detail on processes and activities, such as managing risk in the organization, implementing the RMF, and even performing risk analysis. The three primary standards that support the RMF are:

- SP 800-30, Guide for Conducting Risk Assessments
- SP-800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
- SP-800-39, Managing Information Security Risk

Keep in mind that there are other standards, however, that support the individual steps of the RMF. These three provide the overall guidance and detail concerning how to implement the RMF's processes. Appendix A goes into detail on decomposing the different steps and associated publications with the NIST RMF, so see that part of the book for a complete breakdown of the framework.

COBIT 5 (ISACA)

Control Objectives for Information and Related Technology (COBIT) is a framework developed by ISACA; it covers several key areas in business governance and IT enterprise management. COBIT covers key areas in auditing, compliance, information assurance, IT operations, and security risk management. This framework has been around for several years and through several iterations; COBIT 5 integrates several other frameworks developed by ISACA into a single unified framework, including the Risk IT, Value (Val) IT, and the IT Assurance Framework (ITAF). It also provides for easy integration of other popular frameworks and standards, including The Open Group Architecture Forum (TOGAF), the Project Management Body of Knowledge (PMBOK), the Information Technology Infrastructure Library (ITIL), Projects In Controlled Environments 2 (PRINCE2), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the many International Organization for Standardization (ISO) standards. This interoperability enables new users of COBIT to leverage any of these other standards they have already been using in their adoption of COBIT.

COBIT combines the best of tried-and-true standards into its fold; it is compatible with the principles of ISO/IEC 38500:2008, *Corporate Governance of Information Technology*, for example, and provides strategy and activities supporting those principles. COBIT also is interoperable, to various degrees, with standards such as the ISO/IEC 27000 series of standards and covers similar security and risk management areas under its domains.

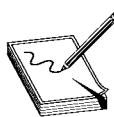
COBIT consists of two layers in its model, governance and management, and separates those two layers into five governance processes and four management domains, respectively. These layers further break down into a total of 37 separate processes. Table 1-2 quickly summarizes these layers and domains and the process they decompose into.

Governance Processes: Evaluate, Direct, and Monitor (EDM) (5)				
EDM01: Ensure Governance Framework Setting and Maintenance	EDM02: Ensure Benefits Delivery	EDM03: Ensure Risk Optimization	EDM04: Ensure Resource Optimization	EDM05: Ensure Stakeholder Transparency
Management Domain: Align, Plan, and Organize (APO) (13)				
APO01: Manage the IT Management Framework	APO02: Manage Strategy	APO03: Manage Enterprise Architecture	APO04: Manage Information	APO05: Manage Portfolio
APO06: Manage Budget and Costs	APO07: Manage Human Resources	APO08: Manage Relationships	APO09: Manage Service Agreements	APO10: Manage Suppliers
APO11: Manage Quality	APO12: Manage Risk	APO13: Manage Security		
Management Domain: Build, Acquire, and Implement (BAI) (10)				
BAI01: Manage Programs and Projects	BAI02: Manage Requirements Definition	BAI03: Manage Solutions Identification and Build	BAI04: Manage Availability and Capacity	BAI05: Manage Organizational Change Enablement
BAI06: Manage Changes	BAI07: Manage Change Acceptance and Transitioning	BAI08: Manage Knowledge	BAI09: Manage Assets	BAI10: Manage Configuration
Management Domain: Deliver, Service, and Support (DSS) (6)				
DSS01: Manage Operations	DSS02: Manage Service Requests and Incidents	DSS03: Manage Problems	DSS04: Manage Continuity	DSS05: Manage Security Services
DSS06: Manage Business Process Controls				
Management Domain: Monitor, Evaluate, and Assess (MEA) (3)				
MEA01: Monitor, Evaluate, and Assess Performance and Conformance	MEA02: Monitor, Evaluate, and Assess the System of Internal Control	MEA03: Monitor, Evaluate, and Assess Compliance with External Requirements		

Table 1-2 COBIT 5 Layers, Domains, and Processes

Note that while COBIT covers a variety of business and IT processes and areas, those specific to risk management happen at both layers—governance and management—and are tightly integrated with other processes. COBIT in this regard is not a risk management framework per se, as is NIST’s RMF, but offers a broader view of management and

governance across all major areas of a business. The next topic we cover, ISACA's Risk IT Framework, supports COBIT and provides a more granular view of risk management practices and activities.



NOTE Understand that while COBIT is important to the overall risk discussion, it is not a risk framework itself. It does, however, support management and governance of not only IT but other critical business areas as well. It also leads into a more detailed discussion on the ISACA Risk IT Framework, which does deal with IT risk.

The Risk IT Framework (ISACA)

The Risk IT Framework is a more concise, risk-related set of processes than offered by its related parent framework, COBIT 5. While COBIT covers the “big picture” of governance and management processes that support risk management programs in the organization, the Risk IT Framework gets more into the key processes of risk management, such as risk governance, evaluation, and response. The Risk IT Framework is also a mere summary of ISACA's *The Risk IT Practitioner Guide*, available to ISACA members, which is an even more in-depth treatment of the processes and activities encountered during risk management.

The Risk IT Framework comes from traditional risk management principles of various enterprise risk management standards and describes activities and processes thought of as best practices in the industry. It provides a starting place for establishing these processes—sort of a map to navigate from a nonexistent or immature risk management program to a formalized, defined set of processes. The Risk IT Framework focuses more on the business risks of using IT in the organization's structure and how risk is involved with the gap often found between IT implementation and business goals. Table 1-3 lists the different domains of the Risk IT Framework model, with each of their three major processes.

Keep in mind that we've covered only a few of the risk-related frameworks and standards available in the industry. Also, be aware that we've only scratched the surface of these bodies of knowledge in this chapter; a full discussion of every one of them is beyond the scope of this book. You should obtain and review these publications more before you sign up for the exam. There are also many other available frameworks and standards developed and promulgated by other professional organizations, government entities, industries, vendors, and so on. You should be familiar with as many of these as is relevant

Risk Governance (RG)	RG1: Establish and maintain a common risk view	RG2: Integrate with ERM	RG3: Make risk-aware business decisions
Risk Evaluation (RE)	RE1: Collect data	RE2: Analyze risk	RE3: Maintain risk profile
Risk Response (RR)	RR1: Articulate risk	RR2: Manage risk	RR3: React to events

Table 1-3 The Domains and Processes of ISACA's Risk IT Framework

to your work since they help you turn risk management from “magic” into an art and science for your organization. The frameworks and standards we have described so far are the ones most relevant to your studies for the CRISC exam.



EXAM TIP While you may not be expected to know the intricate details of each framework described here, it will be helpful to know at least the basic characteristics and descriptions of each. You may be asked to identify a particular characteristic of a framework on the exam.

Business Perspective of IT Risk Management

Up until this point, we have discussed risk strictly from an information security perspective; however, the business aspect of risk management is far more inclusive and broad than the information security focus we have presented so far in this chapter. Although, as an information security professional, you probably tend to look at things through a data protection lens, you must realize that information security risk is really a subset of the risk management considerations that affect the entire organization from a mission or business point of view.

There are several different perspectives of risk in the context of the business environment, most related to legal liability, governance, profitability, market share, and operations sustainability, to name just a few. We could also include risks to intangible elements, such as reputation, consumer confidence, shareholder value, and so on. Opportunity represents potential growth for a business, but opportunity always comes with some level of risk involved. The key to managing this risk is to balance risk of failure with the potential benefits of the business opportunity. Risk tolerance and appetite are factors that figure into this balance for the organization.

In this part of the chapter, we'll cover the risk of information technology systems from more of an organizational and business perspective. We'll explain different business and information technology structures and how they affect risk management within the organization. We'll also cover infrastructure, platforms, and other aspects of technology that can introduce risk into the organization.



CAUTION Remember that the focus on risk from upper management is usually on business risk, not merely IT risk. IT risk is only a small part of the risks faced by the organization in carrying out its mission and goals. You must sometimes frame risk in terms of the business mission, not only from an information technology perspective.

Business Goals and Objectives

Businesses exist with clear missions, goals, and objectives. The organization is in business for a particular purpose, not merely because people want to come to work every day and socialize. Missions, goals, and objectives directly relate to why the organization is in business in the first place, whether that is to develop and market a product or provide

a service. Organizational senior management defines the business's mission, goals, and objectives, typically on a strategic or long-term level. Senior management also defines the levels of risk tolerance and appetite, based upon factors that include the market space, operational environment, economy, governmental regulation, and so on. These risk levels directly articulate and support the business mission, balancing business opportunity that can generate revenue and move the business forward with potential negative events that may cause the business to fail, or at least have a detrimental impact to the organization.



TIP Remember that risk appetite and tolerance are directly related to the business mission, although different business pursuits may have varying levels of each. Senior management sets those levels based upon the potential rewards from risky opportunities and the amount of loss the organization could endure if those rewards don't materialize.

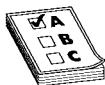
Business Information Criteria

Information is a commodity. Even if the company is in the business of producing goods to bring to market, it still relies on its information and its technology as enablers to produce those goods and deliver them to the market and consumers. Without the ability to generate, process, and otherwise use information, modern businesses would not be able to produce goods or services and compete in market spaces. So, any negative events that affect the organization's ability to process information directly affect the ability of the organization to survive. Information technology directly supports business goals, objectives, and strategy. All elements of a business endeavor depend upon IT, including the organization's information or data, its people, its line-of-business applications and systems, and its overall infrastructure, including all of its equipment and processes.

Information technology affects risks to the business enterprise in two ways. First, information technology is used to help *protect* the enterprise from risk; in other words, it serves to protect the information the business generates and relies on. That's the purpose of having high-capacity storage, faster networking equipment, redundant systems, and security devices sprinkled throughout the infrastructure. The second way that IT affects risk is that it helps the organization to *produce* the information needed to fulfill its business goals and objectives in the first place. Without IT, there would be no information processed, no systems designed, and no advanced technologies developed for a business to take to market and compete with. So, IT serves to both protect information and generate it to advance business goals.

The information the business generates and uses has several key characteristics. First, it should be relevant to the processes it supports. It should also be timely; stale information can prevent a business from fulfilling its functions in both the short-term and the long-term. It should also be accurate and complete. This is where information integrity comes in, which is one of the goals of information security. Anything that affects the accuracy and completeness of information is a risk. Information should also be controlled for access. Again, you learned earlier in the chapter that confidentiality is one of the goals of information security; controlled access to information and the systems that

process it is a must in order to maintain business function. As you might guess, another characteristic of business information is availability to the users who need it whenever and however they need it. This means that authorized users should have business information on a timely basis and in a format that suits their needs. Risk factors that affect any of these information characteristics, such as relevance, timeliness, integrity, confidentiality, and availability, must be considered in the overall risk management process for the organization. Any detrimental impact on these characteristics presents a risk to the business mission.



EXAM TIP Many elements of risk management can be traced back to the three information security goals or the security tenets discussed earlier in the chapter. You should be able to examine risk and determine how it can be traced back to (and how it affects) those goals and tenets.

Organizational Structures

How the business is organized can help drive how it deals with risk, in several ways. Most businesses are organized from a functional perspective; in other words, there are departments and other hierarchical structures established to take care of specific functions that contribute to the business goals and objectives. For example, in a production-driven business, there may be a manufacturing or production department, an engineering department, a research and development department, or an assembly line. There will likely be additional departments that cover support functions, such as marketing, accounting and finance, public relations, and so on. A hospital, on the other hand, will be organized according to its specific functions, such as the emergency department, surgery, neurology, radiology, and so on. Businesses in other markets or areas will be organized differently as well. In any case, the organization of the business is structured as its mission and business purposes dictate. There are certain functions that may be found in any business and may deal with information technology, information security, or even legal compliance. These functional areas may have the primary function of dealing with risk, but an important thing to consider is that all different organizational structures, from lower-level work sections to higher-level departments and divisions, have responsibilities regarding risk.

The organization must look at its structure and decide how each individual unit will manage risk at its own level, understanding that risk management must be uniform throughout the entire organization. Another consideration is that risks tend to “roll up,” or be combined at the higher levels of organization. For example, risks that the accounting department incurs are only part of the higher organizational levels’ risks and included in the risk management processes. Each lower-level unit in an organizational hierarchy has risks that are part of the next higher levels’ risk considerations. While individual units may be responsible for only a small piece of the overall organizational risk, their parent units also bear responsibility for managing that risk, as well as the risk of other subordinate units. Another concept relating to organizational structures is that the risk incurred by one part of the organization is borne by all parts of the organization; there is almost

no such thing as risk that affects only one small part of the business. Risk ripples across the entire organization in some way.

Each individual unit, whether it is a unit in the lower levels of the business hierarchy or at the highest levels, must take steps to identify, evaluate, and assess risks at their level. Risks may be thought of as tactical, operational, and strategic. Tactical risks are those that are encountered by smaller-level production sections, in other words, those that carry out the day-to-day work of the organization. Operational risks can span several work units and relate to how the business conducts its functions, as well as how the different work units interact with each other. Strategic risk is borne at the higher levels of the organization, including senior management, and involves risks incurred by leading the business toward opportunities and away from decisions that exceed the organization's capacity for risk appetite and tolerance. Respectively, these three types of risks also correspond to short-term, mid-term, and long-term risks.

Regardless of the level of risk incurred within the organization, there must be an enterprise risk management strategy and program in place to deal with the lower-tier, middle-tier, and higher-tier risks, as well as ensure that all of the risks are managed consistently and uniformly. Governance from the higher levels of the organization affects risk appetite and tolerance and shapes the organization's risk management strategy throughout all the different hierarchical levels. Organizational structure must support that governance, as well as clearly define lines of authority and responsibility in terms of risk leadership and management.

Information Systems Architecture

The information technology architecture within the organization affects the risk of the business in several ways. Aspects of IT architecture risk include interoperability, supportability, security, maintenance, and how the different pieces and parts of the infrastructure fit into the systems development life cycle. The business views IT as an investment of capital funds, much as it would facilities and other equipment, as a means to an end in supporting the business mission. Information systems represent risk to the business because of the aforementioned interoperability, supportability, security, and other issues. It costs the organization money to maintain and support all of the IT assets within the company, in the form of parts, training for administrators and users, and upgrades. There are also the intangible aspects of IT, such as business value and liability. IT systems affect the bottom line of the organization, so there's a lot of thought put into managing risk for them. Additionally, you should take care to remember that information technology risk is only a piece of the entire enterprise risk picture. In the next few sections, we'll talk about different aspects of the information systems architecture and how they contribute to the overall enterprise risk in the organization.

Platforms

Platforms are the operating systems and distinct architectures the business information systems run on. Businesses could use the Windows and Unix platforms or the Intel and SPARC platforms. Platforms are an element of the IT infrastructure that contributes to the information security and business risk for several reasons. First, it costs to

simultaneously maintain different operating systems and environments that come in different platforms. Platforms also introduce risk into the environment in the form of interoperability, security, and supportability. A diverse platform environment (with mixed platforms, such as Windows, Linux, Macs, Unix, and so on) can affect interoperability with other systems because of differing versions of software and different network protocols, security methods, and so on. A diverse environment can also affect supportability because the organization must maintain different skill sets and a wide knowledge base in order to support the diverse platforms.

On the other hand, maintaining a homogeneous environment can reduce costs, ensure interoperability, and allow a more common set of security controls and mechanisms, such as patch management and configuration management. However, there is even risk involved in a homogeneous platform environment because of the likelihood that a vulnerability discovered in one system would also be shared in many others, offering a wider attack vector for a potential malicious actor. It is really a matter of the systems development life cycle (SDLC) as to how and when platforms are developed, introduced into the infrastructure, implemented, maintained, and, eventually, disposed of, and there is risk inherent to all of these different phases, which we'll discuss more in Chapter 2.

Networks

A network is another aspect of the IT infrastructure that inserts risk into the business environment. While networks are necessary to carry data both within and outside of the organization, these benefits do not come without some degree of risk. Risk can be introduced from a variety of issues, such as unsecured protocols, lack of encryption for data in transit, improper data or system access through weak authentication mechanisms, interception and modification of data, and so on. Networks should be designed to carefully control traffic during all aspects of data transmission, routing, and reception in order for a network to be considered secure.

Applications

Applications introduce risk simply because in this day and age they're so critical to the operations of businesses. Businesses need not only basic word-processing and spreadsheet software but also complex databases, line-of-business applications, specialized software, security software, and other types of applications. Applications have to be managed to their own life cycles as well; they're constantly being patched, upgraded, superseded, and replaced by better, faster software with more features that usually cost more. Risks that are inherent to managing applications within an organization include supportability, backward compatibility, data format compatibility, licensing, and proper use.

Adding to this complexity are the decisions an organization makes in terms of selecting proprietary software, open source software, general-purpose commercial software, or highly specialized software. All of these different categories incur different levels of cost, supportability, licensing, and feature sets. Interoperability also plays a part in application risk, like it does with other infrastructure components. Applications that do not use common data formats or produce usable output for the organization create risk of expense or additional work that goes into transforming data between incompatible applications.

Applications also introduce risk into the business environment with the level of security mechanisms built into them and how effective those security mechanisms are in protecting data residing in the application.

It's worth mentioning here that web-based applications, in addition to presenting the same risks as normal client-server apps, also have their own unique risks. Security is a definite risk imposed by web-based applications since they often directly connect to unprotected networks, such as the Internet. Other risks include those that come from the wide variety of web programming languages and standards available for developers to use.

Databases

Databases, as a subset of applications, impose some of the same risks that applications and other software do. Additionally, databases incur risks associated with data aggregation, compatibility, privacy, and security. Aggregation and inference are risks associated with database systems. Unauthorized access and data loss are also huge risks that databases introduce into the enterprise environment.

Operating Systems

Although we discussed platforms in a previous section, it's worth mentioning operating systems as their own separate risk element in the IT infrastructure. Platforms and operating systems are sometimes used interchangeably, but truthfully, a platform is more a hardware architecture than an operating system categorization. A platform could be an Intel PC or a tablet chipset, for example, which is designed and architected differently and run on totally different operating systems. Different operating systems, on the other hand, could run on the same platform but still introduce risk into the organization, for the same reasons discussed previously with applications. First, there are interoperability and supportability risks and all of the other issues that go hand-in-hand with the normal operating system life cycle, such as patch and vulnerability management. Licensing, standardization, level of user control, and configuration are also issues that introduce risk into the organizational computing environment.



EXAM TIP Although information security professionals tend to focus more on the technical aspects of IT risks, for the exam keep in mind that all IT risks contribute to the overall business risks in the enterprise as well. Make sure you look at the larger picture beyond the IT realm.

Managing Risk Ownership

It makes sense that the organization owns all of the risk that it incurs, which is definitely true to a certain extent. However, within each organization, there are areas that "own" their own piece of risk; in other words, they are responsible for managing it and responding to it. In some cases, they are also responsible for identifying, analyzing, and evaluating risk as it pertains to their functional or defined area. Risk ownership is an effort that requires risk owners to take responsibility for their areas of risk and ensure that they are

properly managed throughout its life cycle. In this section, we'll cover risk ownership in-depth and how it relates to the concepts of risk tolerance and appetite that we discussed earlier in the chapter.

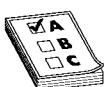
Another related area to risk ownership is that of risk awareness training. The reason this is related to risk ownership is that everyone in the organization, including those responsible for managing risk, must be aware of how risk is identified, evaluated, managed, and responded to throughout the organization. They should also be made aware of the risk management strategy the organization uses and their role in that strategy. This section will also cover risk awareness training and how to implement it within the organization.

Risk Ownership

Risk ownership is a concept that provides a focal point for responsibility and accountability for managing risk throughout its life cycle, including identifying it, assessing and evaluating it, responding to it, and monitoring it. Risk owners take responsibility for risk in their own functional domains within an organization, although you should understand that the risk from several areas is usually “rolled up” into overall organizational risk and is owned by the senior executives or board members who are legally responsible for the organization. There are several components to risk ownership.

The first component is governance. Governance, remember, can be external laws and regulations that the organization is required to comply with. It can also be internal regulations and requirements set by senior leadership within the organization. As part of governance, the organization should set a formal risk strategy and risk management plan, which should detail how risk ownership is defined within the organization. Risk ownership may be defined by functional area, hierarchy within the organization, or any number of other factors.

Other components of risk ownership include responsibility, accountability, and the ability to control the resources that can effectively manage risk (people, funding, equipment, supplies, facilities, and so on). Responsibility means someone has been given the formal authority to manage risk, either by position or by specific appointment from the organization's leaders. A risk owner may have responsibility for a specific area of risk. Responsibility also means that the risk owner bears the burden of being held accountable for their actions in risk management. Accountability means that risk owners must be prepared to take the consequences for success or failure of the risk management efforts. Finally, risk owners must be given the resources and the authority to control those resources in order to effectively manage risk within their area of responsibility. If they have the responsibility and accountability but don't have any control over resources to help manage risk, they will be quite ineffective and won't be able to meet their responsibilities.



EXAM TIP Remember that regardless of what area within the organization is considered a risk owner, ultimately the responsibility for owning and managing risk belongs to the highest level within the organization. This would likely be either the person or the group that has legal liability and responsibility for the organization, such as the chief executive officer (CEO) or the board of directors, as appropriate.

Risk ownership is directly affected by appetite and tolerance. Since these two factors are derived from the organization, they are defined by senior leaders and management, boards of directors, shareholders, and other key entities within the organization. Governance can also help drive risk appetite and tolerance; the organization may establish rules and regulations that strictly limit or are less restrictive toward taking and managing risk. The organization's take on appetite and tolerance directly affects risk ownership because risk owners must manage the risk within their areas based upon these two factors in order to be in line with the organization. Senior leaders, shareholders, and boards of directors must establish the organizational risk culture in order to give boundaries to risk owners within the organization. They may also require that risk owners consult and validate risk decisions with senior management, based upon different threshold or tolerance levels.



EXAM TIP Remember that risk acceptance and tolerance come from the senior management levels of the organization and drive the organization's risk culture. They also drive how risk ownership is defined and structured within the organization.

Risk Awareness

Risk awareness is a necessary part of risk management. It can't be viewed as simply just another two-hour training session to check a box for management or compliance. Risk awareness is essential because it helps form and maintain the organization's risk culture. It also educates personnel at all levels of the organization, including employees, managers, and senior leadership, on the organization's risk strategy, its appetite and tolerance levels for risk, its risk management plan, and other relevant topics necessary to manage risk in the organization. Beyond the education on organizational governance and risk management processes, awareness training can give all members of the organization the knowledge they need to better identify, assess and evaluate, and respond to risk. Risk awareness training may be required for compliance with governance in some cases, but even if it's not, it should be considered critical to the overall risk management strategy in the organization and given its due consideration in the organizational priority list. The next two sections will discuss the different tools and techniques used in risk awareness training and how to develop a risk awareness program within an organization.

Risk Awareness Tools and Techniques

Like most training, risk awareness training should meet several criteria. First, it should be geared toward specific groups of audiences. This might include basic employee training that everyone receives, more advanced training for managers or senior leaders, and in-depth training for those personnel with assigned risk management responsibilities, such as risk owners, risk analysts, and so on. Second, training shouldn't be a one-time event. Periodic, recurring training is a good idea simply because it can be used to reinforce and refresh stale knowledge and bring trainees up-to-date on the latest tools, techniques, and risk considerations. Finally, risk awareness training should be well organized and conducted by knowledgeable instructors, both from inside and outside the organization.

Internal trainers can give the benefit of the organization's specific views on risk culture, appetite, and tolerance, while external trainers bring the benefit of objective knowledge and risk management methods from industry.

The subject of the training depends upon the audience, of course. The basics may include familiarization training with rules and regulations regarding risk within the organization, as well as the basic steps of risk management. Basic concepts and definitions may also be provided in familiarization training. Specific training on risk management techniques and tools may be reserved for those employees who have direct risk management responsibilities. There also may need to be training for senior leadership on how to develop risk management strategy and plans for the organization.

There are several ways that an organization can deliver risk awareness training; different combinations of all of them should probably be used to deliver an effective training program. Classroom training is, of course, one standard method. Other methods might include individual-based training that comes from reading, computer-based training, and so on. Employees might also be required to read a risk management handbook that defines the different rules and regulations covering risk within the organization. Specialized training on risk management might have to be provided by an external training provider for those individuals with defined risk management responsibilities.

Developing an Organization Risk Awareness Program

Establishing a risk awareness program in an organization can be a challenge. One way organizations fail is to simply direct someone to develop a training program when the organization has not even established its risk management strategy or plans. Developing the organization's take on risk is an essential first step before implementing risk awareness training. The organization has to develop, formally if possible, its stance on risk appetite and tolerance, as well as its risk management strategy. It should decide what risk management methodologies it will use, as well as what standards and frameworks. Only then can a training program be developed based upon a good solid risk management framework within the organization.

Establishing the risk awareness training program also requires buy-in from management at all levels. The program should be adequately funded, and allowances should be made for employees to be able to take part in the training. Management should be committed to risk awareness training as part of its overall risk management strategy. Sufficiently trained and experienced instructors or a training program manager should be selected in order to develop and maintain the program. Finally, the training program should articulate not only the risk culture of the organization but also the different risk management needs the organization has. These might include its specific risk factors, threats, vulnerabilities, and so on, taken into account when the training is developed. Employees who participate in risk awareness training should be able to easily put into practice the concepts, tools, and techniques they learn. Additionally, the training program should be periodically evaluated for effectiveness, as well as updated with current risks, governance, tools, and techniques.

Beyond initial or recurring risk awareness training, ongoing communication within the organization is a must for effectively managing risk awareness. Employees in general, but also specifically those with key risk management duties, should be given information on an ongoing basis regarding organizational risks and how to manage and deal with them. Obviously, some information would be restricted from the general organizational

population, but specific instances of threats and vulnerabilities, risk factors, and so on, should be provided to risk managers in key areas so they can keep updated on the most current risk posture for the organization.

Exercise 1-1: Developing a Risk Awareness Program

Review any risk awareness training programs, procedures, or documents within your organization. How often is training conducted? Is it geared toward both the general population of the organization and the specific key roles and responsibilities? Does it cover not only regulations but also risk management methodologies and frameworks? What suggestions could you make to your organization regarding the improvement of its risk awareness training program?



TIP While training programs are sometimes the first things that are cut from the budget or the last things to be developed in a program, don't underestimate the importance of risk awareness training within the overall risk management strategy. Not only can training make the risk management process within the organization more effective, but it can also help reduce or mitigate risks by itself since it also has the effect of educating people on risk and this alone may even help minimize it.

Legal and Governance

An organization's way of dealing with risk—how it formulates strategy, risk management plans, risk response methods, and so forth—comes from a desire to succeed in its business, mission, and goals, of course. But risk management can also be compulsory and not just a smart way of doing business. How an organization manages risk is often directive in nature and can come from different types of governance. Governance includes laws, regulations, and statutes, of course, but it also includes organizational directives. Policies, as well as the procedures and standards that support them, are also considered governance. Depending on its source, different types of governance may be legally binding or not. Obviously, laws and statutes are legally binding, while organizational policy may not necessarily be so.

As a risk manager, you should know something about the various laws and regulations that require an organization to engage in a definitive, coherent risk management strategy and process. While a detailed legal discussion of the dozens of laws and regulations that compel an organization to establish a risk management program are beyond the scope of this book, you should have an understanding of some of the key directives that govern risk management with regard to information protection. This section will discuss a few of those key regulations, as well as how to identify the governance that applies to your organization and how that governance drives your risk management strategy.

Laws, Regulations, and Standards

Many of the different laws and regulations that govern risk management in organizations are business sector and data specific; that is, they specifically apply to a particular area or type of data. For instance, the Health Information Portability and Accountability Act

(HIPAA) requires hospitals, doctors, clinics, and other healthcare providers to establish a risk management program to protect sensitive healthcare information. HIPAA wouldn't apply to a bank or financial company, although other laws would. We'll discuss some of these in the upcoming paragraphs.

One of the most common laws requiring risk management within the information technology world is the Federal Information Security Management Act (FISMA) of 2002. FISMA applies to all U.S. federal government agencies, requiring them to establish information security programs for all federal systems, as well as report risk management and compliance information on an annual basis. FISMA is implemented using various programs within the federal government, depending upon the agency. For example, the U.S. Department of Defense implemented FISMA using the Defense Information Assurance Certification and Accreditation Program (DIACAP) as its vehicle for IT risk management in 2006 but has since replaced it (in March 2014) with NIST's Risk Management Framework. The RMF, as described earlier, provides a risk management process for use in all federal agencies.

The aforementioned HIPAA applies to healthcare providers in the United States and specifically requires that a formal risk management program be established in its Security Rule subsections. The rule further states that risk assessments be performed on all systems that process electronic protected health information (EPCI). Healthcare providers are subject to periodic audits to verify that the provisions requiring risk management are followed.

The Payment Card Industry Data Security Standards (PCI-DSS) were developed by the members of the payment card industry, such as Visa, MasterCard, and so on, to establish a recognized set of standards for information security that applies across all industry partners (for example, banks, retailers, and card issuers). While more technical in nature, the standards require information security policies, vulnerability management, and other risk-based security controls to protect cardholder data.

Financial institutions (banks, brokerage companies, and so on) are the primary focus of the Gramm-Leach-Bliley Act (GLBA), although it also applies to some extent to other organizations. GLBA requires periodic risk analysis performed on processes that deal with nonpublic financial information and personal financial data. While GLBA was primarily designed to allow certain types of financial institutions to merge and interoperate, important risk management requirements were also put into place with this law, such as the Financial Privacy Rule, the Safeguards Rule, and the Pretexting Protection. These rules were included in this legislation to protect consumer privacy, establish information security safeguards (including risk management and analysis), and guard against social engineering attacks, respectively.

Identifying Legal and Governance Requirements in the Organization

Regardless of the type of market or segment in which your organization is involved, there are likely requirements levied by the law, regulations, contract requirements, and even internal organizational policies that require some type of risk management program to be developed and put into place. Obviously, if your organization is a federal agency, a healthcare provider, or some type of financial institution, then you probably fall under the requirements from one of the laws described earlier. Additionally, if you process any

type of consumer credit cards or maintain financial information on individuals, they likely fall under at least the PCI-DSS, if not others. However, even if your organization does not fall under one of the previous categories, you may have legal or regulatory requirements to maintain a risk management program. Often, businesses are members of the industry associations or professional organizations that require risk management as a condition of membership. Additionally, contractual agreements with other organizations often have stipulations built in that require risk management.

Some of these nonregulatory requirements may include requirements for the organization to have a risk management program, for the organization to perform risk assessments and analysis, and for the organization to demonstrate due care and diligence in reducing or mitigating risk. While some of these requirements might not be specifically stated as “risk management” activities, they may come in the form of requirements to maintain security policies, require separation of duties or data, implement standard safeguards (such as strong authentication and encryption methods, for example), and periodically test systems for vulnerabilities. Regardless of how they are stated in policies or contracts, these requirements can be legally used to determine liability for an organization in the event its risk management activities are ever questioned.

When determining legal or regulatory requirements for risk management activities, you should consult with both your organization’s legal representatives, as well as its executive management. You should also research any requirements levied by external organizations or contractual obligations. You must take these requirements into account when developing a risk management program, as well as when developing an information security program. These requirements will likely impact the organization’s stance on risk, as well as its levels of risk appetite and tolerance.

Exercise 1-2: Identifying Legal, Regulatory, and Contractual Requirements

For this exercise, you should attempt to identify and record any legal, regulatory, or other requirements levied on your organization that require a risk management program or activities. You could consult your legal department, talk to senior management, or even perform research on similar organizations. In your attempt to identify these requirements, you may actually uncover other sources that could require risk management activities within your organization. How do these requirements affect your business? Do they influence the organization’s risk appetite and tolerance levels? How are information security programs developed and implemented to meet the requirements for risk management levied by these laws, regulations, or contract requirements?

Chapter Review

In this first chapter, we discussed fundamental concepts of both security and risk management. The three goals of security, known as the CIA triad, are confidentiality, integrity, and availability. Supporting these three goals are other elements of security, such as access control, data sensitivity and classification, identification, authentication, authorization, accountability, and, finally, nonrepudiation.

Risk management is the overall process of developing a strategy for addressing risk throughout its life cycle and includes several components, including risk identification, evaluation, and assessment. We discussed the different concepts associated with risk management, including the threat agents, threats, and vulnerabilities that are associated with assets. We also looked at the variables that affect how these elements create risk: likelihood and impact. The relationships between these elements are what define risk. We also looked at the organizational culture and examined the definitions for risk appetite and risk tolerance.

We then defined standards, frameworks, and practices, and we detailed some of the ones relevant to risk management. We looked at the NIST Risk Management Framework, COBIT 5, and the Risk IT Framework.

We then looked at the business perspectives of IT risk management and discussed how risk from the IT perspective is only a subset of the overall enterprise risk. We examined how business views risk from a mission perspective and covered the criteria business information must meet in order to support that mission. Organizational structures also affect the overall business risk since how the business is organized affects how it incurs and manages risk. We also looked at various elements of information systems architecture and some of the inherent risks involved with those elements. Platforms, networks, applications, databases, and operating systems are all elements of the infrastructure that contribute not only to the IT risk but also to the overall enterprise risk.

We then examined concepts of risk ownership and risk awareness. Risk ownership, while ultimately held by the senior levels of the organization, is also shared by people who have responsibilities and accountability to manage risk within their areas of control. Risk awareness is an educational program that should be implemented to provide the right level of risk-related training to both employees and managers. Risk awareness training can actually help reduce risk throughout the organization. A risk awareness also means keeping the members of an organization informed on the current risk environment.

Finally, we concluded this chapter with a discussion of legal, regulatory, and contractual requirements levied on organizations that make risk management programs and activities mandatory. We discussed a few examples of common laws, such as HIPAA, GLBA, and FISMA, as well as the PCI-DSS; they require organizations to implement and maintain formalized risk management activities.

Review Questions

1. Which of the following security goals is concerned with ensuring that data has not been modified or altered during transmission?
 - A. Confidentiality
 - B. Availability
 - C. Integrity
 - D. Nonrepudiation

2. Which the following is most concerned with ensuring that users cannot deny that they took an action?
 - A. Accountability
 - B. Nonrepudiation
 - C. Auditing
 - D. Authorization
3. Which of the following terms describes a weakness in a system?
 - A. Threat
 - B. Vulnerability
 - C. Risk
 - D. Threat agent
4. Which of the following are both necessary for risk to exist and are often paired together? (Choose two.)
 - A. Impact
 - B. Threat
 - C. Vulnerability
 - D. Likelihood
5. The likelihood of a threat exploiting a vulnerability, causing an impact on an asset, describes which of the following terms?
 - A. Attack
 - B. Threat agent
 - C. Exploit
 - D. Risk
6. Which of the following terms describes the acceptable variation in risk that an organization is willing to deal with for a particular effort?
 - A. Risk acceptance
 - B. Risk appetite
 - C. Risk culture
 - D. Risk tolerance
7. Which of the following describes a set of mandatory procedures or processes used by an organization?
 - A. Standard
 - B. Framework
 - C. Practice
 - D. Policy

8. Which of the following frameworks might be used in business governance and IT enterprise management?
- A. NIST RMF
 - B. COBIT
 - C. The Risk IT Framework
 - D. ISO 27001
9. You are implementing an organizational-wide risk management strategy, and you are using the NIST Risk Management Framework (RMF). You have just completed step 1 of the RMF, categorize information systems. Which of the following steps should you complete next in the RMF sequence?
- A. Authorize system
 - B. Assess security controls
 - C. Continuous monitoring
 - D. Select security controls
10. All of the following are major processes of the Risk Response domain of ISACA's Risk IT Framework, except which one?
- A. Articulate risk
 - B. Manage risk
 - C. Maintain risk profile
 - D. React to events
11. Who defines the organization's mission, goals, and objectives?
- A. Senior management
 - B. Government regulators
 - C. Risk managers
 - D. External corporate auditors
12. Which of the following statements most accurately reflects the effect of information technology (IT) on risk to the business enterprise? (Choose two.)
- A. Information technology is a serious risk to the mission of the organization.
 - B. Information technology is used to protect the organization's information.
 - C. Information technology is used to eliminate risk to the mission of the organization.
 - D. Information technology is used to generate the organization's information.

13. Which of the following terms describes risk that occurs at the lowest levels of the organization, usually corresponding to short-term risk?
- A. Operational risk
 - B. Strategic risk
 - C. Tactical risk
 - D. Enterprise risk
14. All of the following are risks to the enterprise incurred by the organization's information systems architecture, except which one?
- A. Economical
 - B. Interoperability
 - C. Security
 - D. Supportability
15. Who is ultimately responsible for risk ownership within an organization?
- A. Risk assessor
 - B. Mid-level manager
 - C. Designated risk owner
 - D. Senior executives and board of directors
16. What responsibilities do risk owners have toward managing risk?
- A. Managing risk for a given area of responsibility throughout its life cycle
 - B. Eliminating risk from their area of responsibility
 - C. Informing senior executives and the board of directors about risk levels within their area of responsibility
 - D. Delegating risk management responsibilities to a lower-level manager
17. What are the two goals of a risk awareness program within an organization? (Choose two.)
- A. Eliminating risk
 - B. Informing organizational personnel about the risk environment
 - C. Training organizational personnel on risk concepts and responsibilities
 - D. Training risk managers on risk reduction and mitigation techniques
18. In addition to the legal and regulatory requirements for risk management, what are two other sources of requirements for risk management programs within an organization?
- A. Contractual requirements
 - B. Risk assessor requirements
 - C. Industry association requirements
 - D. Activist group requirements

19. Which of the following regulations requires a formalized risk management program in order to protect electronic patient health information?
- GLBA
 - PCI-DSS
 - HIPAA
 - FISMA
20. Which of the following is an industry standard, established by an association of vendors, that requires stringent information security safeguards as part of a risk management program?
- PCI-DSS
 - HIPAA
 - GLBA
 - FISMA

Answers

- C. Integrity is concerned with ensuring that data has not been modified or altered during transmission or storage.
- B. Nonrepudiation is concerned with ensuring that users cannot deny that they took a particular action.
- B. A vulnerability is a weakness in a system.
- B, C. Threats and vulnerabilities are both necessary for risk to exist and are often paired together in assessments since you cannot have risk if you have one without the other.
- D. The likelihood of a threat exploiting a vulnerability, causing an impact to an asset, describes risk.
- D. Risk tolerance is the acceptable variation in risk that an organization is willing to deal with for a particular effort.
- A. A standard is a set of mandatory procedures or processes used by an organization.
- B. COBIT is used in business governance and IT enterprise management.
- D. Step 2 of the RMF is to select security controls and is accomplished after information systems have been categorized.
- C. Maintain risk profile is not a process of the Risk Response domain of ISACA's Risk IT Framework; it falls under the Risk Evaluation domain.
- A. Senior management in the organization defines the organization's mission, goals, and objectives.
- B, D. Information technology is used to generate the business's information, as well as protect it.

13. **C.** Tactical risk occurs at the lowest levels of the organization, usually corresponding to short-term risk.
14. **A.** While there is a financial risk involved in capital expenditures for IT, economical risk is not one specifically introduced into the enterprise as a direct consequence of the IT architecture.
15. **D.** Senior-level executives, as well as the board of directors, are ultimately responsible for risk ownership within an organization, even when a lower-level person has been designated as a risk owner.
16. **A.** Risk owners have responsibility for managing risk in their areas of responsibility throughout its life cycle.
17. **B, C.** A risk awareness training program is designed to both train organizational personnel on risk concepts and their various roles and responsibilities related to risk management and train all personnel on the risk environment in which the organization resides.
18. **A, C.** Both contractual requirements, as well as industry associations, may mandate that an organization have a formalized risk management program.
19. **C.** HIPAA regulations require a formalized risk management program in order to protect electronic patient health information.
20. **A.** PCI-DSS is an industry standard, established by an association of vendors, that requires stringent information security safeguards as part of a risk management program.

Threats and Vulnerabilities in the Enterprise

In this chapter, you will:

- Learn how to identify potential threats and vulnerabilities
- Understand the different business initiatives and processes that create risk
- Analyze how threats and vulnerabilities factor into different aspects of enterprise risk, including areas such as data management, third-party relationships, the systems development life cycle, project management, business continuity and disaster recovery, IT operations management, and implementation of new technologies

This chapter covers the second part of the first Certified in Risk and Information Systems Control (CRISC) domain and focuses on threats and vulnerabilities associated with different aspects of the enterprise. Aspects of business we'll discuss include managing technology changes, working with external parties, planning for disasters and other negative events, and managing the information infrastructure that the business depends on daily. These aspects create risk and are a necessary part of a business.

The CRISC exam objectives covered during this chapter include the following task statements:

- 1.1 Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization's business objectives and operations.
- 1.2 Identify potential threats and vulnerabilities to the organization's people, processes, and technology to enable IT risk analysis.



NOTE Throughout the book, the knowledge and task statements are listed in the order they are described in the CRISC Job Practice areas, not necessarily the order they are presented in the chapter.

Threats and Vulnerabilities

In Chapter 1 we defined threats and vulnerabilities: A *threat* is a negative action or event, which is exercised against a *vulnerability* (a weakness or lack of security control within a system or asset). Threats can be categorized in many ways; they can be human-made or natural, accidental or intentional, internal or external, and so on. By itself, an event or action is not necessarily a threat against a particular organization or system; there must be a vulnerability present on that particular system or in that organization that could be negatively affected (exploited) by the event or action for it to be actually considered a threat to that system or organization.

A vulnerability could be within an asset, a system, a process, an organizational entity, or even a person. It could be a weak algorithm, a faulty procedure, a lack of a physical barrier, an uneducated or careless user, or any of a number of other examples. Weaknesses in these elements, or a lack of security protections for them, are vulnerabilities, and they enable threats to materialize in negative ways when those weaknesses are exposed. A *threat agent* (sometimes called a *threat actor*) is the entity causing or enacting a threat against a vulnerability.

Threats and vulnerabilities create risk. These two elements alone don't, however, tell you the magnitude or level of risk; that's where the elements of impact and likelihood come in. One simple method of defining risk in terms of threats and vulnerabilities (not the only method, by the way) is by using the formula $\text{threats} \times \text{vulnerabilities} = \text{risk}$. You might not want to think of this formula in strict mathematical terms; it's more helpful to look at it as a relationship formula more than a mathematical one. It helps illustrate the point that threats and vulnerabilities go hand-in-hand in producing risk; if you are lacking for either a particular asset or a scenario, then you have no risk.

Over the next several sections, we will discuss threats and vulnerabilities from several different perspectives. Some of these directly relate to business processes, objectives, and initiatives. All of these perspectives discuss the various threats and vulnerabilities that affect these different aspects of the business and organization. First, though, we'll discuss general concepts in discovering threats and vulnerabilities.



EXAM TIP Keep in mind the definitions of and relationships between threat agents, threats, and vulnerabilities. Threat agents initiate or cause threats, which exploit vulnerabilities in a system.

Identifying Threats and Vulnerabilities in the Enterprise

As we mentioned in the first chapter, identifying threats and vulnerabilities is part of the first steps in risk management. There are discrete processes, *threat assessments* and *vulnerability assessments*, that are used to perform these tasks. A threat assessment develops a comprehensive list of all the possible threats to an asset, an organization, or any other level of business process the organization wants to focus on. The threat assessment includes potential threats and threat agents, and classifies them in different categories since some of these threats are not within the control of the organization (think tornadoes, for example).

A vulnerability assessment, in turn, looks at an asset, process, or other element in the organization to determine its weaknesses. These could be weaknesses inherent to the asset or process or in the form of a lack of protection for the asset. While threat and vulnerability assessments are two separate processes, neither is really done without consideration of the other. Threats and vulnerabilities are almost always expressed as a pairing; it's difficult to discuss one without the other for context. For the sake of discussion and learning, however, we'll discuss both of the processes involved with determining threats and vulnerabilities separately in the next two sections.



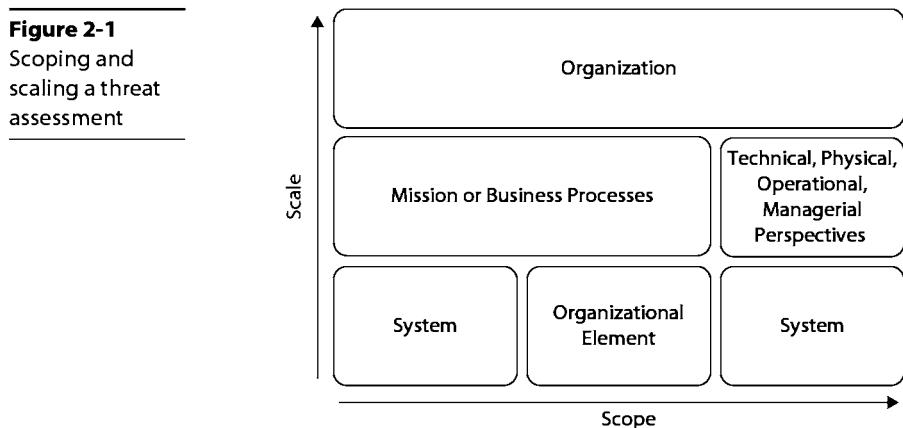
EXAM TIP Threats and vulnerabilities are always expressed together as a pair. For a given set of circumstances, if you have no threat that could exercise a particular vulnerability or no vulnerability that could be exploited by a particular threat, then you have no definable risk for those particular sets of circumstances.

Threat Assessments

A term that you may occasionally hear is *threat modeling*. Threat modeling involves looking at every possible threat agent, action or event, attack vector, and vulnerability for a given system, asset, or process, and then modeling or simulating how it could progress and the damage that could occur. It has its origins in the U.S. and U.K. defense industries. A threat assessment examines how these threats could affect the particular asset, organization, or system you are looking at, in context. With that, a threat assessment could be done on one of several levels, either simultaneously or separately. For example, you could perform a threat assessment on a new system that is being developed or installed. You would examine the different threat agents and threats that could affect that particular system. You could also look at an organizational process, or even the entire organization itself, and perform a comprehensive threat assessment. In addition to *scaling* a threat assessment, as we just described, you could look at threats from a particular perspective, performing a threat assessment specifically for technical threats, physical ones, or even external operating environment threats. This relates to *scope* of the assessment. For example, you could look at the technical aspects of a given system or examine threats inherent to the processes and procedures associated with a particular business unit. Figure 2-1 shows this scoping and scaling process.

As this figure illustrates, you could scale an assessment to include only certain systems within certain functional areas. You could scope it by examining not only all of the threats that apply to the technical aspects of systems in those particular functional areas but also threats that affect associated business or management processes. You could have any combination of scope and scale that the organization needs to fulfill its assessment goals.

Table 2-1 illustrates how threat agents and threats could be categorized, given factors such as intent, relationships, skills, and so on. Note that these could affect any number or combination of elements (processes, systems, and so on) within an organization. You could categorize threats and threat agents using these characteristics, as well as develop others that frame and define them for your organization.



Intent	<u>Accidental</u> : Untrained or careless employee; business partner <u>Intentional</u> : Hacktivist, competitor, disgruntled employee, foreign agent, unbalanced individual, organized crime, terrorist, thief, script kiddie
Relationship to organization	<u>Internal</u> : Employees, managers, executives <u>External</u> : Contractor, supplier, vendor, government agency, nation-state, competitor, civil activists
Skills	None, basic, intermediate, advanced
Objectives	<u>Accidental</u> : Workarounds or cut corners, faster/less work <u>Intentional</u> : Theft, destruction, sabotage, embarrassment, blackmail, monetary gain, competitive advantage, intelligence
Methods	<u>Accidental</u> : Inattentiveness, ignorance, arrogance, complacency, poor planning <u>Intentional</u> : Social engineering, hacking, theft, physical damage, data alteration, impersonation
Results	System/data theft, modification, or destruction, unauthorized access, compromised information, loss of business, loss of customer confidence, loss of revenue or reputation, facility damage

Table 2-1 Characteristics of Threat Agents

Note that this information is only a sampling of what you may come up with in a threat assessment. You may also break down some of these elements into far more specific ones, based upon your needs and the organization and systems you are focused on. For example, a defense contractor or military organization would likely have a more specific set of threats and agents in its assessment than would a nonprofit, charitable organization.



NOTE Appendixes D and E in National Institute of Standards and Technology (NIST) Special Publication 800-30, "Guide for Conducting Risk Assessments," offer a much more comprehensive list of threat agents and their related threats.

Vulnerability Assessments

Vulnerability assessments are used to discover weaknesses that could be potentially exploited by a threat. Weaknesses could be in systems, networks, processes, procedures, physical controls, people, or even a combination of any of these elements. Vulnerabilities may be a weakness inherent to a system or process because security was not considered or built in. A vulnerability could also be a lack of a security control or measure or a failure on the part of people or systems to correctly follow a process or procedure. While some vulnerabilities may become readily apparent after a system or process has been put into place, most won't be unless an in-depth vulnerability assessment takes place.

The assessment can be purely of a technical nature; it can be used to review policies, procedures, and operations, or, as most assessments usually are, it can be a combination of all of these. A technical vulnerability assessment would be focused on the security and operations of systems, hosts, and networks. An assessor might do several things to determine technical vulnerabilities, such as run a vulnerability scanner, review the configuration files on a system to look for obvious issues, capture network traffic to look for nonsecure protocols or potential traffic issues, or use any number of other methods.

A vulnerability assessment can be scoped and scaled to a particular host, network, or process. It can be applied to an entire organization or a selected division under its control. It can also be conducted at a surface level or go into great depth. Obviously, the wider the scope and larger the scale, as well as the more in-depth an assessment is, the more vulnerabilities will be uncovered; therefore, a more accurate assessment will be produced. However, the scope, scale, and depth of the assessment will depend upon many factors, including the organization's purpose for the assessment, the resources it is willing to commit to the assessment, and so on.

Exercise 2-1: Determining Vulnerabilities

Pick a system that you have worked with and try to think of all of the vulnerabilities associated with this system. Are there associated threats with these vulnerabilities? If so, list those threats. Did you find that you had either threats or vulnerabilities that weren't paired?

Table 2-2 shows how you might list vulnerabilities for a particular system and even categorize them in terms of technical, administrative, or operational/physical.

Of course, what's missing from all of this is the final piece, which is adding the other elements of risk into the mix. In this process, the threat and vulnerability assessments

Vulnerability	Category
Lack of access control policy	Administrative
Inadequate encryption mechanisms	Technical
Faulty media storage or transport procedures	Operational
Use of single-factor authentication	Technical
Lack of closed-circuit television (CCTV) cameras near sensitive areas	Physical

Table 2-2 Vulnerabilities Developed During a Vulnerability Assessment

Threat	Threat Agent	Vulnerability	Impact	Likelihood	Result
Exploit code	Malicious outsider	Software flaw	High	Medium	Buffer overflow, unauthorized access
Data pilfering	Malicious insider	Inadequate permissions on sensitive files	High	Medium	Unauthorized access to data
Fire	Careless employee	Lack of fire suppression systems	High	Low	Loss of systems
Natural disaster	Tornado	No off-site storage of backups	Medium	Low	Destruction of systems and media containing data

Table 2-3 Combining All Four Risk Elements

are factored in with impact and likelihood to generate a risk assessment. Table 2-3 shows how a simplistic example might look after factoring in all of these different elements.

Business Processes and Initiatives

Within the organization, there is a defined mission, as well as strategic and tactical goals established to support that mission. Business processes and initiatives that the organization undertakes every day are designed to get the organization to those goals and support the mission. In the business world, there are factors that contribute to the risk incurred in any business venture or initiative. There are also threats to the business processes, as well as vulnerabilities inherent to them. In this section, we'll look at all three of these items: the risk factors that come from the operating environment of the business, the threats to the business mission and processes, and the vulnerabilities that are inherent to those same processes. After we've explained some basics about how risk factors, threats, and vulnerabilities generally affect the business processes, we'll go into more depth on specific processes and look at how these elements affect them at a more detailed level.

Environmental Risk Factors

Risk factors affect the organization by influencing the level of risk, either by helping to lower risk or by creating higher levels of risk. Risk is created by manipulating one of the four elements discussed in Chapter 1: threats, vulnerabilities, likelihood, or impact. Risk factors can influence all four of these elements in different ways. For example, risk factors can increase the likelihood of a threat exploiting a vulnerability or can increase the impact that could occur if this vulnerability were exercised against the organization. These factors can also affect the organization's ability to mitigate or reduce risk. So while risk factors aren't necessarily the same thing as threats, vulnerabilities, impact, or likelihood, they can influence these different elements in many unpredictable ways.

Factors that affect risk are environmental in nature; that is, they come from the organization's operating environment. Risk factors can come from inside the organization, as well as from outside. Some factors actually come from the nature of the organization itself. These factors include the characteristics or attributes of the business, such as its size, its mission, its location, its financial status, and so on. These factors affect risk because they also, in turn, affect the ability of the business to function.

Internal factors include the organizational structure, culture, its ethics, and its people. The people of the organization include not only its employees and managers but also anyone who has a stake in the success of the organization. Other internal factors could include the organization's investment in equipment and facilities, the training of its employees, what type of IT environment the organization has, and how it is structured internally. All of these factors affect risk because the organization uses these factors to balance its risk appetite and tolerance levels. Internal factors also serve to allow the organization to gauge how successful it would be in a particular business initiative. From a management perspective, internal factors are, to a large degree, within the organization's ability to control and affect, so these factors are often manipulated or adjusted to assist in reducing or mitigating risk. For example, training employees in new technologies in response to market trends and technological advances is an internal risk factor that can be controlled by the organization. Hiring new employees, laying off employees who are no longer needed, and restructuring the internal architecture are all also other examples of internal factors that can be controlled by the organization.

External factors, on the other hand, are factors not easily controlled by the organization. The organization usually has to react to those factors rather than influence them. The degree to which this reaction is successful depends largely on how well the organization has planned and prepared itself and its resources. Market spaces shift, economies rise and fall, natural disasters occur, governments change programs and priorities, and so on. The organization has little influence over these types of factors but can prepare itself by training its personnel, investing its capital in long-term projects that may withstand market shifts, diversifying its business operations, creating alternative and redundant sites, and so on, to prepare for these unpredictable environmental factors. Again, these are factors that are usually reacted to but not easily controlled.

Threats

Because business processes and initiatives are so widely different between organizations, it's probably difficult to nail down specific threats that could affect these elements, other than simple generalization. Threats that affect business processes and initiatives include things that are caused by both external and internal risk factors, such as IT platforms, new and emerging technologies, software and system supportability, and so on. These particular factors, focused on the information infrastructure, can affect business processes simply because technology is a direct enabler of business. So, business processes could be greatly enhanced by using new technologies, or even be hindered by them because of the lack of training or supporting infrastructure the organization may have when implementing new technologies. Since it is a possibility, this is a potential threat if not handled correctly by the organization. Most organizations find that there is a fine line between threat and opportunity in the business world.

Vulnerabilities

There are, of course, vulnerabilities inherent to a business's processes and initiatives that threats can take advantage of. Again, it's difficult to state vulnerabilities beyond basic generalization simply because they are so specific to a particular business, with its mission and processes, that is operating in a particular business environment. However, there are several general vulnerabilities that can apply here. Some of the vulnerabilities that may influence the business processes include dependency on older technologies, lack of trained personnel, inflexible business processes or methods, an unwillingness to change or adapt to new technologies and processes, lack of interoperability, lack of security, and so on. All of these vulnerabilities could negatively affect the business if corresponding threats were to exploit them.

For instance, if a business has a dependency on older technologies, it may not be easily able to interact with new markets or business partners that use newer technologies, systems, data formats, and information-processing methods. It also may not be prepared to interact with other businesses that use social media or the Web for product marketing and delivery. So, this would be a serious vulnerability inherent to its business processes. Another example may come from an organization's culture. Suppose the key staff members have been in their positions for years and have adopted a "that's the way it's always been done" attitude toward processes and technologies and are reluctant to change based upon new market situations, accelerated development and product delivery requirements, and new enabling technologies. These attitudes are cultural in nature but are vulnerabilities because they may directly affect an organization's ability to change to be more flexible or even secure processes or technologies.

Project and Program Management

Organizations use project, program, and portfolio management to manage and sustain both short- and long-term aspects of systems and processes. These categories apply to the scope and scale of different sets of activities or processes within an organization. *Projects* are limited-duration sets of activities geared toward a particular goal; *programs* are ongoing and longer-term and may also encompass several individual projects, as well as other activities specific to processes that may have an indefinite duration. *Portfolio* management is the oversight and management of several different programs by a senior person in the organization. Keep in mind that the major difference between a project and a program is duration; a project has a definite beginning and ending, while a program is indefinite.

At the core of a project, three elements are the primary drivers. They are scope (amount or range of work), schedule (when work is to be done and its completion date), and cost (including all of the resources that are expended toward the completion of the project). All projects depend on these three elements to ensure success. Any shortfalls in cost, delays in schedule, or out-of-scope work (also called *scope creep*) affect the ability of the project to succeed on time, within budget, and with all of the agreed-upon work completed. We'll discuss the risk factors that can affect all three of these elements next.

Risk Factors

Since the three major elements of a project or program are scope, schedule, and cost, risk factors associated with projects and programs primarily affect each of these elements. Factors that affect scope usually come from disagreement on exactly what work has to be accomplished, in what order, and who will do it. These factors should be examined and agreed upon during the requirements process, where the project is formally scoped. In complex projects, factors that may affect scope include the necessity to task workers from different sections or departments, the exact amount of work to be done, in what order it will be done, and the priority of each task and subtask. Political culture within the organization can adversely affect scope as well, since there may be disagreement between departments or executives on what work is actually required and whose responsibility it is to accomplish it.

The scheduling component of a project has several risk factors as well. The amount of work to be done (scope) affects the schedule as a risk factor because of the time given to accomplish a specific amount of work and the resources allocated to this work. Lack of workers or materials adversely affects the schedule, as does the availability of equipment, the work location or site, and external factors such as contract negotiations, government shutdowns, and so on.

Cost risk factors stem from lack of budget control during the project, including an inaccurate budget or estimation of cost, unexpected expenditures, weak economy, and so on. Project costs are affected by the costs of labor (to include wages, insurance, and benefits), as well as the costs of supplies or materials needed to complete the project. Additionally, since all three of the elements of scope, schedule, and cost are also risk factors for each other, a delay in schedule or any extra, out-of-scope work impacts the project budget and costs.

Other risk factors for projects include training and staffing the project with the right mixture of personnel who have the right skill sets, attitudes, and focus on making the project or program a success. A manager without the right project management skill set is a risk factor that can affect scope, schedule, and cost if that person does not manage those three critical elements properly. A technician without the right technical skills may cost the project more money in training or delay work unnecessarily because of rework or slow production.

In addition to factors such as scope, cost, and schedule, adding an indefinite or longer-term duration affects programs as a risk factor because you must project how they will be staffed, funded, equipped, and otherwise managed in the future, over a longer, indeterminate period of time. So, risk factors are not only short-term but could be long-term and fluctuate over that time period. Factors such as market, economy, and technology changes will influence risk in a program much more so than a project, affecting its scope, schedule, and cost over a longer period of time.

Threats

The threats to a project or program are similar; the major difference is the duration of the time that the threat represents potential harm to a project or program. Keep in mind that threats for a project or program aren't those you might traditionally think of as

threat sources; they are rarely malicious in nature and come from the business environment itself. For example, threats to cost are usually those that involve money or resource issues, such as price increases, currency value fluctuation, stock market variations, and so on. These are usually external threats; internal threats to costs might include a sudden budget restructuring, cutting funds for a project, bankruptcy, and so on. Threats to the schedule might include worker shortage, strikes, inadequate training, delays in contract negotiations, delays from suppliers, and so on. Scope threats usually involve additional work because of faulty requirements gathering and decisions about what actually falls into the project's scope and scale.



NOTE Sometimes it's difficult to distinguish between threats to each of these elements individually and threats that actually affect all three project elements simultaneously because it is more often the case that any threat affecting one element will usually, even indirectly, affect all three.

Vulnerabilities

Since vulnerabilities are weaknesses, or a lack of protective controls, the vulnerabilities found in project and program management are inherent to weaknesses in their critical elements and processes. For example, a weakness often found in the cost element of a project or program is a failure of the organization to adequately budget for all of the resources required for the project. The organization may not list every piece of equipment or every major supply it needs or take into account labor costs such as overtime in the event of a schedule slippage. It may not adequately negotiate firm prices with a supplier, who then may raise prices on critical parts or equipment. These are all vulnerabilities inherent to the budgeting and cost element of a project.

Scheduling also has some common vulnerabilities associated with it. If an organization fails to build in potential scheduling delays such as work stoppages, dependencies on other organizations to fulfill parts of the schedule, or even holidays, this can lead to problems with completing the project on time. Another scheduling vulnerability is to incorrectly estimate the amount of time it takes to perform a task or get a piece of work accomplished.

Vulnerabilities inherent to the scope element of a project affect how much work has to be done, in what order, and by whom. A *work breakdown structure* (WBS) is a document that the project manager develops that covers exactly all of this information, and more. The WBS describes, in excruciating detail, the work, its subcomponent parts and tasks, what skill sets are needed, and what resources are required to do the job. Other documents may break down individual tasks into much more detail, even describing step-by-step how a task is accomplished. If the project manager and team do not create these documents, this is a weakness in that the work may not be performed exactly as needed. Resources may not be adequately allocated for the work, or the work may be performed by unskilled people. Additionally, the amount and quality of work may not be performed to requirements. Failure to set requirements initially in the project and to periodically check and track the work against those requirements are also vulnerabilities associated with scope because this can affect whether the work meets the established requirements.

Risk Factor	Threat	Threat Agent	Vulnerability	Affects
Unstable economy	Cost increases for critical parts	Supplier	Tight budget or inexact budget estimates	Cost
Inability to accurately define scope during requirements meetings	Scope creep; inexact work specifications	Different department managers and supervisors	Lack of defined scope or work specifications	Scope
Manufacturing expensive parts for sensitive components	Delays because of inability to receive spare or replacement parts	Supplier	Lack of critical parts	Schedule
Training levels/skill sets	Incomplete or shoddy work	Untrained worker	Precision or delicate work required	All

Table 2-4 Summary of Project Risk Factors, Threats, and Vulnerabilities

An additional vulnerability that simultaneously affects all three project elements is the failure to monitor or control all of these elements on an ongoing basis throughout the life of the project or program. Scope, schedule, and cost must be monitored on a continuing basis to ensure that they meet the original requirements set forth in the project's charter. The project or program manager must monitor and control these things to prevent cost overruns, schedule slippage, and scope creep. Failure to monitor or control these elements is a serious vulnerability and could jeopardize the success of the entire project or program. Table 2-4 gives examples of some of the risk factors, threats, and vulnerabilities related to project and program management.

Third-Party Management

In today's business world, an organization rarely functions independently from any other entities. Most businesses are not entirely independent and self-sustaining; they depend on other entities, such as suppliers, service providers, and so on, to help them bring their products and services to market. These third parties often perform services that are outsourced from the organization because of a lack of infrastructure or simply a desire to not perform these functions or services internally. A great example of a third-party service provider is one that provides cloud services to businesses, such as data storage, applications, and even entire infrastructures to organizations that don't have the means or the desire to create the internal structures needed to manage them internally. Sometimes it is more cost effective for an organization to simply hire a third party to perform a function or provide a service than it is to expend the resources to create and maintain all of the equipment and processes itself.

Sometimes a portion of the risk an organization incurs during a particular business or IT effort can also be offset by a third party. Transferring risk includes the use of third

parties to bear some of the risk in performing certain business functions. Insurance is the classic example of transferring risk used in most risk management training texts, but this instance usually only provides monetary funds in case of a disaster or liability scenario. Transferring risk to third parties also includes outsourcing certain functions and services to third parties, so this, too, is a standard risk treatment method. The organization, for example, can reduce its risk of accounting and budget errors with a small, untrained staff by outsourcing its accounting functions to a third-party accounting firm. It's important to note that while this strategy of dealing with risk is effective and common, the organization is transferring only risk, not responsibility. The organization almost always retains final accountability and responsibility for functions and services outsourced to a third party. For example, transferring a business's accounting functions to an outside firm mitigates risk by transferring some of it to the third party, but the organization is still ultimately responsible to its stockholders, government regulators, banks, and financial obligations, even if the accounting firm makes an error. As another example, an organization that makes use of cloud data storage services still maintains accountability and responsibility for any data stored with a provider if the provider suffers a breach that results in the release of sensitive information. While third-party providers may still incur some level of liability in these cases, the final liability rests with the organization that contracted with them. Liability, accountability, and responsibility are also some of the key risk factors with third parties that we'll discuss next.

Risk Factors

As indicated earlier, several risk factors relate to the legal aspects of dealing with third-party providers. Most of these risk factors deal with trust in the third-party provider or in dependencies the organization may have on the provider services. For example, the organization must be able to trust that the third-party provider will provide adequate security for any data that is maintained in its infrastructure. In addition to trust as a risk factor, risk factors include interoperability with existing systems in the organization, data protection and security, and legal liability. Remember we said earlier that an organization can outsource risk to third-party providers, but the organization typically retains accountability, responsibility, and legal liability. Some legal liability, however, is levied on the third-party provider since it has a duty to provide services, as well as assurances that those services will meet certain legal standards, as written in the contract between the provider and the organization.

The risk factors relating to third-party providers depend upon the types of services provided, as well as how the contract agreements are set up between the organization and the provider. A document known as a *service level agreement* (SLA) is the key to reducing risk factors when dealing with a third-party provider. The service level agreement stipulates what the third party must provide in terms of level of service, performance, and so on. It could also specify what security measures a third-party provider must take in order to protect any organizational data in its custody.

Threats

Like the risk factors mentioned earlier, threats associated with dealing with third-party providers primarily relate to trust and the contractual and legal aspects of those arrangements. Threats include failure to provide services as specified in contracts, failure to meet

performance or security levels, failure to protect data, and loss of availability for systems or data to an organization's users. Third-party providers can certainly succumb to some of the same threats that the organization would, such as natural disasters and so forth. So, some of the threats could also include loss of service or data for the business in some of these negative events. Third-party providers are also susceptible to hacking and malicious insiders, the same as any organization would be. Therefore, threats of data loss or disclosure are also present with third-party providers.

Vulnerabilities

Vulnerabilities that result from associations or dealings with third-party providers include failure to adequately cover contingencies in contractual agreements, such as system or data availability or loss, security protections, and service levels. Furthermore, any vulnerabilities that the third-party provider has inherent to its own organization are, unfortunately, indirectly incurred by any organization that deals with the third party since those vulnerabilities could affect data in its custody or services it must provide to others. Examples of internal vulnerabilities that could affect organizations for whom the third party provides services include infrastructure vulnerabilities (such as loss of equipment or hacking), organizational vulnerabilities (such as loss of revenue or bankruptcy), or even technological vulnerabilities (such as lack of sufficient encryption strengths or strong authentication methods). All these vulnerabilities could indirectly affect any organization that has a contractual agreement with a third-party provider.



CAUTION Remember that even if risk is transferred to a third party, accountability and responsibility usually remain with the business.

Systems Development Life Cycle

The systems development life cycle (also sometimes referred to as the *software development life cycle*, if only software is involved), or SDLC, is essentially the entire life of a system, product, or piece of software. The life cycle covers every single aspect of a system or product, from concept to development and from implementation to disposal. There are several popular systems development life cycle models, including waterfall, iterative, and so on. We won't cover any of these models here because an in-depth discussion on them would take an entire book. However, we will mention some of the more generic parts or phases of the SDLC and briefly describe them so that we can put them in the context of risk factors, threats, and vulnerabilities.

At the basic level, the SDLC consists of several phases that include conceptualizing the system, discovering the requirements for the system, designing its architecture, developing the system, testing that it both is a single unit and is integrated with larger systems in its environment, implementing the system, and, finally, disposing of it after it has reached the end of its useful life. Each phase of the life cycle has different aspects that include planning, management, resourcing, and so on. Each also has inherent risks. We'll discuss these phases generically in the next few paragraphs. Note that some of the names we give to the different life cycle phases may vary among different life cycle models, but

in general, the concepts are the same. Also note that some models are linear, in that they progress in a sequential manner only, and some are cyclic in some way (repetitive, recursive, or iterative), where a system can be re-introduced into an earlier phase for updates, for upgrades, or to fix problems or issues.

The first phase of the SDLC normally involves some type of conceptual planning process, where the need for the system is determined and a general idea is developed of what the system needs to do and what purpose it will serve. Some models refer to this as the *initiation phase*. During this phase, the feasibility of developing or acquiring a system is studied and includes considerations such as when the system is needed; how much it might cost; what type of staffing it might need to develop, implement, maintain, and support it; what other systems it might need to connect to or interface with; and so on.

The next phase of the SDLC is generally the *requirements phase*, which is typically named as such in most models. During this phase, different sets of requirements are developed. These requirements might include functional requirements, performance requirements, security requirements, and business requirements. Requirements dictate concrete terms, such as what a system is exactly supposed to do, how it will do it, to what degree, and what standards it must meet. Without a clear set of requirements, there can't be any good traceability back to what the system was supposed to do in the first place. That's why it's important to try to accurately cover all the possible requirements and needs the system may have to meet. This is also where the scope of the development process is established.

The next few phases can be a bit different based upon the model under discussion and whether the product being developed is a system or software. System developers move from the requirements phase into designing the architecture, in terms of developing a general high-level design of how the system is supposed to work, what major components it might have, and what other systems it might interface with. Software developers similarly might design software architecture at a higher level during this phase. As the SDLC development processes move forward, this overall architecture is decomposed into smaller pieces, until finally individual components or pieces of code are developed. Again, how this design process progresses depends upon which model is being used.

After the design phase, there must be decisions made as to whether to build a system or software or simply acquire it from a third party. Some systems or software can be bought from other developers, but some must be developed specifically for the end application or use. If the system is to be acquired from an outside source, the design specifications are provided to that developer, and they should, in turn, provide a system or software that meets the requirements and design. If the system is to be developed, then the next phase of the SDLC comes into play. During this phase, software is written, and systems are assembled from individual components.

Following the development phase, many SDLC models include a test phase. In the test phase, different aspects of the software and systems are tested. There are many different tests that can take place during this phase. Some of these tests might involve unit testing, which simply means to test an individual component or unit of software

at its most basic level for functionality and performance. Integration testing, another type of testing, usually involves testing the overall function and performance of all the components of the system or pieces of software working together, as they would when assembled. During this phase, other types of testing could take place, including interface testing (testing different aspects of the system when it interfaces with other separate systems in its environment) and security testing (which may include compliance testing, vulnerability testing, and even penetration testing).

Once a system has been tested and accepted, the implementation phase usually follows. In this phase, systems and software are actually put into production and used for their originally intended purpose. Some development models describe an overall implementation phase that includes the day-to-day maintenance and operations of the system. Other models move from the implementation phase to a more long-term maintenance or sustainment phase for the product. Regardless of how the phase is described in the model, during these phases the system is used, undergoes minor maintenance and upgrades, and is periodically tested to make sure it still meets its original design and requirements.

Once the system has been in operation for a while, it may eventually be superseded or replaced by a more efficient or updated system. When the system is replaced or removed from the environment, it is said to have entered the *disposal phase*. Some models refer to this as the *retirement phase*. During this phase the system is taken out of production, is dismantled, and is no longer used. Its components may be reused, or they may be disposed of. Figure 2-2 illustrates the generic SDLC model.



EXAM TIP While you will likely not be expected to know the details of any specific SDLC model, be familiar with the generic phases of the SDLC: Initiation, Requirements, Design, Development, Testing, Implementation, and Disposal. Also keep in mind that different models may refer to these phases by different names or even combine or separate phases to some degree.



Figure 2-2 The generic SDLC model

Risk Factors

Most of the risk factors inherent to the SDLC affect both the entire model and each of the phases separately. Since the SDLC could be considered to have several different facets, including a management process, an engineering framework, and even a methodology, you could say that risk factors that affect the SDLC are also common to other types of processes. For instance, earlier we discussed risk factors that affect project and program management. These risk factors affect scope, schedule, and cost. The SDLC suffers from similar risk factors because each of the phases, as well as the SDLC as a whole, has different scope, schedule, and cost elements. Each of these phases can also be affected by risk factors that impact the availability of resources (including manpower, funding, equipment, facilities, and so on), such as management commitment and organizational structure.

Unique risk factors that affect the SDLC include those that affect system changes, those that affect system configuration throughout the life cycle, and those that affect releasing different versions of the system as updates take place. Most of these elements occur during implementation, maintenance, and sustainment of a system but also can occur in other phases of the SDLC where multiple versions of a system are fielded simultaneously, as well as in models where there is a continual iterative process of updating and upgrading a system or software. Risk factors that affect system changes include how well the change and configuration management processes work and how changes are implemented into the system. Change and configuration management processes that are not well managed are risk factors because this could cause changes that are not documented or not tested for security, functionality, or performance. Additionally, factors such as the complexity of the system, how the organization is structured to manage the systems development process, and how rapid system changes occur are potential risk factors.

Threats

Threats to the SDLC manifest themselves when systems are produced that are not interoperable or compatible with other systems and their environment or systems that are not secure. Other threats might include systems that do not meet the requirements they were originally intended to meet. These threats would definitely affect both the functionality and the performance of the system. Threats to the design process include faulty design specifications, as well as faulty requirements input from the previous requirements phase. Most of the threats to the SDLC come in the form of mismanagement, miscommunication, incorrect expectations, and lack of a commitment of resources or expertise.

Vulnerabilities

Many different vulnerabilities can affect the SDLC; again, a great many of them were previously discussed as also affecting the project or program management process. These vulnerabilities affect scope, schedule, and cost, of course, but can also affect the quality of the system or product. In addition, the system's security, functionality, and performance are also affected by these different vulnerabilities. While there are probably too many to list here, examples of vulnerabilities that affect the SDLC start with a lack of firm requirements and mixed expectations from the different system stakeholders. A lack of documentation in all phases is also a significant vulnerability to the entire SDLC but

particularly to the requirements and design phases. Failure to develop solid design specifications and systems architecture is a vulnerability that can result in a faulty design that does not meet system requirements. In the development phase, lack of adequate consideration for system interfaces, as well as how subcomponents fail to support higher-level components or meet technical requirements, can result in a shoddy system or software. Failure to properly and thoroughly test systems, as well as their interaction with their environment, may mean that serious functional or performance issues with the system are not discovered until well after it is put into production. Vulnerabilities in the implementation phase include faulty implementation, lack of traceability to original requirements, and failure to properly maintain a sustained a system after it has been put into production. And lastly, vulnerabilities associated with the disposal or retirement phase of the SDLC can result in systems that are not properly replaced or not securely disposed of. This can cost the organization money and potential liability.

Emerging Technologies

New or emerging technologies can present risks to organizations simply because there are several different important considerations when integrating the latest technologies into the existing infrastructure. Many organizations have an unfortunate tendency to rush out, buy, and attempt to implement the latest and greatest technologies on the market, without careful planning or consideration of the existing infrastructure and how it will react to the new technologies. One of the primary considerations organizations must look at is making a business case for the new technology, which may be to fill a gap that the older technology does not provide or to provide a capability that the organization must now have to compete in the market space. In other words, the company really must justify new technologies to make them worth the risk they could incur.

Risk Factors

Emerging technologies have several risk factors inherent to their integration into the existing infrastructure. If the organization has been able to justify the implementation based on a true business need for the emerging technology, it must consider several risk factors. One of the major risk factors is interoperability with existing infrastructure. Frequently, newer technologies don't always work properly with older systems right out of the box; there may be adjustments that need to be made to the existing infrastructure to integrate the new technology, or bridging technologies may be needed to connect the two. Interoperability doesn't just involve the right connections; it can involve data formats and flows, security methods, and interfaces into other systems. These considerations, and many others, are risk factors that must be taken into account before acquiring and integrating new technologies.

Another risk factor is security. New technologies may have security mechanisms that are not necessarily backward compatible with existing ones. Examples include encryption algorithms and strengths, identification and authentication technologies, integrity mechanisms, and even redundant or backup systems. Additionally, the systems may involve a learning curve that may intimidate users who must now learn new security methods for the system. The human factor can be a weak link in the security chain, so either a lack of training or a lack of adaptability to the new security mechanisms can introduce risk.

Earlier, when we discussed the SDLC model, we pointed out that system updates and changes can be risky if not managed properly. Integrating new technologies into the environment with older ones can introduce both intentional and unintended changes into the environment, affecting the stability of the organization's SDLC with a particular system, so change is also a risk factor. Even in the disposal or replacement phase of the SDLC, introducing new technologies to replace older ones can be problematic if not planned and executed properly. New technologies that are not adequately tested for functionality, performance, integration, interoperability, and security may not be able to adequately replace older systems, resulting in extended costs and possibly even requiring the extension of the older systems' life cycle.

Threats

Threats resulting from the introduction of new and emerging technologies into the existing infrastructure are numerous. If the organization has failed to adequately plan for the new technology, then these threats can become significant. Some of these threats include untested or unproven technologies, noninteroperability, incompatible security mechanisms, and suitability of the technology for use in the organization. The organization could also incur additional cost and require more resources because of a faulty implementation. These threats can be minimized by careful planning and integrating new technologies using a stable SDLC model.

Vulnerabilities

As with threats, vulnerabilities that go along with working with emerging technologies are numerous as well. Vulnerabilities could include a lack of trained staff committed to managing and implementing the new technology. Lack of adequate project planning is also a serious vulnerability that could affect the organization's ability to effectively integrate new technologies. Another vulnerability could be a weak support contract or other type of warranty, guarantee, or support for a new technology or system. Most of these vulnerabilities appear when the new technologies are first implemented and tend to become mitigated or lessened as the technology is integrated into the existing infrastructure but still exists.



EXAM TIP The key areas of concern with emerging technologies are interoperability and compatibility. These two concerns affect the security, functionality, and performance of the new technologies when they are installed into an existing infrastructure.

Management of IT Operations

Managing the IT infrastructure is one of the most work-intensive efforts in an organization, especially in a larger business. The IT infrastructure in an organization covers a broad scope of areas. Infrastructure, of course, covers employee workstations, printers, and other end-user devices. It also covers the major pieces needed to conduct business, such as servers, cabling, switches, routers, and a variety of other network and security devices.

Most organizations also include wireless networks in their supporting equipment. Additionally, infiltration of mobile devices into businesses makes this a new and sometimes difficult area to bring under the organization's infrastructure umbrella. Challenges with the IT infrastructure include not only maintenance, upgrades, updates, and implementing new technologies but also include some of the more typical traditional management challenges, such as budgeting, project management, and staffing.

Key areas in IT operations management include server and infrastructure management, end-user support, help-desk and problem escalation management, and, of course, cybersecurity. IT managers must maintain and meet any internal agreements that cover guaranteed service delivery in support of the different divisions within the organization, as well as service level agreements with other organizations. While information security personnel tend to focus more on IT risk, we find that most of the risk factors, threats, and vulnerabilities affecting IT also affect all the operations within the business. In the next few paragraphs, however, we'll focus on those that directly affect managing the IT operation in an organization.

Risk Factors

The management of IT operations incurs risk factors previously discussed in other sections of this chapter. These include the size and complexity of the organization and its IT infrastructure, the criticality and priority of the different systems that make up the infrastructure, and the internal management processes of the organization. Resourcing issues also affect the management piece of IT operations, such as staffing the right people who are trained on the various technologies the organization needs and creating and maintaining a budget that supports maintaining the current level of support, as well as future growth for IT. Additionally, compliance with legal and governance requirements in the face of increased regulation is a risk factor the IT managers must deal with.

Organizational structure also affects IT operations because the IT infrastructure may be managed on either a centralized or decentralized basis, sometimes by one centralized IT shop or, in the case of larger organizations, by multiple areas within other divisions that are delegated the task of managing their own piece of the infrastructure. IT might also be managed on a functional basis; the accounting and human resources divisions may have responsibility for managing the systems that support their mission. Additionally, the IT infrastructure may be managed on a geographical basis, in the case of physically separated locations in large organizations. All of these structural considerations are factors that contribute to risk in managing IT operations.

Also directly affecting IT operations risk are two key processes: the change and configuration management processes. We've already discussed risk factors that affect the SDLC model in an organization, as well as how new and emerging technologies can affect the existing infrastructure. These same risk factors also directly affect the daily management of IT operations simply because they introduce change into the network. Some of this change can be planned and carefully introduced, but often there is change, from the large-scale network side all the way down to individual configuration items on hosts, that may cause unforeseen changes and affect the network in different ways. How the organization deals with change and configuration management is a risk factor that affects not only the SDLC but also the day-to-day operations management.

Threats

Threats that affect the IT operations are similar to those that affect other areas of the business and can be external or internal threats from a variety of sources. Some of these threats have a ripple effect in that they may first affect other areas of business and in turn affect IT. For example, the threat of a poor economy may affect the profitability and sustainment of the business, resulting in making cuts, which often include IT personnel or equipment. Obviously, there are also direct threats to the daily management of the IT infrastructure. These include external threats such as hackers, of course, but also more common ones such as increases in cost to maintain operations, issues with external service providers, and disaster-related events (weather, fire, and so on). Internal threats can include those carried out by malicious insiders or even careless employees, such as theft, sabotage, accidental equipment breakage, and so on. Internal threats can also come from management processes and include budget cuts, loss of trained personnel, shifts in organizational priorities, and transitioning from one market segment to another.

Vulnerabilities

Technical vulnerabilities are beyond the scope and purpose of this book; our focus here is on those associated with the IT management aspect of the organization. Vulnerabilities affecting IT management include faulty processes and procedures, lack of resources, and lack of trained technical personnel. An end-user population that has not been trained or held accountable for proper care and treatment of the infrastructure can also be a vulnerability. Other vulnerabilities might include a lack of infrastructure monitoring, lack of control of sensitive information in IT systems, and failure to maintain a stable SDLC throughout the entire infrastructure.

Data Management

Data management is a holistic way of controlling all the various information and data that the organization uses and processes and includes considering its various formats, how it is used, how it must be stored and transformed, and, of course, the confidentiality, integrity, and availability of the data. While we won't be discussing the technical aspects of a database management system (DBMS), we will discuss some of the various aspects of managing data processed in those systems, as well as what risk factors they face, threats to data, and vulnerabilities that plague data and database management systems.

Information technology and security personnel are responsible for the systems that process data, as well as keeping data secure from a technical perspective. However, typically there are personnel in the organization who are formally assigned as the responsible party for the overall management of a particular class or set of data. That position is called a *data owner*. The data owner has overall responsibility for determining who should access data, determining how it should be used, and making decisions regarding its security and processing. In coordination with both technical and risk management personnel, the data owner should be cognizant of risk potential with data in database systems.

Risk Factors

Some of the risk factors we're discussing in this section are part of a recurring theme; the nature of the organization itself, including its market segment, how large it is, and how complex it is affect not only the system aspects of IT in the organization but data and database systems as well. Data in particular is subject to unique risk factors. Depending upon the sensitivity or confidentiality of data, it may be subject to regulatory considerations that affect risk. Laws and regulations may require that data be protected in specific ways and at certain levels. Another risk factor might be the type of systems that data has to be processed and transformed over. Some of these many systems may be incompatible and require that data be in prescribed formats. If the data is not natively in one of these formats, it may have to be transformed or changed into a different type of format. For example, data in a flat-file database may have to be transformed in order to be fed into a relational SQL-based database so that it can be used by another system. Data formats, such as text or binary, also are factors in transformation. When transformed, there's a risk that data may be lost or changed in unexpected ways. During the data transformation process, the organization has to take care that sensitive data is not unintentionally modified or available for unauthorized personnel.

There are also risk factors that affect the availability of data. Backup types and schedules, as well as processes on how to correctly back up organizational data, are risk factors that affect availability. Additionally, backup systems that may be antiquated or may not have the capacity for the organization's data can be factors. If an organization uses its own infrastructure to store and process data, then trained personnel and adequate equipment can affect backups. If an organization outsources to a cloud provider, for example, availability is still an issue if the organization has not adequately planned for contingencies by negotiating them into the cloud provider agreement.

On the lower technical levels, database design can be a risk factor if it does not adequately account for all the different data elements, their formats, and security mechanisms built in to limit unauthorized access. Scalability can be an issue with database design, in that the organization may be using systems that aren't scalable as more and more data is fed into them or that aren't accessible by large numbers of users in the enterprise simultaneously. These are risk factors that relate not only to design but also to the database management system selected for use in the organization.

Threats

Most of the threats that are common to data and database systems directly affect confidentiality, integrity, and availability. Confidentiality threats come in the form of unauthorized access to data that ranges from unintentional access by unauthorized employees to malicious insiders who purposefully attempt to access data to outside hackers who are actively trying to infiltrate the organization's network and steal or modify data. Integrity threats are a large concern with data simply because unauthorized modification can result in many different types of processes in the organization being conducted with errors. These can include financial transactions, healthcare transactions, or even erroneous transactions with personal data. Finally, threats that affect availability include accidental or intentional deletion of data, database system downtime, or any other instance where users can't access the data they need in order to do their job.

Vulnerabilities

Likewise, vulnerabilities that data and database management systems incur also directly affect the three goals of security: confidentiality, integrity, and availability. From a confidentiality perspective, vulnerabilities might include the lack of adequate permissions on database objects, such as tables or queries; lack of encryption for sensitive data; and failure on the part of the data owner to adequately classify data based on sensitivity level. Integrity vulnerabilities might include lack of permissions for personnel authorized to change data, inability of the database system to control changes to the data, lack of a transaction checking or rollback process in DBMSs, and, of course, old, unreliable storage media that might affect data stored on it. Vulnerabilities that might affect availability could include inadequate or faulty backup processes, lack of trained personnel, outdated equipment, equipment that doesn't have the capacity to handle the organization's data backup requirements, lack of redundant systems or capabilities, and so on.

Business Continuity and Disaster Recovery Management

Business continuity and disaster recovery management are necessary parts of running a business, regardless of its market area. This is because incidents, disasters, and other negative events happen to all organizations eventually, in spite of the most favorable conditions and the most careful planning. Remember during our discussion in Chapter 1 about the three goals of security that availability is one of those goals. Business continuity and disaster recovery are primarily concerned with the availability goal. There is actually a whole area of expertise dedicated to this goal with these processes in mind; sometimes it's referred to as *continuity management*.

One thing to keep in mind is the difference between business continuity and disaster recovery. Business continuity is concerned with the careful planning and deployment of resources involved in keeping the mission of the business going, that is, keeping the business functioning regardless of negative events. This process is more long-term and requires continual commitment from the organization. Disaster recovery, on the other hand, is primarily concerned with the quick reaction involved with preserving lives, equipment, and data immediately following a serious negative event. Disaster recovery is (ideally) a short-duration process and does not concern itself with conducting the daily mission of the business. Business continuity is more concerned with the long-term survival of the business, while disaster recovery is more concerned with the short-term process of reacting to a disaster. While closely related, these two efforts are not the same thing; in fact, disaster recovery could be viewed as a subset of the activities that go on during overall continuity management strategy.

Business continuity planning involves several steps. Since the focus of this chapter isn't solely on the subject of business continuity and disaster recovery, we're not going to go into an in-depth treatment on these processes. However, we will discuss some of the basic concepts of business continuity and disaster recovery as they relate to risk. Two of the key processes involved in business continuity planning are conducting a *business impact assessment* (BIA) and determining a recovery strategy. A business impact assessment closely

resembles some of the steps you would take during a risk assessment simply because you are identifying assets (which include, of course, people, equipment, facilities, and processes) and prioritizing those assets. The reason they are prioritized is that, in the event a disaster were to occur, the business would have to rely on certain assets or processes more so than others in order to get back in business. These critical assets or processes should be brought back online and recovered first, but in order to accomplish this, they have to be identified by the organization, and plans have to be made for their recovery. That's where the business impact assessment comes in. The organization must identify critical processes and assets, prioritize them for recovery, and, additionally, measure the impact on the business if those assets or processes were lost for any given amount of time because of an incident or negative event.

Two key areas of concern in business continuity are the *recovery point objective* (RPO) and the *recovery time objective* (RTO). Both of these areas can be measured in the context of time. The recovery point objective is the amount of data that can be lost, based upon a time measurement. In other words, if the recovery point objective is two days, then the most amount of data that can be lost without a serious effect on the organization's ability to function would be two days' worth of data. Note that this measurement isn't concerned with the actual amount of data in terms of quantity, such as gigabytes, for example. It's concerned with measuring how many days' or hours' worth of data can be lost, at most, without impeding the function of the business. The recovery time objective, also measured in terms of time, is the maximum amount of time the organization can afford to lose before it starts recovery. This measurement of time could be days, hours, minutes, or even seconds.

The recovery strategy developed by the organization is a result of careful planning, as well as budgeting and allocating resources to the continuity management efforts. The recovery strategy should address most efficient methods of getting the business back online and functioning after properly responding to the critical needs of protecting people and equipment during the disaster itself. Keep in mind that recovering the business to an operational state does not necessarily mean it will be working at 100 percent of its previous operational capacity; the business may be able to get only a few key services up immediately following a disaster. The organization should take a realistic look at the degree of continuity possible, given the seriousness and scope of the disaster, its resources, the environment it is working with after the disaster, and the availability of people, supplies, infrastructure, facilities, and equipment. All of this should be considered in the recovery strategy planning.

Testing the disaster recovery plan is of critical importance; without testing the plan, the organization won't really know whether it's effective until a disaster actually occurs. Normally, that's a bit too late to find out that you haven't carefully considered all the different events that could occur during a disaster and how you will deal with them. Testing the plan involves making sure that people know what their responsibilities are, that they are well trained, that they have all the equipment and resources needed to adequately respond to disaster, and that they practice these responses. Testing the disaster recovery plan will point out deficiencies in training, equipment, resources, and response activities.



NOTE Much more information on business continuity and disaster recovery planning can be found in the NIST Special Publication 800-34, "Contingency Planning Guide for Federal Information Systems," which was written for use by government agencies but can be used by anyone or any business to help understand and plan for business continuity.

Risk Factors

Resilience is a term that refers to the ability of the business to survive negative events and continue with its mission and function. In other words, it could be said that resilience is the ability of an organization to resist the effects of negative events and its ability to bounce back after one of these events. Resilience can affect to what degree different risk factors, as well as threats and vulnerabilities, impact the normal business operations of the organization. A more resilient organization can better tolerate risk factors and the effects they have on the organization's ability to prepare for and respond to negative events.

There are various risk factors that can affect the organization's ability to respond to disasters, as well as continue the business and mission functions after it has recovered from the disaster. Some of these risk factors are inherent to the organization itself; these include size of the organization, its facilities, its people, and how well it has performed business continuity and disaster recovery planning. A higher level of management commitment to business continuity planning reduces the effect of risk factors on the business; less commitment may render the organization more susceptible to these risk factors. A larger organization may have more complexity in terms of numbers of people to take care of during a disaster, as well as numbers of critical assets or processes that must be planned for. Small organizations don't necessarily have an advantage, however; a small organization may have fewer resources to adequately plan for and address business continuity and disaster recovery.

Another risk factor that an organization could face is physical location and geography. For example, a business situated on the U.S. Gulf Coast is probably more susceptible to adverse weather, such as hurricanes and tornadoes, than a business located inland. Businesses that are located in areas that are prone to heavy flooding or have forest fires or extreme snow storms at various times of the year should plan for these weather conditions appropriately. Distance could also be a risk factor; if the organization is located farther away from population centers or infrastructure services (such as fire departments, police, hospitals, telecommunications providers, and so on), there is a greater risk that the organization could not adequately respond to a disaster.

Earlier in the chapter we discussed risks associated with third-party providers, and these providers can affect business continuity and disaster recovery as well. Yet another risk factor could be the degree of outsourcing the organization is involved with. A business that outsources some of its processes or key functions may have less control over those functions or processes during an incident or disaster. They may be at the mercy of the third party with whom they are contracted and subject to the third party's disaster recovery strategies (or lack thereof). Business continuity and disaster recovery are two areas that should be carefully considered when engaging in business with any external provider, usually through a service level agreement or other method.

In addition to the factors we discussed earlier, the nature of the organization's mission or business could be a risk factor. Organizations that have critical processes or produce critical goods and services that are time sensitive, for example, may incur more risk than an organization that can afford to be down or out of service for a few days. Time sensitivity can increase the impact of a disaster on an organization so should be considered when developing continuity and recovery strategies. Market factors, such as the perishability of goods, for example, can become risk factors that an organization must deal with as well.

Threats

Most people associate the threats involved with business continuity and disaster recovery with natural disasters. Obviously, there are the natural threats that exist, such as severe weather, earthquakes, fires, and so on. These are threats that can't be typically prevented or neutralized, but they can be planned for. Hardened facilities, adequate ventilation, fire suppression systems, and other physical or environmental controls can mitigate the damage from these threats. There are also human-made threats that can affect the ability of an organization to recover from an incident or continue to function. These can be broken down into unintentional and intentional threats. Intentional threats include those associated with hackers, terrorists, theft, and other malicious actors and activities. Unintentional threats may be attributed to accidents that are caused by carelessness, lack of training, and so on. All of these threats, both natural and human-made, are usually the type that cause incidents or disasters. However, there are also threats to the continuity management process.

Threats to the business's ability to manage its continuity and disaster recovery include incomplete or inadequate planning, as well as limited resources to carry out any business continuity planning (BCP)/disaster recovery planning (DRP) activities. Because of regulatory considerations in many cases, a business usually must have some degree of business continuity planning accomplished; the real threat centers on whether it is enough and adequately covers the different facets of recovery and continuity that the business must consider. Usually, inadequate planning or insufficient resources committed to this area are a result of shortsightedness on the part of the organization's leadership and management.

Vulnerabilities

A wide variety of vulnerabilities can affect the ability of an organization to respond to and recover from an incident or disaster. The same vulnerabilities can also in turn affect the organization's ability to continue to function at some level or degree after the disaster. Some of these vulnerabilities involve the lack of resources, such as a lack of personnel, lack of equipment or facilities, or dedicated recovery resources. For instance, if the organization has not acquired an alternate processing site, there may be no way it can quickly recover its operations back to a functional state. Other vulnerabilities include the lack of training for personnel tasked with disaster recovery or business continuity responsibilities. Additionally, there are also process vulnerabilities. Process vulnerabilities are those that result from a failure of the organization's management to adequately plan for, staff, and equip continuity management efforts. For example, a lack of management commitment is a vulnerability that will certainly lead to a lack of training, resources, and personnel dedicated to continuity management. An inadequate or nonexistent business

impact assessment is a vulnerability because an organization won't be able to adequately identify its critical processes or assets and determine how the loss of those critical items impacts the organization. Another critical vulnerability could be faced if the organization has failed to adequately test the response plan.



EXAM TIP Be familiar with the different business process areas and their respective risk factors, threats, and vulnerabilities. Remember that risk factors, while not a threat or a vulnerability, contribute to the overall risk of the organization by increasing or decreasing the likelihood or impact of threats exploiting vulnerabilities or the organization's resilience to negative events.

Chapter Review

In this second part of our discussion on Domain 1 topics, we covered additional information on threats, threat agents, vulnerabilities, and risk factors. We examined these different elements from a business perspective, rather than from purely a technological perspective. This is important because most of the risk a business incurs comes from engaging in the normal business operations, both day-to-day and strategically. We looked at risk from the different processes that go on in a business, such as the internal business processes, dealings with third parties, the systems development life cycle process, and business continuity and disaster management. We discussed the different risk factors, threats, and vulnerabilities that are inherent to each of these processes and how they introduce risk into the organization and affect its mission and goals.

Review Questions

1. For a negative event or action to materialize and cause risk to an organization or system, what other factor must be present?
 - A. Risk factor
 - B. Vulnerability
 - C. Threat agent
 - D. Threat
2. Which the following collects information about different actors and negative events that could exploit the vulnerabilities in a system?
 - A. Threat assessment
 - B. Vulnerability assessment
 - C. Compliance assessment
 - D. Penetration test

3. Which of the following terms describes an entity that initiates a threat?
- A. Threat agent
 - B. Vulnerability
 - C. Risk
 - D. Risk factor
4. _____ are elements that could influence the likelihood or impact of a threat exploiting a vulnerability or even influence the ability of the organization to withstand the effects of risk.
- A. Risk agents
 - B. Risk indicators
 - C. Threat agents
 - D. Risk factors
5. All of the following are considered external risk factors affecting business processes, except which one?
- A. Economy
 - B. Market segment
 - C. Organizational structure
 - D. Law and regulation
6. You are managing a project that involves the installation of a new set of systems for the accounting division of your organization. You have just been told that there have been budget cuts and the project will not be able to purchase additional equipment needed for the installation. You now have to find other areas to cut in order to fund the extra equipment. Which element of project management is most affected by this threat?
- A. Schedule
 - B. Scope
 - C. Cost
 - D. Quality
7. Which of the following is a vulnerability that affects the business processes that deal with third-party providers?
- A. Lack of a well-written service level agreement
 - B. Failure to test new technologies as they are integrated into the existing infrastructure
 - C. Lack of common data formats between internal systems
 - D. Failure to conduct a business impact analysis

- 8.** Failure to determine exactly what standards or needs a system must meet in terms of functionality, performance, and security is a vulnerability of which of the following phases of the systems development life cycle?
- A. Implementation
 - B. Development
 - C. Design
 - D. Requirements
- 9.** As a risk practitioner in a larger organization, you have been asked to review the company's SDLC model for potential risk areas. The model includes the Requirements, Design, Development, Implementation, and Disposal phases. Software and systems are moved from the development environment immediately into the production environment and implemented. Which SDLC phase would you recommend that the business add to reduce risk of integration or functionality issues as the system is implemented?
- A. Initiation
 - B. Test
 - C. Sustainment
 - D. Maintenance
- 10.** Lack of a well-written work breakdown structure document can contribute to a vulnerability that affects which aspect of project management?
- A. Cost
 - B. Schedule
 - C. Scope
 - D. Quality
- 11.** Which of the following are two elements that are critical in planning a threat or vulnerability assessment?
- A. Scope and scale
 - B. Threat agents and threats
 - C. Impact and likelihood
 - D. Vulnerabilities and risk
- 12.** Which of the following is the major risk factor associated with integrating new or emerging technologies into an existing IT infrastructure?
- A. Security mechanisms
 - B. Data format
 - C. Vendor supportability
 - D. Interoperability

13. You are trying to install a new system in the infrastructure. While testing its interoperability with the legacy systems on the network, you discover what may be issues with interoperable security mechanisms. You realize that you must use the strongest common security mechanisms that exist between the two systems. Which of the following related interoperability issues would contribute to increasing the risk involved with integrating this new technology into the existing systems? (Choose two.)
- A. The new system can use only AES 128-bit encryption or higher.
 - B. The new system can use either single-factor or multifactor authentication.
 - C. The legacy system can use only DES 64-bit encryption.
 - D. The legacy system can use only single-factor authentication.
14. Which of the following would be considered a direct internal threat to the IT operations management business process?
- A. Outside hacker
 - B. Unintended consequences from configuration changes
 - C. Market fluctuations
 - D. New regulations on data protection
15. Which of the following vulnerabilities could affect the management of the IT infrastructure within an organization? (Choose all that apply.)
- A. Failure to meet internal service level agreements
 - B. Failure of the business to succeed in a particular market segment
 - C. Lack of a service level agreement with a third-party provider
 - D. Lack of resources committed to explore new technologies
16. Which of the following is a vulnerability associated with the integrity aspect of data management?
- A. Faulty backup processes that do not completely back up all sensitive data
 - B. Lack of encryption for sensitive data being transferred between two systems
 - C. Failure to assign correct permissions to sensitive tables in a database
 - D. Failure of a DBMS to perform transaction checking on data
17. Which of the following organizational roles is responsible for determining data sensitivity levels, as well as who has access to sensitive data?
- A. System administrator
 - B. End user
 - C. Data owner
 - D. Security engineer

- 18.** Which of the following is a short-term process primarily concerned with protecting personnel, facilities, and equipment immediately following a disaster or major incident?
- A. Disaster recovery
 - B. Business continuity
 - C. Business impact analysis
 - D. Recovery point objective
- 19.** Which of the following would be a vulnerability that stems from the business not identifying its critical assets and processes during the continuity management process?
- A. Failure to adequately consider system requirements during the SDLC
 - B. Failure to perform a business impact analysis
 - C. Failure to consider interoperability with integrating new technologies
 - D. Failure to maintain redundant systems or data backups
- 20.** Your business just went through a major storm that flooded your data center. Members of your recovery team are attempting to salvage equipment, as well as locate critical data backups. No one seems to know exactly what they're supposed to do, and they don't have the right equipment available to them. Additionally, there is no coordinated effort within the team to perform specific tasks. Which of the following vulnerabilities most likely led up to this scenario?
- A. Failure to back up sensitive data
 - B. Failure to acquire an alternate processing site
 - C. Lack of a business impact analysis
 - D. Failure to test the disaster recovery plan

Answers

1. **B.** For a negative event or action (threat) to materialize and cause risk to an organization or system, a vulnerability must also be present.
2. **A.** A threat assessment collects information about different actors and negative events that could exploit the vulnerabilities in a system.
3. **A.** A threat agent is an entity that initiates a threat.
4. **D.** Risk factors are elements that could influence the likelihood or impact of a threat exploiting a vulnerability or even influence the ability of the organization to withstand the effects of risk.
5. **C.** The organization's structure would be considered an internal risk factor affecting its business processes.
6. **C.** Cost is the element of project management most affected by the threat of not enough funding.

7. **A.** A lack of a well-written, comprehensive service level agreement is a vulnerability that affects the business processes that deal with third-party providers.
8. **D.** Failure to determine accurate functional, performance, and security requirements for a system is a vulnerability inherent to the Requirements phase of the SDLC.
9. **B.** A test phase introduced into this model would reduce risk by ensuring that a system or software application meets performance and functionality standards before it is introduced into the production environment, potentially eliminating costly issues before they occur.
10. **C.** Lack of a well-written work breakdown structure document can contribute to a vulnerability that affects a project's scope.
11. **A.** Scope and scale are two elements that are critical in planning a threat or vulnerability assessment so the person conducting the assessment knows exactly what they are assessing and to what level of depth.
12. **D.** Interoperability is the major risk factor associated with integrating new or emerging technologies into an existing IT infrastructure, and it covers a wide range of factors, which typically include backward compatibility, data format, security mechanisms, and other aspects of system integration.
13. **A, C.** The encryption algorithms and strengths between the two systems are incompatible and will result in increased risk incurred because of their lack of interoperability. The other two choices are somewhat interoperable since both systems can support single-factor authentication.
14. **B.** Unintended consequences from the change management process are an internal threat to IT operations. The other choices are external in nature.
15. **A, C, D.** Failure of the organization to succeed in a particular business market area is typically not a vulnerability that would affect the management of the internal IT operations.
16. **D.** Failure of a DBMS to perform transaction checking on data is a vulnerability that could affect data integrity if the transaction is not processed correctly.
17. **C.** The data owner is responsible for determining access to sensitive data, as well as its sensitivity levels.
18. **A.** Disaster recovery is a short-term process primarily concerned with protecting personnel, facilities, and equipment immediately following a disaster or major incident.
19. **B.** Failure to perform a business impact analysis could cause a vulnerability in that the organization would not be able to adequately identify its critical business processes and assets.
20. **D.** Failure to test the disaster recovery plan on a periodic basis, as well as make sure that people are trained and have the right equipment, can result in poor or ineffective recovery efforts.

This page intentionally left blank

Identifying and Managing Risk Scenarios

In this chapter, you will:

- Understand how to identify and categorize risk factors
- Learn to develop and analyze risk scenarios
- Develop and manage a risk register

This chapter covers different aspects of managing risk scenarios within an organization as well as documenting and updating risks on a *risk register*. Now that we've discussed the fundamentals of risk and its concepts, as well as identified threats and vulnerabilities associated with business processes, we'll cover the other aspects of managing risk that occur before you even get the point of assessing or responding to risk.

The CRISC exam objectives we will discuss in this chapter include the remaining task statements that apply to Domain 1, as well as the first task statement of Domain 2:

- 1.3 Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations
- 1.4 Identify key stakeholders for IT risk scenarios to help establish accountability
- 1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile
- 2.1 Analyze risk scenarios based on organizational criteria (for example, organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk

We will also cover the supporting knowledge statements that support these objectives.

Developing and Managing Risk Scenarios

Risk management is the set of processes used to manage risk from the beginning of an endeavor all the way to the end. These are defined processes and include major activities such as risk identification, evaluation and analysis, and response. Note that these

activities are presented in accordance with ISACA's objectives and knowledge statements for the exam. These processes are generic but should be consistent with most popular risk management frameworks and processes. The end goal of the identification part of the process, the subject of this chapter, is to identify and document the risk scenarios associated with the organization, based on different risk factors. These identified factors and collected information are used to develop risk scenarios. While you may be able to evaluate and analyze aspects of risk after this process, this is a separate part of the process and is discussed in Chapter 4. You can also provide recommendations for risk response as part of this process, but understand that risk response is the primary discussion of Domain 3 and will be discussed in-depth starting in Chapter 5. For this chapter, we'll be looking at risk identification, classification, and risk factors, as well as how they help us develop risk scenarios.

Risk Identification and Classification

Before we delve into the process of creating risk scenarios, it is useful to consider the basics of how risk is identified and classified. This can help you frame the risk scenario, as well as assist in evaluating, analyzing, and developing a response for it later. There are different considerations in risk identification, some of which we have briefly touched on in the previous two chapters and will further refine here. Classifying risk can help put the risk, as well as factors that contribute to it, in perspective when developing both the scenario and its response actions.

Identifying Risk

To begin the process of developing risk scenarios, one of the first things you must do is try to identify what risks the organization is subject to. To identify risk, you must first identify all the components of risk that exist in the organization. This includes threats, vulnerabilities, and the assets the organization places value on. To acquire knowledge of all of these different elements, you may have to perform in-depth assessments to give you this information. For example, you'll have to inventory all of your assets and determine their value and priority to the organization. Value indicates how much they're worth to the organization; this could be in terms of dollars to replace an asset or how much revenue the organization will lose if that asset is lost. Priority could mean the relative criticality of the asset to the organization; this could indicate how much protection the organization believes an asset warrants and the urgency of protecting or restoring the asset (or the capability it provides) if it is lost. Although the terms *value*, *priority*, *criticality*, and *urgency* may seem to be ambiguous, they are all interrelated terms that the organization must define for each of its assets. For instance, assets that are deemed critical will likely have a higher value to the organization, as well as a higher priority for restoration if the asset is lost or damaged. There is a related term called *exposure factor* that describes the level of loss an asset could suffer; we'll discuss this term in Chapter 4 when we talk about quantitative and qualitative risk analysis techniques.

Classifying Risk Factors

Organizations attempt to classify risk for various reasons. First, to provide a point of reference to base decisions on, risk is classified by its consequences or the impact it has on

the organization. The organization may classify risk and its contributing factors by using subjective or objective (usually with numerical values) means and normally will correlate these values to thresholds the risk must meet in order for the organization to take certain action or commit resources to dealing with the risk. We'll discuss the subjective and objective classifications of risk in Chapter 4, where we discuss qualitative and quantitative risk assessment techniques.

Risk can also be classified as *internal* or *external* risk. Internal risk comes from the interaction of elements within the organization's control, such as internal governance (policy and procedures, for example), organization structure, and resources (for example, personnel, time, money, equipment, and so on) and business goals and strategy. These elements are decided upon and changed by the organization at its discretion, usually in reaction to external factors or in planning for business opportunities. External risk, on the other hand, is usually the type of risk that the organization has limited control over. Examples of external risk factors include the market space, government regulation, currency valuation, international and world events, natural disasters, and so on. While the organization can't control these factors, it must plan for them in its risk management strategy and develop plans to assess and deal with these factors. These factors are used to develop risk scenarios.



TIP Identifying and classifying risk are generic steps and really are intended for you to get situational awareness of what risks your organization may be exposed to. They should be considered precursor steps to developing risk scenarios.

Risk Scenarios

Risk scenarios are created by developing an idea of potential events that can affect an organization or its assets. The scenarios are based upon different risk factors that an organization experiences. These can be factors that are internal to the organization, such as personnel, training, technology, and so on; there could also be external factors such as market space, regulation, and the economy, for example. There are several different elements that make up a risk scenario, which we will discuss in this section.

Threat Agent

Threat agents, as you recall from Chapter 1, are the actors and initiate a threat event. Threat agents could be internal or external, their motivation could be intentional or accidental, and their focus or goals could be wide and varied. Threat agents are a necessary part of risk scenario development simply because there has to be some entity that initiates a threat. Remember that threats are merely negative events; there must be a catalyst for them to occur. Developing risk scenarios requires that the organization be aware that many different types of threat agents may potentially initiate negative events against them. The threat agents should be matched to potential threat events, as well as vulnerabilities that a threat might exploit.

Threat

Threats are negative events; they are initiated by threat agents and exploit vulnerabilities inherent to an asset, a process, people, technology, or an organization. Understanding all of the potential realistic and relevant threat events that could affect an organization is necessary to developing risk scenarios. The possible gamut of threat events that concern the organization is developed through threat assessment and modeling methods.

Asset

Risk scenarios target and directly affect assets. Remember that assets are not only tangible equipment or systems; they can also be a process, a proprietary manufacturing method, people, facilities, equipment, or anything else the organization places a value on. Assets can also be intangible items such as consumer confidence, customer loyalty, reputation, and so on. These intangible assets are more difficult to develop risk scenarios around, but they're no less important than the tangible ones. When developing risk scenarios, assets should be identified as concretely as possible; even intangible assets, such as reputation, might be defined in terms of dollar values derived from customer satisfaction surveys or statistical analysis of return customer business. Identifying assets and prioritizing them based on their importance to the organization is sometimes referred to as a *criticality analysis*. In any event, identifying assets, as well as prioritizing them in order of importance to the organization, is an essential step in the process of developing risk scenarios. Asset value is a critical concern in developing risk scenarios because it directly affects the impact the organization bears when the risk scenario successfully affects an asset.

Vulnerability

Vulnerabilities are weaknesses inherent to assets. Threats directly affect vulnerabilities, turning any "potential" for damage into real damage and impact if they are able to successfully exploit those vulnerabilities. Risk scenario development directly depends upon the organization thoroughly identifying all the potential vulnerabilities an asset may have. If all the different vulnerabilities are not identified, then the organization could have risk scenarios it is not even aware of. Recall that for risk to exist, there must be both a threat and a matching vulnerability for it to exploit. Without adequate knowledge of either, the risk scenario can't be developed.



EXAM TIP Keeping in mind the basic definitions of the four elements of threat agent, threat, asset, and vulnerability will help you understand how they contribute to risk scenarios in particular and risk in general. Threat agents initiate threats, which exploit vulnerabilities, which are inherent to assets. The two other factors that are considered with these four are likelihood and impact. Together, all of these elements make up risk.

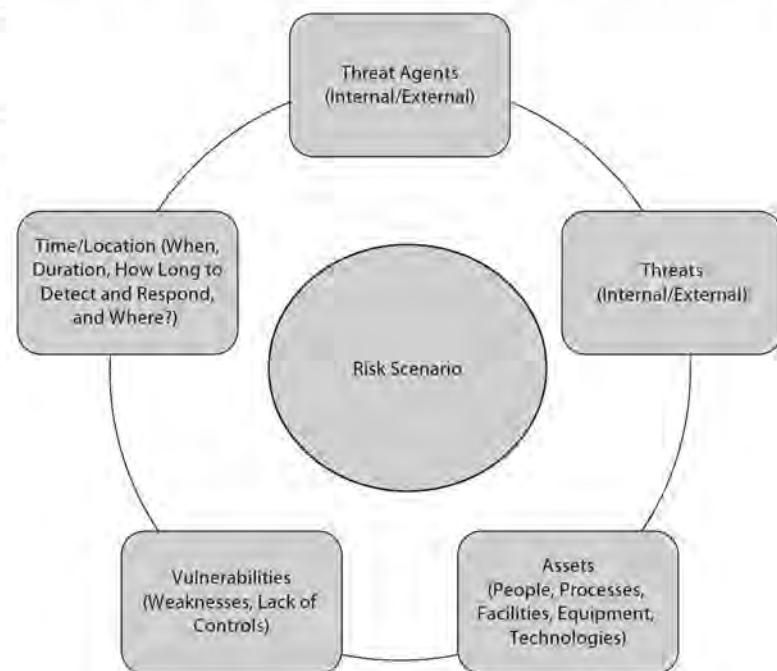
Time and Location

Time and location are characteristics of the risk scenario occurrence itself. You could have a threat agent, a threat, an asset, and a vulnerability, and these are different elements of risk when combined with impact and likelihood. However, until the risk scenario

actually occurs, all of this is only theoretical. The time and location defines the risk scenario event occurrence itself, turning it from risk into reality. These are variable factors that, until the risk scenario actually occurs, may be difficult to predict or measure with any accuracy, in terms of how they contribute to likelihood and impact of the scenario occurring. Time is not simply a characteristic defining when the event occurs, although the timing of a risk scenario is important. Time also describes the duration of the event and how long it takes the organization to detect, respond to, analyze, and contain an event. During its development of risk scenarios, the organization may find that some risk scenarios are more likely, or carry more impact, if they occur at different times, such as during peak or even off-hours, for example. Some risk scenarios may also have more of an effect on an organization if they occur during critical events, such as fiscal year reconciliation, for example, or during tax season. Time should be a factor considered when examining the likelihood and impact of a risk scenario.

Location is not only a geographical characteristic of the risk scenario event, although geography is certainly a consideration. Risk scenarios may certainly depend upon the geographic location of a business or its infrastructure, but location could also mean whether a risk scenario occurs internally to a business or in its external environment. For example, consider an attack that targets the external perimeter network. This may affect the organization's continuing communications with the outside business world. Contrast that to an attack on the internal network as a result of a malicious insider cutting fiber cables in a data center. The organization typically has little control over risk scenarios that occur outside of its physical or logical confines or span of control, but these risk scenarios should still be considered. Figure 3-1 shows the different elements that contribute to a risk scenario.

Figure 3-1
Elements of a risk scenario





NOTE The time and location elements of a risk scenario are really characteristics of the event itself; they actually describe details about the occurrence of risk scenarios. They should be used to help develop the scenarios to the extent that time and location factors could also affect the likelihood and impact of the scenario.

Example Risk Scenario

To frame these elements into something that may be easier to understand, consider the following as an example for a risk scenario:

A foreign intelligence agency uses a zero-day exploit to cause a buffer overflow in a critical U.S. Department of Defense Internet-facing web application, resulting in the ability to execute arbitrary commands on the system and exfiltrate data. The attack is not detected because of a lack of adequate intrusion detection security controls in place; therefore, the response and mitigation for the attack are delayed. Because of potential delay in detection and response, the foreign agency could carry on the attack at any time they want, for as long as they want, until the threat is detected and defended against.

Obviously, this scenario is generic and not very detailed at all. The risk scenarios generated during the course of an organization's efforts would likely be much more concrete and detailed and apply to specific assets. In the previous example of a risk scenario, you could break out each of these factors, following the illustration in Figure 3-1, as in Table 3-1.

Note that what's missing here, completing this as a consideration of risk, are the elements of impact and likelihood. Keep in mind that risk scenarios are possibilities of *what* could happen but without considering how likely they are or the impact they would cause. These two elements are added to the equation and considered during risk evaluation and analysis, which will be covered in Chapter 4.

Risk Scenario Component	Description
Threat agent	Foreign intelligence agency
Threat	Zero-day exploit
Asset	Critical system application
Vulnerability	Application vulnerability allowing a buffer overflow
Time/location	Time and duration of attacker's choosing; external systems only; indefinite delay in detection and response time

Table 3-1 Examples of Risk Scenario Components



EXAM TIP Risk scenarios are events that could occur, based on an understanding of threat agents, threats, assets, vulnerabilities, and time/location considerations. These are just possible events, without consideration of likelihood and impact.

Developing Risk Scenarios

To identify risk scenarios, the organization must first look at its business and mission and determine what types of risk could impact the achievement of the mission. The organization would then generate risk scenarios to account for all the possible negative events that could happen to the organization. The organization might also develop more detailed risk scenarios that could affect particular business objectives or units. To properly identify risk scenarios, the organization must collect and assimilate data on the business's operational environment, both internal and external, as well as the different potential risk events that can occur and the factors that contribute to them. Additionally, as we mentioned earlier, gaining information on the possible threat agents, threat vectors (methods that a threat actor uses to deliver a threat), assets, and vulnerabilities is also a necessary step in developing risk scenarios.

ISACA calls for a formal process for developing risk scenarios that takes one of two possible approaches. The first approach is driven from the top of the organization downward and starts with identifying the business's objectives and identifying risk scenarios that would have an impact on achieving them. The second approach, called a *bottom-up* approach, looks at developing any and all possible scenarios first and then culling those down through a comprehensive analysis. Both approaches have their merit, and both are qualitative (subjective) approaches at best. The advantage to the top-down approach is that the scenarios developed specifically target relevant business objectives. The disadvantage is that it is narrowly focused and may not consider all potential risk scenarios, especially remote or seemingly unrelated ones. The bottom-up approach, on the other hand, can consider all manner of scenarios, even ones that might not be developed through conventional thought. The disadvantage to this approach, however, is that the risk scenarios developed may be too numerous and may span all manner of likelihood, causing them to be unwieldy to manage and maintain. Additionally, it may take a lot of work to reduce the number of relevant, likely scenarios to a manageable level. We will briefly describe each approach in more detail next.

Top-Down Approach to Developing Risk Scenarios

The top-down approach to risk scenarios, as mentioned earlier, begins by looking at the different business objectives an organization has. These can be either general or specific objectives or goals and are dependent upon the business mission. In the top-down approach, business objectives are examined for potential risks that may negatively affect the success of achieving those objectives. For example, if a business objective is to deploy a robust web-based customer interface and online ordering system, the organization would look at risk scenarios that would affect this particular system. It might first develop an idea of the different threat agents and threats that could affect the system

and then look at the system itself (the asset) for vulnerabilities that match up to these threats. Considering potential event characteristics, such as times that the risk scenario might occur (peak ordering times, for example, or even during off-hours when there may not be an administrator available to address the problem), location (considering both internal database servers and external Internet-facing web application servers, as well as geographic locations where infrastructure assets may be dispersed), and potential risk factors that could both increase or decrease the risk, is also part of this approach. The result would be a more detailed list of specific risk scenarios that affect the different business objectives under scrutiny. The top-down approach is considered objective-centered and requires more participation from upper-level managers who may have more strategic information regarding business objectives and goals than lower-level employees. It is also more directive and structured in nature.

Bottom-Up Approach to Risk Scenarios

The bottom-up approach can begin with participation from lower-level employees, who should be experts in some area of risk management, or at least in the areas that the risk scenarios may apply to. While the bottom-up approach tries to look at any and all potential scenarios, there must be at least some beginning focus of what asset, process, or area of concern the risk scenarios might affect. Think of the bottom-up approach as more of a brainstorming approach than the top-down approach; it begins from a more general perspective with the goal of narrowing down risk scenarios as the process progresses. With the bottom-up approach, the participants are likely to be much more open to different risk scenarios that, while they may be more unlikely, should at least be considered. The bottom-up approach is more susceptible to “thinking out of the box” than the top-down approach and is more collaborative and unstructured in nature. As this approach is conducted, risk scenarios are examined more in-depth, considering how actually realistic they may be with regard to different threats, threat agents, assets, vulnerabilities, and event characteristics. Many of these risk scenarios will be discounted as highly unlikely, but some will be retained as possibilities that may not have been otherwise considered.

An example of the bottom-up approach could be where a team brainstorms all of the different hypothetical possibilities for risk scenarios that could occur to the business. Obviously, general, typically realistic scenarios would be mentioned by the group for consideration, such as natural disasters, hacking attacks, and so forth. As the process moves forward, however, and narrows down the realistic list of possible scenarios, earthquakes or hurricanes might be discounted because of geographic location, for example, and hacking attacks might be further narrowed down to insider attacks, discounting the role of external attacks on the business if the participants do not think this is a realistic scenario.

As we discussed earlier, there are advantages and disadvantages to both approaches; it's probable that the most effective approach is a combination of the two, where business objectives are introduced as the focus but brainstorming sessions are conducted to consider any possible scenario. These risk scenarios could be carefully considered and then refined or discarded as needed. Figure 3-2 shows the top-down and bottom-up approaches. Regardless of approach, information technology-related risk scenarios are further refined by adding in consideration of risk factors, such as internal and external factors, the ability of the organization to manage risk, and so on.

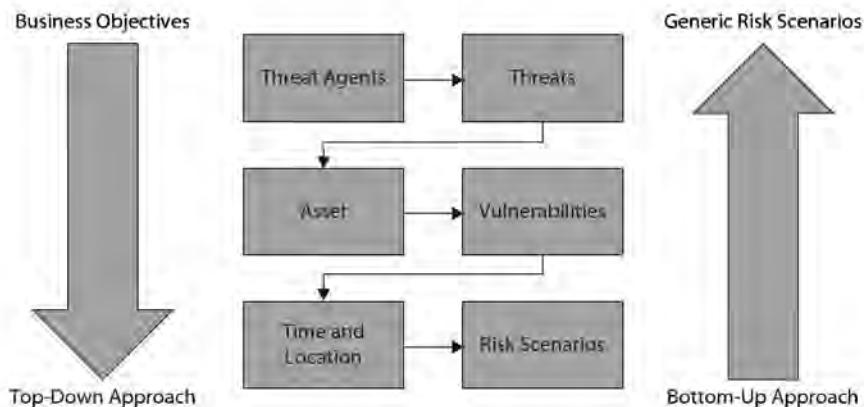


Figure 3-2 Top-down versus bottom-up approach



EXAM TIP The top-down approach develops risk scenarios from a business objective perspective, whereas the bottom-up approach is more general and is designed to look at all possible scenarios, regardless of business objective.

External Risk Factors

We discussed factors in Chapter 2 that could be considered external to the organization's environment. These were factors such as governance, government regulation, the economy, market trends, and so on. These same factors that affect the business processes and infrastructure components discussed in Chapter 2 can also be identified and used to create risk scenarios. They can help shape risk scenario development because scenarios may be more or less realistic or likely because of the way these external factors affect the organization and risk. For example, government regulations may affect the mandatory protections certain classes of data must receive. If the organization is in compliance with these regulations, then a given scenario describing a data breach or loss may become less likely.

Internal Risk Factors

Internal risk factors can affect risk scenarios because they may also, like external factors, influence the conditions in which the risk scenario is likely to occur. These factors can reduce or increase the likelihood of the scenario or even reduce the impact to assets in the organization if the risk scenario occurs. Internal factors include the organizational structure, risk appetite and tolerance, compliance with governance, resource commitment and constraints, organizational priorities, competing organizational objectives, and even internal politics. As we also mentioned in Chapter 2, the organization exerts more control over internal factors than it does external ones, so more of an investment of attention, time, and resources should be paid to these factors in order to reduce the likelihood and impact of risk scenarios.



TIP The same internal and external factors are the ones that affect risk from several different viewpoints. Not only do they affect risk scenarios, but they also affect different business processes and activities within an organization, as discussed in Chapter 2.

Organizational Risk Management Factors

The ability of an organization to effectively manage its risk is also a factor affecting risk scenario development. The maturity of an organization's risk management strategy, methods, and techniques directly affects the effort that the organization will put into developing risk scenarios and attempting to reduce their likelihood and impact. Organizations with ad hoc or informal risk management processes will be less likely to develop realistic, relevant scenarios and deal with them. Organizations that have structured, proven processes in place already will likely employ the expertise and proactive steps necessary to develop solid risk scenarios.

IT Infrastructure Factors

We've already discussed internal and external factors, as well as risk management processes, and the effect these factors have on developing and dealing with risk scenarios. IT infrastructure is both an internal and external risk factor since there are internal pieces of the IT infrastructure that support the processes of the organization, as well as external pieces that support its interaction with the outside world. Often the lines between internal and external IT infrastructure are blurred since there may be a seamless connection between internal and external networks and the technologies that support all the different business processes. Additionally, outsourcing to third parties makes the infrastructure straddle both internal and external environments since some of the infrastructure may be off-site and located in a different geographical location behind some other businesses firewall yet process sensitive internal data.

IT infrastructure affects the development of risk scenarios the same way other factors do; the way the infrastructure is designed and implemented can increase or decrease the likelihood or impact of the risk scenario and make the scenario more likely or not. Outdated or overtaxed infrastructure introduces risk into the organization and exposes the organization to many more risk scenarios than a more modern, robust infrastructure. Because infrastructure can exist in both the internal and external environments simultaneously, this increases the risk and the number of possible scenarios it may encounter. The IT infrastructure must be carefully considered when developing risk scenarios.

Business Process Factors

An organization's business processes could also be considered to be either internal or external, or both, in nature. More often than not, business processes are themselves considered assets and are directly affected by risk scenarios. However, in addition to being the target of a risk scenario, these processes affect risk scenario development as factors in themselves because their interaction with the environment could increase or decrease the likelihood and impact of a risk scenario on other business processes or assets. Business processes are, by their nature, complex interactions of tasks and activities performed by

people and processed by the infrastructure and may result in products or data. Any of these different elements can affect or be affected by risk scenarios. And whenever any of these individual elements are affected by a risk scenario, ripple effects often are carried to other processes or assets. Business processes could be seen also as a combination of all the different factors and elements we have discussed so far, so their inclusion in the development of risk scenarios might be at different complexity levels.



CAUTION Many of the factors we have discussed in this section could be considered either internal or external, or both. Frequently, it's hard to distinguish whether a factor is primarily internal or external. Most of the time, all these factors, in some way or another, could be considered either, depending upon the specific context under discussion at the moment.

Risk Scenario Stakeholders

Each risk scenario you develop will have various stakeholders that are affected by the scenario to varying degrees. Typically, stakeholders would include those who directly manage or are responsible for the asset or process in question or who manage the affected organizational level. They could also be the people responsible for managing risk associated with their asset or area, so they could be considered the risk owners as well. Additionally, stakeholders will likely include those people who are in management or executive positions responsible for managing risk throughout the entire organization. For risk scenarios, you should develop a list of potential stakeholders and include them in your discussions concerning risk to their areas that might be affected. They should receive all relevant products you produce regarding the risk that could potentially affect them, including assessments, briefings, and reports. You should consider including these stakeholders both before and after developing risk scenarios since they can contribute to developing a more detailed scenario, based on their knowledge of factors relevant to the asset or area in question.



EXAM TIP Risk scenario stakeholders include anyone who is affected by the scenario itself. These could be asset owners or managers, risk managers, or anyone responsible for responding to risk in any way. Stakeholders could also include people who manage processes that affect risk. Additionally, all the stakeholders should be included in the scenario development process.

Exercise 3-1: Develop a Risk Scenario

Select an asset, process, or organizational structure within your organization. Develop a risk scenario around your selection, accounting for threat agent, threat, vulnerability, and possible event characteristics, such as possible time, location, and other circumstances. Feel free to make up notional data if you choose or use realistic information if you have it available. Who are the stakeholders affected by this risk scenario? What approach did you use to develop the scenario, top-down or bottom-up? Is this a realistic scenario that could occur in your organization?

Analyzing Risk Scenarios

Now that we've discussed the different factors and processes involved with developing risk scenarios, we're going to take a look at analyzing these risk scenarios. Analyzing them will help you frame them better for when you're looking at their impact and likelihood, which is the subject of Chapter 4. For this portion of the chapter, we are not going to calculate the likelihood and impact, but we will discuss some of the factors that may affect the calculation. Some of these factors include organizational factors, such as structure, policies, and standards but may also include infrastructure factors, such as technology, architecture, and security controls. These different factors weigh in on how likely a risk scenario is to take place, as well as what its potential impact will be to the asset or organization.

Likelihood and Impact

Related to but separate from the different factors that may affect how risk scenarios are developed are factors that influence how much harm the organization suffers if a risk scenario is realized, as well as whether these scenarios are realistic in terms of likelihood. Remember from Chapter 1 that likelihood is the realistic level of certainty that an event will occur, that is, how likely a threat is to exploit a particular vulnerability. Note that we intentionally avoid using the word *probability*; while the terms *likelihood* and *probability* are similar, determining the probability of an event implies the use of statistical analysis, definitive quantifiable data, and mathematics. This is definitely one way to determine how likely an event is, but likelihood can also be determined by using subjective (or qualitative) means, which we'll discuss in Chapter 4. Also recall that impact could be considered the degree of harm to an asset or the organization. Sometimes impact is measured in terms of cost, such as dollars to replace an asset or how much money the organization loses if the asset is damaged or lost. Impact may not necessarily be a single instance of loss; for example, losing a major system that processes financial data would not be confined to just how much the data or the system costs to recover or replace. It could also be a major impact that increases every single day that the system is out of commission since the organization would be losing revenue for every day that it does not have the system's capabilities.



NOTE Here we have discussed only generalities regarding likelihood and impact. We'll discuss how to actually evaluate risk, considering likelihood and impact in the calculations, in Chapter 4.

Organizational Factors Affecting Likelihood and Impact

Organizational factors can affect likelihood and impact because they may increase the likelihood of a risk scenario or increase the impact to the organization if the scenario were to occur. Likewise, they can reduce both likelihood and impact the scenario as well. Organizational structure can influence the likelihood and impact because the way the business is organized and structured affects different factors, such as chain of command, span of control, budget and resource allocation, and business priority. Additionally, organizational structures affect processes since the organization may be organized on

a functional basis. These different factors in turn affect likelihood and impact since they may drive the way the organization prepares for and responds to risk scenarios.

Organizational governance such as policy, standards, and procedures affect likelihood and impact since they drive the organizational direction in terms of compliance. These elements of governance may help or hinder the business's risk strategy, depending upon the importance that organizational leadership places on risk management within the organization. For example, a policy could strongly support risk management methods and techniques or give little emphasis to them at all. The supporting standards and procedures would fall in line with the policy's stance on risk management. If these elements do not support a strong risk management program, then the organization will have a higher likelihood that the different risk scenarios will occur, and their impact will be more serious.

Another organizational factor that may affect likelihood and impact of risk scenarios is an organization's tolerance and appetite for risk. We discussed these in Chapter 1, and you'll remember that the organization's appetite for risk describes how much risk it is willing to accept in pursuit of a particular business endeavor. Its tolerance for risk describes the variation it's willing to accept from its appetite. Both these factors affect likelihood and impact because as the appetite and tolerance for risk increase, the organization may engage in riskier business pursuits, which may increase risk scenarios, as well as their likelihood and impact. Organizations that have a low tolerance and appetite for risk tend to "play it safe," reducing the number and level of risk scenarios that may affect them and reducing likelihood and impact. Organizations that tend to have a lower risk tolerance and appetite may also increase their level of commitment to controls that would reduce risk.

Technological Factors Affecting Likelihood and Impact

Technological factors can affect likelihood and impact as well but possibly not as concretely as you might think. Certainly, technological factors, such as infrastructure, technical security controls, network architecture and design, and so on, are "hard" controls that are more easily justified, installed, and measured, and they typically produce tangible results. But the same technological factors can also be "soft" in nature because of the unpredictability of different elements, such as both the external and internal business environments. Organizations that rapidly change business strategy or markets or develop new products or processes are typically at the mercy of established infrastructures that are more slow-moving or even static in nature. Organizations typically don't revamp their entire network infrastructure every time they develop a new business process or take a new product to market. It would be economically unfeasible, of course, for constant, short-term changes of that nature. In some cases, then, the static nature of installed technology may actually increase the likelihood and impact of risk scenarios. New and emerging threats that are identified every day also cause an organization's technologies (and the personnel that manage them) to be in reactive mode. They are often forced to simply keep up since they are not likely going to buy a new firewall every single time a new threat comes out or quickly implement a new encryption methodology when their existing one is discovered to have vulnerabilities. Technology, just like other factors, can have both positive and negative effects on likelihood and impact.



CAUTION Both organizational and technological factors can influence risk scenarios, as well as their likelihood and impact, in different ways. These ways are not only always positive or always negative; most of the time these factors could influence risk scenarios both negatively and positively, resulting in increases or decreases in likelihood and impact.

Risk Register

A risk register is a product or document that reflects the different risk scenarios and factors for a given context. It could be for a single system, for a component of the system, or even for a higher-level organizational element. It also may address only a small portion of the specific piece of risk. Normally the risk register has several components, which we'll discuss in the next few paragraphs. The risk register is used to record and manage risk and serves as a reference point for tracking risk through its life cycle.

If you've ever been exposed to Plan of Actions and Milestones documents found in the Department of Defense and in NIST's Risk Management Framework, then you've looked at one type of risk register. While there are different components that a risk register should have, different organizations may have different entries or elements on their own risk registers. We'll take a look at some of the more common elements of a risk register in this section.

Elements of a Risk Register

As mentioned earlier, a risk register can contain different types of data elements depending upon what the organization wants to include on it. Most commonly, however, risk registers record a variety of information, including various risk factors and risk scenarios. There might also be data included that describes different technical or management findings contributing to the risk. Additionally, threats, vulnerabilities, assets, likelihood, and impact data may be included on the risk register. All in all, the risk register could include the following:

- Risk factors
- Threat agents, threats, and vulnerabilities
- Risk scenarios
- Criticality, severity, or priority of risk
- Asset information
- Impact of the risk on an asset
- Likelihood of the threat exploiting the vulnerability
- Current status of risk response actions
- Resources that may be committed to respond to risk
- Risk ownership information
- Planned milestones toward risk response

Risk Description	Likelihood	Impact	Risk Owner	Resources Required (Hours, Dollars, etc.)	Estimated Completion Date	Actual Completion Date	Current Status	Comments
Data theft from malicious user (via risk assessment on 04/2015)	Medium	High	Engineering Department	\$10K for new DLP system	Jan 2016		Assessing different DLP vendors	Purchase and implementation by Dec 2015
Loss of primary accounting server data	High	High	Accounting department	15K for backup system	Oct 2015	Sep 2015	Vendor selected	Final purchase and installation in August 2015

Figure 3-3 Basic risk register entries

Any or all of these data elements could be included on the risk register. Additionally, the risk register could span more than one document as part of a multidocument package describing the overall risk toward the organizational asset. Essentially, the data points that are included on the register need to be those that support the organization's risk management strategy and plan and help it to adequately identify, manage, monitor, and mitigate risk throughout its life cycle. Figure 3-3 illustrates how a basic risk register might look.



NOTE These are only notional entries for a risk register but are the most commonly used. Organizations should include the data most relevant to their management needs.

Creating and Maintaining a Risk Register

How the risk register is created and maintained, and what data elements are included with it, is usually determined as part of the organization's risk management strategy and plan. The organization should decide upon a defined format and carefully consider all of the different data it wants to include. Obviously, it will need to include the data elements that help to manage risk throughout its life cycle.

Designated risk owners will usually be held responsible for creating and maintaining the risk register document, but there also may be other external agencies or entities that help with or even audit this process. The first step in creating a risk register is to determine all the different risk factors that affect a given asset or organizational element. From there, risk scenarios, as described earlier, are developed within the context of the specified asset or process and are mapped to those assets on the register document. Threats, vulnerabilities, likelihood, and impact are all considered, and risk is quantified or qualified, according to the assessment methodology used, and recorded in the risk register. Risk response, discussed in Chapter 5, is also considered and included on the register. Risk registers are discussed in-depth in ISACA's "The Risk IT Framework" and "The Risk IT Practitioner's Guide" publications.

Chapter Review

In this chapter, we discussed several aspects of managing risks, particularly those that take place before risk evaluation, assessment, and response. We looked at developing risk scenarios in-depth and the different factors and components that make up risk scenarios. A risk scenario is a potential event that could affect the organization. It consists of a threat agent, a threat, an asset, and a vulnerability. Risk scenarios are part of the overall risk consideration, less the likelihood and impact calculations.

Finally, we discussed the purpose and elements of the risk register and how different information and data points are recorded on the register. Some of these different data points include risk scenario information, such as threat agents, threats, assets, and vulnerabilities, as well as criticality, likelihood, and impact information. The risk register may also include information on risk owners and other responsible parties that must manage risk. Finally, it also may include resources that are dedicated to risk management and mitigation. The risk register is a living document that allows the organization to manage risk throughout its life cycle for given scenarios and assets.

Review Questions

1. Which term describes a potential risk event that can affect an organization?
 - A. Risk factor
 - B. Risk scenario
 - C. Risk consideration
 - D. Risk agent
2. Which of the following could initiate a risk scenario?
 - A. Threat agent
 - B. Threat
 - C. Asset
 - D. Vulnerability
3. Risk scenarios are all the elements of risk, except for _____ and _____.
(Choose two.)
 - A. Threat
 - B. Likelihood
 - C. Impact
 - D. Vulnerability

4. _____ are elements that influence the development of risk scenarios, as well as their likelihood and impact.
- A. Risk agents
 - B. Risk indicators
 - C. Risk factors
 - D. Threat agents
5. All of the following are considered external risk factors affecting development of risk scenarios, except which one?
- A. Market
 - B. Economy
 - C. Legal governance
 - D. Organizational structure
6. You are developing risk scenarios and are considering how different circumstances involving timing of the scenarios might affect their likelihood and impact. Which of the following would most likely increase the likelihood and impact of different risk scenarios?
- A. A hacking attack that occurs during an out-of-state IT conference that most of the organization's information security personnel would be attending
 - B. The loss of a production server while the company is hosting a local business conference
 - C. Unscheduled maintenance downtime during the rollout of a new version of the company's graphics software
 - D. Corruption of the company president's workstation hard drive data during her absence because of a business trip
7. Which of the following approaches to risk scenario development begins with business objectives and attempts to identify risk scenarios that could affect those objectives?
- A. Bottom-up approach
 - B. Top-down approach
 - C. Cross-functional approach
 - D. Quantitative approach
8. Which of the following approaches to risk scenario development "brainstorms" all the possible risk scenarios that could occur in the organization?
- A. Quantitative approach
 - B. Top-down approach
 - C. Bottom-up approach
 - D. Threat modeling approach

9. All of the following are organizational factors influencing risk scenarios, except which one?
- A. Policies
 - B. Structure
 - C. Resource allocation
 - D. Market trends
10. Which of the following are concerns with the IT infrastructure in terms of how it affects risk scenarios? (Choose all that apply.)
- A. Level of modernization
 - B. Level of performance
 - C. Internal and external interfaces and connections
 - D. Cost
11. Which of the following are two elements that are critical in risk scenario development? (Choose two.)
- A. Asset identification and valuation
 - B. Likelihood calculation
 - C. Impact calculation
 - D. Threat assessment
12. Which of the following would be considered primary stakeholders with regard to risk scenario development?
- A. Production control managers
 - B. Accounting executives
 - C. Vendors
 - D. Asset managers
13. Which of the following are factors of organizational structures that could have an effect on likelihood and impact of a risk scenario? (Choose two.)
- A. Technology upgrades
 - B. Budget or resource allocation
 - C. Strategic product development
 - D. Organizational chain of command
14. Compliance is a factor that influences risk scenarios as a direct result of organizational _____.
- A. Threats
 - B. Risk management strategy
 - C. Governance
 - D. Vulnerabilities

15. Which of the following levels of risk appetite and tolerance could contribute to an increased number of risk scenarios, as well as higher likelihood and impacts? (Choose two.)
- A. Higher risk appetite level
 - B. Lower risk appetite level
 - C. Higher risk tolerance level
 - D. Lower risk tolerance level
16. Which of the following describes a management product that is used to track risk scenarios?
- A. Risk report
 - B. Vulnerability assessment
 - C. Threat assessment
 - D. Risk register
17. Which of the following determines how a risk register is created and maintained?
- A. Risk assessment
 - B. Risk management strategy and plan
 - C. Risk scenario
 - D. Risk methodology
18. Who is responsible for creating and maintaining the risk register document?
- A. Board of directors
 - B. Risk owner
 - C. Senior executive
 - D. Risk assessor
19. Which of the following do risk scenarios typically map to on the risk register?
- A. Risk areas
 - B. Threats
 - C. Assets
 - D. Vulnerabilities
20. Which of the following data elements should be recorded on the risk register? (Choose all that apply.)
- A. Risk factors and scenarios
 - B. Information concerning assets
 - C. Impact and likelihood
 - D. Risk management strategy

Answers

1. **B.** A risk scenario describes a potential risk event that can affect an organization.
2. **A.** A threat agent could initiate a risk scenario.
3. **B, C.** Risk scenarios include all the different elements that make up risk, except for likelihood and impact.
4. **C.** Risk factors are elements that influence the development of risk scenarios, as well as their likelihood and impact.
5. **D.** The organization's structure would be considered an internal risk factor affecting the development of risk scenarios.
6. **A.** A hacking attack that occurs while most of the company's IT security personnel are away would have a serious impact on the entire organization, and could even be more likely, if the attack were planned during this time.
7. **B.** A top-down approach starts with business objectives and attempts to identify risk scenarios that could affect particular business objectives.
8. **C.** The bottom-up approach involves brainstorming all the different potential risk scenarios that could affect an organization.
9. **D.** Market trends are not organizational factors.
10. **A, B, C.** All of these are concerns with how the IT infrastructure would influence risk scenarios, except for cost. Cost would be a concern about how the IT infrastructure is used to respond to risk but not necessarily its influence over the likelihood or impact of a risk scenario.
11. **A, D.** To develop risk scenarios, you need to know details about assets, such as criticality and their value, vulnerabilities, threat agents, and threats. Likelihood and impact are not necessary to create risk scenarios, but they are necessary to evaluate and assess risk.
12. **D.** An asset manager would be considered a primary stakeholder since that person is directly responsible for the risk an asset incurs.
13. **B, D.** Both chain of command and resource allocation are factors of organizational structure that could affect risk scenario likelihood and impact.
14. **C.** Compliance is a factor that influences risk scenarios as a direct result of organizational governance.
15. **A, C.** Organizations that have a higher level of appetite and tolerance for risk typically incur more risk scenarios, which could have a higher likelihood of occurring and a greater impact.
16. **D.** A risk register is a management product that allows the organization to track risk.
17. **B.** The organization's risk management strategy and plan determines how a risk register is created and maintained.

18. **B.** The risk owner is responsible for creating and maintaining the risk register document.
19. **C.** Risk scenarios typically map to assets on the risk register.
20. **A, B, C.** All of these pieces of data should be included on a risk register. The organization's risk management strategy, however, is a higher-level document that is not part of a risk register.

This page intentionally left blank

Risk Assessment and Analysis

In this chapter, you will:

- Review the processes of risk identification, evaluation, and assessment
- Learn about qualitative and quantitative risk assessment techniques
- Understand how to evaluate existing controls for effectiveness
- Assess gaps between current and target states of risk in the IT environment
- Consider risk ownership and accountability during risk analysis
- Be able to report risk results to appropriate levels of management

This chapter covers Domain 2 of the Certified in Risk and Information Systems Control (CRISC) exam objectives and knowledge statements and focuses on the risk evaluation, assessment, and analysis processes. We will cover the overall process for evaluating likelihood and impact for risk, examining both qualitative and quantitative assessment methods. We will also cover how control effectiveness is examined and how you might identify gaps between how effective controls are in the existing risk state and the desired level of effectiveness at which controls need to be functioning. Finally, we'll discuss how the results of the risk analysis are communicated to upper management and risk owners and reported on the risk register.

The CRISC exam objectives covered during this chapter include the following task statements:

- 2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
- 2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment
- 2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability
- 2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making
- 2.6 Update the risk register with the results of the risk assessment

As indicated in previous chapters, these objectives and knowledge statements are shown in order of how they are listed in the CRISC Job Practice areas, not necessarily how they are presented in the chapter.

Risk Assessment Processes

As we've mentioned, many of the terms you'll encounter on the exam are generic and may have different definitions based upon the different frameworks or standards you are using in practice. The term *assessment* is one such term that may confuse you. For the purposes of taking the exam, and in this book, an assessment refers to the overall combination of steps of identifying, evaluating, and analyzing risk. Remember that risk identification involves identifying the threats, vulnerabilities, assets, and existing controls. Evaluation, on the other hand, focuses on determining the likelihood and impact if the vulnerabilities are exploited by the threats, resulting in damage to the asset. Risk analysis puts everything together and informs the organization about the realistic risk involved and helps determine how effective existing controls are and what gaps exist between current and desired states of risk.

Risk assessment processes sometimes include the risk identification piece of the process but are often separate from this part, depending upon the framework or standard you are using. In general, this process includes threat source and event identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and results documentation; these steps follow the same pattern and path as we're describing here for you in terms of identifying risk and then evaluating it. We'll describe some of these generic processes here in this chapter.



NOTE Different risk assessment methodologies and frameworks use varying terms that may have the same or different definitions. You should always look at a term in view of its context and particular framework or methodology.

Some organizations see risk assessment as one large monolithic process, but many frameworks and standards break it down into different steps. We'll take another look at several important frameworks we briefly touched on in Chapter 1, including the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), the ISACA Risk IT Framework, and others. In this chapter, however, we will go into more detail and examine them from a risk assessment perspective.

NIST RMF

The NIST RMF, found in Special Publication 800-37, describes an overall risk management process that covers all aspects of the risk life cycle. For the assessment piece of the RMF, NIST uses a four-step risk assessment process found in Special Publication 800-30, "Guide for Conducting Risk Assessments." You'll see that these four steps are broken down into nine distinctive processes and are listed here:

Step 1: Prepare for assessment.

Step 2: Conduct assessment.

- a. Identify threat sources and events.
- b. Identify vulnerabilities and predisposing conditions.
- c. Determine likelihood of occurrence.
- d. Determine magnitude of impact.
- e. Determine risk.

Step 3: Communicate results.

Step 4: Maintain assessment.

While we won't go through every step of this process like NIST does, the process is similar to what we've been describing all along in this book, and it is similar to the other frameworks we discuss in the next section. The NIST assessment process is a subset of the integrated RMF, which includes not only assessments but categorizing assets according to criticality and protection (a necessary first step in the process), as well as managing and monitoring risk throughout the entire life cycle of a system or asset. The NIST RMF also includes a control framework and methods for assessing the various controls, which we will cover in upcoming chapters. Appendix A of this book covers the overall RMF and its supporting publications in detail.

OCTAVE Methodology

As part of a U.S. government contract with Carnegie Mellon University, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology was developed to assist organizations in identifying and assessing information security risk. The methodology was originally developed by the Software Engineering Institute (SEI) at Carnegie Mellon University in 1999 and has been updated over the years to its current version, OCTAVE Allegro, in 2007. OCTAVE uses a concept called *workshops*, made up of members of an organization, sometimes including outside facilitators with risk management and assessment expertise. The methodology has prescribed procedures, which include worksheets and information catalogs to assist organizational members, drawn from all functional areas of an organization, to frame and assess risk based upon internal organizational context (infrastructure, governance, business environment, and so on). OCTAVE has three iterations: the original OCTAVE, OCTAVE-S, and OCTAVE Allegro.

OCTAVE and OCTAVE-S

The original OCTAVE methodology was released in 1999 and was designed for organizations with at least 300 employees. The assumptions for using OCTAVE included that the organization operate and maintain its own multitiered information infrastructure and be able to perform vulnerability assessments. While OCTAVE is flexible and allows an organization to tailor its use based upon its own assessment needs, the methodology is performed as three sequential phases. The first phase covers identifying assets, threats,

protection practices, vulnerabilities, and security requirements. You can see where this maps to the practices we've described throughout this chapter as determining threats, identifying assets and their vulnerabilities, and evaluating existing controls. In the second phase, the members of the workshop perform assessment activities and evaluate the infrastructure. In the third phase, the workshop members develop response strategies for the identified risks.

OCTAVE-S is fundamentally the same as the original OCTAVE, with a few minor differences. First, OCTAVE-S was designed to assess smaller organizations, usually with fewer than 100 people. Second, this iteration relies more on internal personnel with extensive knowledge of the organization and its infrastructure and less on outside risk experts or facilitators. The number of workshop members will also be considerably less; the team may rely on fewer than ten key experts in the organization. OCTAVE-S processes and procedure documents were also written to include more detailed security-related information since this approach does not rely on outside security experts or risk facilitators to assist the team.

OCTAVE Allegro

The OCTAVE Allegro methodology, introduced in 2007, expands the previous two iterations but does not necessarily replace them. It includes a more business-centered and operational risk approach to the assessment. It is also asset-centered in its approach; it focuses on assets and their use or misuse, the environment they are used in, and how threats and vulnerabilities specifically target and affect the assets. Allegro can be used on a scaled basis; either individuals or workshop teams can use this method without the need for a high degree of risk management or assessment knowledge and experience. OCTAVE Allegro is divided into four phases, which include eight steps. These phases and steps are described next.

Phase 1: Establish Drivers

Step 1: Establish risk measurement criteria. This step serves to develop and establish the organization's methodology and measurement criteria used to assess risk. OCTAVE uses a qualitative assessment methodology and measurements but can use quantitative methods for certain aspects of the overall process, such as determining likelihood and impact.

Phase 2: Profile Assets

Step 2: Develop an information asset profile. In this step, the organization develops an asset profile, which is really a collection of information that describes the asset, including its characteristics, priority, impact to the organization, and value. This profile also contains security requirements the asset may have.

Step 3: Identify information asset containers. The information asset container describes how data is stored, where it is processed, and how it is transported. Containers are usually networks and systems, including those that the organization directly operates, as well as those that it outsources.

Phase 3: Identify Threats

Step 4: Identify areas of concern. In this step, potential risk factors are identified and are used to develop threat scenarios.

Step 5: Identify threat scenarios. Threat scenarios, in the context of OCTAVE, describe categories of actors and the relevant threats in each category. The scenarios are typically identified by the use of a threat tree, which simply maps actors and scenarios.

Phase 4: Identify and Mitigate Risks

Step 6: Identify risks. In this step, consequences such as impact and likelihood are identified and measured, which inform risk.

Step 7: Analyze risks. Once impact and likelihood have been identified and measured, risks are analyzed. During this step, risk scores are developed. These come from developing impact and likelihood values, with an emphasis on impact in particular, since this is an asset-driven assessment.

Step 8: Select mitigation approach. In this step, risk response strategies are developed, analyzed, and recommended.



EXAM TIP OCTAVE is designed for larger organizations, while OCTAVE-S is intended for use by smaller organizations. OCTAVE Allegro is scalable for use by individuals or larger teams working in organizations of various sizes.

ISO/IEC Standards

ISO stands for the International Organization for Standardization, and IEC stands for the International Electrotechnical Commission. Together, these two organizations are responsible for a plethora of information technology standards that are used worldwide, including several that apply to information security and risk management. We briefly mentioned risk-related ISO/IEC standards in Chapter 1; in this chapter, we will go into a bit more depth on these standards, focusing mainly on those that cover risk management and assessment.

ISO/IEC 27005:2011

Standards in the ISO/IEC 27000 series are all about information security, and the 27005:2011 standard supports the common ideas promulgated in both ISO/IEC 27001 and 27002. The standard applies to risk management, providing a unified risk management approach to organizational security. The standard doesn't necessarily offer a specific risk management or assessment methodology, but it does serve to describe a formalized, structured process of risk management, such as developing context, scope, methods, and so on. It also describes the two primary types of assessment methodologies, qualitative and quantitative. Additionally, it describes processes used to develop risk response strategies, communication with stakeholders, and continuous risk monitoring.

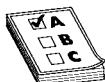
ISO 31000:2009

ISO/IEC 31000:2009, "Risk Management—Principles and Guidelines," covers a broader range of risk management and is not specific to IT or IT security. It generally focuses on business risk and can be used by organizations of any size, regardless of which business area or sector the organization occupies. It is useful for assisting organizations

in developing sound risk management frameworks, processes, and strategies. It replaced a previous comprehensive standard on risk management, the AS/NZS 4360:2004 standard. ISO/IEC 31000:2009 is the governing document for other risk-related documents in the 31000 series, such as the assessment document we'll cover next.

IEC 31010:2009

IEC 31010:2009 is where the meat of information regarding risk assessments is located for the ISO/IEC standards. This document, "Risk Management—Risk Assessment Techniques," articulates with and extends the risk management principles of ISO/IEC 31000:2009 and provides a concrete overview of the risk assessment process. This standard describes risk assessment as the combination of risk identification, analysis, and evaluation, with a precursor step of establishing the risk context within the organization. The standard also addresses communication and consultation with various stakeholders and management, risk treatment (response), and monitoring risk.



EXAM TIP Of the ISO/IEC standards, IEC 31010:2009 is an important one to know for the exam because it covers risk assessments in detail.

ISACA's Risk IT Framework

ISACA (formerly known as the Information Systems Audit and Control Association, but now known only by its acronym) developed the Risk IT Framework to align with its COBIT framework. While COBIT is used to manage other aspects of business infrastructure and risk, the Risk IT Framework specifically is used to allow organizations to identify and manage IT risk. The framework is broken down into three major process areas: Risk Governance (RG), Risk Evaluation (RE), and Risk Response (RR). We discussed this framework briefly in Chapter 1, but the focus of this chapter is on the assessment process, so we will cover the Risk Evaluation portion in more depth here.

The Risk Evaluation processes in the ISACA framework don't cover only assessment; they actually overlap with the risk identification areas. In RE processes, business impact is framed and described, and risk scenarios are also developed. Risks are assessed and analyzed, as well as presented to the organization's management. The RE processes are further broken down into three areas (numbered RE1–RE3), which we will describe in more detail.

Collect Data (RE1)

The data collection process aligns with some of the risk identification processes we've previously described. During this process, risk management personnel develop a model for data collection, which provides for standardized data formats, measurements, and common data definitions. Data is collected on the various aspects of the organization and risk scenarios, including the business's operating environment, risk factors, threat sources and events, vulnerability data, and asset data. Data is also collected on the effectiveness of existing controls in the organization.

Analyze Risk (RE2)

In this part of the Risk IT Framework, the organization begins to look at assessing and analyzing risk. First, it defines the risk analysis scope. The scope determines how broad and deep the risk analysis efforts will be, what areas the risk analysis will cover, and which assets will be examined for risk. To complete this part of the process, you'll need to consider all the documentation assembled up to this point: risk scenarios, asset inventories, breakdowns of business processes, prioritization of assets, and so on. This will help frame the risk analysis as well as determine scope.

During this step, IT risk is also estimated. This involves determining likelihood and impact values associated with the developed risk scenarios. You will also take into account existing controls and how effective they are as they are currently installed and functioning. Likelihood and impact values are taken into account after existing controls are considered.

Although risk response is the subject of the next domain and chapter in this book, during this step of the ISACA process, you also identify and consider possible risk response options. The person assessing the risk may recommend several different response options, based upon the identified risk. What risk options an organization will actually make use of is determined later in the process and typically with the input and approval of senior management. Risk response options should be recommended that reduce risk to an acceptable level directly based upon the risk appetite and tolerance of the organization. Finally, risk analyses should be reviewed by knowledgeable peers to verify that the analysis process is sound and to validate the results.

Maintain Risk Profile (RE3)

A *risk profile* is a collection of detailed data on identified IT risks. Risk profiles can certainly cover a single system or asset but are also often seen as describing risks on an organizational-wide basis. During this step of risk evaluation, a comprehensive document of identified risks and their characteristics, such as details regarding impact, likelihood, and contributing factors, is developed and maintained throughout the asset or system's life cycle. Keep in mind that system or asset risk profiles are usually rolled up into a more comprehensive risk document that covers systems, assets, and business processes across the entire organization.

IT assets are also mapped to the business and organizational processes they support during this step; this helps translate IT risk to corresponding business risk and allows management to see how the organization would be affected if IT risk were realized on specific assets. This also allows the organization to develop criticality estimates of IT resources from a business perspective. It's worth noting that this is similar to the same process followed during a business impact assessment (BIA). The key to understanding how IT risk affects business operations at this point, is in understanding how the capabilities of IT are provided to the business processes in question and how critical IT is to a particular business process or operation. Maintaining a risk profile also means monitoring risk and updating risk scenarios and risk analysis as conditions and risk factors change. This involves keeping the risk register up to date as well. Finally, the organization should develop key risk indicators (KRIs) during this step, specifically focusing on IT resources.

Methodology	Sponsor	Notes
NIST SP 800-30, "Guide for Conducting Risk Assessments"	National Institute of Standards and Technology	Part of the NIST Risk Management Framework
OCTAVE (OCTAVE, OCTAVE-S, and OCTAVE Allegro)	Software Engineering Institute, Carnegie Mellon University	Uses workgroups; suited for any organization; does not require extensive risk management experience or knowledge
ISO/IEC	ISO/IEC	Prescribes methods and processes for developing assessment programs; describes more than 30 different means to assess risk factors and elements
The ISACA Risk IT Framework	ISACA	Risk assessments covered in the Risk Evaluation (RE) phase

Table 4-1 Summary of Available Risk Assessment Methods and Frameworks

While key risk indicators are discussed in upcoming chapters, for now you should know that they allow the organization to monitor changes in risk for given scenarios, enabling the organization to modify its risk profiles as these indicators change. Table 4-1 summarizes some of the different risk assessment methodologies available to you.



EXAM TIP Because this is an ISACA-sponsored exam, it is a good idea to understand risk assessment terms and process from the perspective of the ISACA framework more so than any other. The ISACA Risk IT Framework directly aligns with ISO/IEC standards as well.

Performing a Risk Assessment

Now that we have discussed different frameworks that prescribe risk assessment processes, in this section we'll go through some of these processes in a little bit more detail. By and large these processes are common to the different risk frameworks we've discussed, although the steps and names may be slightly different between frameworks. Nevertheless, these steps are accomplished during risk assessment and analysis, and it's more important that you know the general order and activities that occur during risk assessment and analysis than how they are described in any one particular framework or another.

Collecting Data for the Assessment

One of the challenges for a risk assessor is collecting and managing all the data for an assessment. On one end of the spectrum, the assessor may find it difficult to get the bare minimum of relevant data for a particular asset, threats and threat actors, and vulnerabilities, as well as protective controls. On the other end of that same spectrum, the assessor

may gather so much data that it is overwhelming to analyze and gauge its relevancy to the assessment effort.

Another challenge is the source of the data. While the best data comes from authoritative sources that have expertise in various areas, such as the asset or system in question, current threats, and so on, the assessor has to be able to separate fact from opinion and collect truly objective data versus subjective data. Objective data is evidence that supports an assertion about an asset or risk, which can be proven or verified through independent means. Subjective data, on the other hand, is data whose validity is subject to opinion. For example, auditing normally produces objective data, in the form of audit logs (assuming they are secured) that detail events that occur on a system and trace those events back to individuals, ensuring accountability. Events in question can be verified through the audit logs. System administrators, however, who assert that they regularly audit system activities but have no audit logs to prove this can't have their claims verified. Additionally, if there are no policies or procedures that require auditing or show how to perform those tasks, these events can't be independently verified either.

Data can come in various forms, including performance data, statistical analysis, historical data, trends, or narrative form. The relevance of data should be established by the assessor as it is collected and depends on how it answers relevant risk questions that relate to threats, vulnerabilities, likelihood, impact, assets, and controls. Overwhelming amounts of data can be reduced to relevant summaries and analyzed, sometimes in aggregate, using various automated statistical analysis and database tools.

Data collection typically uses a combination of four methods, designed to collect various types of qualitative and quantitative data from different sources. These collection methods serve to complement and support one another, filling in gaps from one method and verifying information collected from another. The four main methods of data collection are conducting interviews, reviewing documentation, observing systems and assets in operation, and performing technical testing on assets. They are described in more detail in the following sections.

Conducting Interviews One of the best methods to start collecting data involves interviewing key personnel, such as asset owners, system administrators, security personnel, and other people with direct knowledge of important aspects of the asset, relevant threats and vulnerabilities, and controls. Interviews should be scheduled with key personnel and consist of relevant questions that answer questions relating to security posture, processes and procedures, asset characteristics, and implemented security controls. The assessor should carefully record interview results through concise meeting notes or recording devices, for later reference. Keep in mind that while interview data should usually be considered subjective in nature, it can be used as a starting point to gather knowledge and facts about a system that can be later verified using other means, such as documentation, system observation, and testing.

Documentation Reviews Documentation is a mainstay during a risk assessment. A well-documented system indicates what its characteristics are, what security requirements it has, and whether the people responsible for the system have defined processes in place to fulfill system security responsibilities. Documentation gives an assessor a wide variety of information on how the system is routinely used, whether a security patch

program is in place, who has access to systems and data, what policies exist to define security requirements, and how the system is securely configured. Documentation can be either paper-based or electronic; it can come from spreadsheets, databases, network devices, systems, written procedures, physical access logs, and so on. Examples of documentation include organizational policies, backup and restore procedures, security officer appointment letters, and so on. While not strictly documentation (unless printed), audit logs and configuration files could also be considered in this category since they provide documentary evidence that supports an assertion of how events were recorded or how a system was configured. Documentation also serves to verify data collected from other sources, such as interviews. Remember, in the security assessor world, if you don't document it, then you can't prove that you do it.

System Observation and Verification Sometimes it's not enough to interview personnel and review documentation. Unfortunately, people can lie or be mistaken in interviews, and documentation can be falsified. Observing a system in operation can verify whether it is secure and whether its security functions and controls are actually working as intended to protect systems and data. The same is true for physical security controls. An assessor can easily determine whether a control is functioning by observing a system operator perform a security function or by visually inspecting a control to make sure it is in place and implemented properly. Examples requiring the observation method include gates, guards, and locks; other examples are watching a system through the boot process, observing a screen lock go into effect, having a system administrator show you various security features, and so on.

System Testing Obviously, not all data can come from talking to people, reading system architecture documents, and watching the system administrator assign permissions to shared folders and files. Some data must come from looking at the configuration of the system itself, as well as getting relevant data that pertains to patching, vulnerabilities, user accounts, configuration files, registry settings, and other technical data. This data is used to determine not only if a system is configured properly and securely but also what potential vulnerabilities might exist on a system. This is where the technical assessment portion of data collection comes into play. Since technical data can be overwhelming in size and volume, automated tools are typically used to perform system security testing. These tools include vulnerability scanners, sniffers, and other hardware and software tools, some of which are described in Chapter 6.

During system security testing, various types of host-based and network scans may be performed, along with in-depth examination of patches and updates that have been applied to the system, configuration settings, user accounts, and other security settings. Rights, permissions, and privileges on the system and its resources are examined and compared against security requirements and control functions to ensure they match. Network protocols and connections are studied, and the network architecture may be examined to ensure a sound network design has been implemented. Application software code reviews and testing, including fuzzing, may be performed. Authentication and encryption mechanisms are examined in-depth to ensure they are strong and effective and meet governance and best-practice requirements where applicable. Physical access

Method	Examples
Interview	System administrators, facilities personnel, security personnel, asset managers, common control providers, risk management personnel, control owners
Documentation review	Architectural diagrams, printed system configuration files, printed audit logs, access control logs, risk and incident reports, security procedures
Observation	System configuration, resource access controls, physical controls, security processes and procedures as they are being performed, system functions
Test	Systems, networks, devices, controls, procedures, ports, protocols, services, system security configuration, vulnerability scanning

Table 4-2 Summary of Data Collection Methods During a Risk Assessment, with Examples

controls may be tested to ensure that physical separation away from systems for unauthorized users is maintained.

The results of system security assessments (usually in the form of vulnerability assessments or penetration testing, discussed further in Chapter 6) are consolidated with the results from interviews, documentation reviews, and system observations to form a comprehensive data picture of the system or asset; these results further inform the controls analysis and impact determination aspects of risk. Table 4-2 summarizes the different data collection methods you can use during an assessment.



NOTE While you may not be directly tested on data collection methods, it is a good idea to understand these methods, as in actual practice, you will likely use them extensively.

Asset Identification and Categorization

As you'll recall from the discussions in Chapter 3, identifying the different elements of risk is a necessary precursor to assessing risk. One of the goals of the identification process is the development of risk scenarios. Risk scenarios require that you identify assets, vulnerabilities, and potential threat events.

Asset identification not only requires you to inventory all of your assets; you should also determine how critical they are to your business, decide how sensitive the data they process or produce is, and characterize the system or asset in terms of confidentiality, integrity, and availability. Determining criticality is an important aspect of the overall risk management process and typically is done before any assessment takes place. The NIST RMF process, in fact, requires that you perform a system categorization on assets in the first step of that framework. This system categorization later helps you to assign controls to the asset based upon its criticality factors. The set of controls that you assign to each asset, based upon its criticality, is what is actually assessed, for effectiveness in both mitigating risk and compliance. Chapter 6 will also go into more detail on controls and assessing them.

Threat and Vulnerability Identification

Once you have categorized each of your key assets, you must determine the vulnerabilities inherent to that asset and the threat events that could exploit those vulnerabilities. A vulnerability assessment can give you information about the weaknesses inherent to an asset. The vulnerability assessment might include examining all aspects of an asset or capability to determine any vulnerability it has, including the physical, technical, and operational vulnerabilities inherent to the asset. For example, there can be technical vulnerabilities related to configuration issues or lack of hardening on a network device. Physical vulnerabilities could relate to the lack of physical protection for the network device. Operational vulnerabilities might include the lack of backup processes or configuration control exercised for the device.

You will need to do a threat assessment to determine what threats and threat agents exist that could exploit those vulnerabilities. These threats can be internal or external, can be human-made or natural, and should match up with a discovered vulnerability. To complete the development of a given risk scenario, you should consider time and location characteristics of a potential scenario as well. Remember that you are developing scenarios down to the most practical level of detail possible; you will have developed many different possible scenarios for an asset, each covering a particular threat–vulnerability pairing by the time you are done. You should then look at the existing controls you have in place to determine how effective they are in protecting an asset.



TIP Threat and vulnerability assessments are discussed a great deal in this and other chapters of this book. These two assessment processes are critical to understanding the elements that formulate the risk for an asset.

Control Analysis

After you've accomplished asset categorization and determined threats and vulnerabilities associated with those assets, then you must take stock of what existing controls or mitigations you've implemented to determine the level of protection an asset currently has. Based upon this existing level of protection, you should be able to determine the impact to the asset if a particular vulnerability is exercised by a specified threat and how likely that event is, given the protections you have in place. All of this information helps to identify the basic risk involved. Chapters 5 and 6 go into much more detail on how controls are managed, as well as on responding to risk after a risk assessment.

Likelihood Determination and Impact Analysis

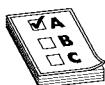
Evaluation is the next step of the process, where you must determine the likelihood of a given threat agent initiating a threat or of an identified threat exploiting a given vulnerability, as well as the level of impact or harm to the asset if a vulnerability were successfully exploited by a threat. While threats and vulnerabilities in assets are necessary ingredients to determine risk, they are static ingredients; in other words, threats, vulnerabilities, and assets don't change much. Likelihood and impact, on the other hand, are variable and are

the primary factors in measuring risk. People who don't understand how risk is framed often mistakenly state risk as a result of only one individual element. You could say that the risk to an asset is high, for example, simply because the likelihood of the negative event occurring is high. You could also say that risk is high because the level of impact if a negative event were to occur would be high as well. But neither of these statements alone really captures the sense of risk. This is because individually they do not convey the other dimension of risk since risk is a product of *both* likelihood and impact. Additionally, you can't make these determinations without the background knowledge of the threat, the vulnerability, and the asset.



CAUTION Make sure you consider controls and their effectiveness when analyzing risk since controls can help decrease likelihood or reduce impact, thereby decreasing the assessed risk for an asset and the organization.

Evaluation involves the measurement of these two primary factors, likelihood and impact. We've already discussed how there can be different ways to measure these factors, based upon subjectivity or concrete values. This is where the discussion on qualitative and quantitative techniques comes into play. We'll go into depth on those assessment techniques next.



EXAM TIP Remember that risk assessments are comprised of the steps of risk identification, evaluation, and analysis. Identification produces threat-vulnerability pairs, asset inventories, and risk scenarios. Evaluation covers likelihood and impact calculations, resulting in risk values. Analysis looks at the overall application of these factors, as well as control analysis, to produce a comprehensive picture of risk.

Quantitative and Qualitative Techniques

You could take two different security professionals, both trained in the latest standards and practices associated with risk management, and have them both do an assessment on the same system, and, chances are, they would produce similar reports, but they would not be exactly the same. Why is that? It's because there are so many different methods of conducting risk assessment and analysis, depending on what governance the organization falls under, how the organization has framed its risk, and so on, that the risk would never be assessed exactly the same; there are too many variables involved. Add to that complexity the natural subjectivity of human beings, and you may have very different risk reports. However, most risk assessment methodologies are still based fundamentally on the two primary ways to assess risk: qualitative and quantitative. Both of these methods have value, depending upon the context of the situation, and often both methods can be combined. We will discuss these techniques at length in the upcoming sections, as well as how they can be used together.

Quantitative

A *quantitative* risk analysis uses concrete (nonsubjective) numerical values and statistical analysis to calculate the likelihood and impact of risk. Quantitative methods use numerical values such as dollar figures, statistical numbers, and any other hard-core numerical assignments. Quantitative risk assessments follow the same general pattern described previously; you must first list your assets (along with their replacement costs and exposure factors), calculate the impact of a full or partial loss of the asset, determine the likelihood of the negative event, and come up with the overall risk to the organization. This might be calculated in terms of dollars, for example. The following is a scenario that will help you to better understand quantitative risk analysis, as well as some of the factors that can actually be quantified and how.

Quantitative Risk Analysis: A Scenario

Let's say you are a new employee in a small family-owned business that has no other security professionals employed. You've been tasked with developing a risk management strategy and program for the business. Suppose the business had a small server farm that was located in an older building on your small campus, with wooden walls, older wiring, no backup electrical power, and reasonably good fire detection and suppression systems. The server farm contains four servers, each performing a specific data-processing function. The data is backed up weekly, but it takes time to restore, and there is a good likelihood that some of the data would be lost because of the weekly backup schedule. Let's also say (just for the sake of illustration) that each of these servers costs \$10,000 to replace with a new server (since they don't make your model any longer, unless you were lucky enough to find a cheaper one on eBay). You've attempted to quantify factors for the owners, such as recovery time objective (RTO) and recovery point objective (RPO). These factors tell you how much data you could afford to lose if a disaster happened (such as a fire burning down that small wooden building) and how fast you would need to recover data in order to resume business operations in order to avoid suffering a significant loss of business.

Let's assume that the small business is located in an area prone to thunderstorms, tornadoes, and hurricanes. One of the natural incidents that could occur in these areas is a lightning strike during a thunderstorm, where lightning strikes the metal roof of the building and one of the servers suffers a power surge that completely renders it inoperable. If, after such an event, an assessment determines that the server can't be repaired, you decide to buy another one. The replacement cost of this server is \$10,000. Let's do some simple quantitative analysis on this scenario:

$$\text{Asset value (AV)} = \$10,000$$

Exposure factor (EF) = 1 (in this case, a 100 percent loss of the server and its data)

$$\text{Single loss expectancy (SLE)} = \text{Asset value (AV)} \times \text{Exposure factor (EF)} = \$10,000$$

With an SLE of \$10,000, you have to hope this scenario never happens. However, based upon analysis of historical weather patterns in the area, and given the shoddy construction and limited electrical protections of the building the server farm sits in, this seems to be a likely possibility. So, you should determine how much the organization is likely to lose, per year, on such a scenario. You can calculate this if you know a couple of other pieces of information. First, you need to know about how often to expect a severe

storm in the area, say on an annual basis. This annualized rate of occurrence (ARO) could be used with the SLE value given earlier to determine your loss expectancy for one year.

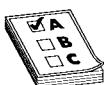
$$\text{SLE} \times \text{ARO} = \text{Annual loss expectancy (ALE)}$$

So, given that severe thunderstorms are historically shown to occur 15 times per year in your area (likelihood), you could conclude the following:

$$\$10,000 (\text{SLE}) \times 15 (\text{ARO}) = \$150,000 \text{ in potential loss per year (ALE)}$$

Obviously, this is a bit of a stretch. Even if there are 15 severe lightning-producing storms per year, it's not likely that each and every one would produce a lightning strike on your server building every time. Even if that *could* happen, it's likely that after it happens the first time, your small business owners would invest in a new facility or relocate its servers, thus reducing the possibility of the other events. So, you might also do some statistical analysis to find out what really is the likelihood of one or more of those 15 severe thunderstorms causing a lightning strike on the server farm building. This analysis might significantly reduce the likely number of events from 15, to say, 3. Now your ALE would be a potential loss of only \$30,000 per year. Keep in mind that the numbers are there to show you the *potential* risk to the organization, which in this case is expressed as lost dollars, in terms of revenue and assets. Note that these formulas are based upon standard basic risk analysis concepts taught in information security certification programs, such as CompTIA's Security+ and (ISC)²'s CISSP program.

Again, the previous scenario is a simplistic (but not too terribly unrealistic) example. Other factors could come into play that are not considered in the previous simple analysis. For example, suppose the business is losing \$1,000 dollars per day in revenue for every day this server is out of commission, which the previous calculations do not take into account. This consideration not only is related to the SLE value (since it increases the SLE over time) but also influences your RTO and RPO values. You should also realize that this scenario takes into account only one of the servers; a better risk assessment should include the possibility of all the assets being partially or completely lost. Additionally, it's possible that a total loss of a server may not occur; let's say it's only a partial loss (say, 40 percent, or an EF of 0.4), which would reduce the SLE for that single asset ($\$10,000 [\text{AV}] \times 0.4 [\text{EF}] = \$4,000$). So, you must take all of this into account when performing a quantitative risk analysis. There are so many other factors that we haven't mentioned here that could figure into your SLE values (asset depreciation, lost labor hours to repair or replace the server, and so on), but you can see the basics based upon this simple example.



EXAM TIP Be familiar with the elements of quantitative risk assessment techniques, such as asset value, exposure factor, single loss expectancy, annual rate of occurrence, and annualized loss expectancy.

The final piece of this puzzle is how much it would cost the organization to reduce this risk. Let's examine all of the factors that the organization could influence. First, it could not influence the weather, so the threat agent and threat can't be reduced or eliminated.

The organization could, however, address the vulnerability (the server building with its ineffective protections against bad weather, in this case), reducing it somewhat by relocating the server farm or even moving its applications and data to the cloud, for example. The organization could also reduce the likelihood for that particular threat-vulnerability pairing if it removed or changed the nature of the vulnerability itself, as described earlier.

The organization could also reduce the impact of this specific event in several ways. It could create a real-time failover cluster for the servers in another location that would instantly be available if said servers got struck by lightning, or it could at least have a hot spare server and a recent backup, if nothing else. The organization can affect the risk factors, but there is a cost for doing this. What is important in developing risk responses is that the organization must balance the cost of mitigations (for example, acquiring another facility, moving to the cloud, server clusters, or at least hot spares and better backups) with how much it loses in terms of SLE and ALE and the added impact of lost revenue per day, as in this example. The bottom line is that you must find a solution that isn't more expensive or impacts the organization to a degree worse than the risk event itself. Risk responses are covered in more detail in Chapter 5.

Qualitative

A *qualitative* risk analysis, on the other hand, involves using subjective scales. These scales could be a numerical scale from one to ten or have subjective values of High, Medium, and Low, for instance. Qualitative risk analysis can come from historical trend analysis, experience, expert opinion, existing internal and external environmental factors, governance, and other inputs that are not always necessarily quantifiable but exist and are important nonetheless. Qualitative risk analysis is appropriate when you must evaluate risk based upon factors that can be hard to quantify, such as those that are not typically measured with concrete, repeatable values. For example, what numerical value could you assign to a potential impact of loss of consumer confidence or damage to reputation? You may attempt to frame it in terms of lost revenue (an educated guess at best) or loss of business. You could also survey a sample population to determine how many people would or would not do business with the organization after a data breach, for example, but even that would be subjective and would offer only a small statistical insight into a hard-to-define measurement.

That's not to say you couldn't assign numerical values to different risk factors, however. Instead of values such as Low, Medium, and High, you might assign numerical values that roughly correspond to those levels. For example, you might use a type of Likert scale, which may have values such as 1 (Very Low), 2 (Low), 3 (Medium), 4 (High), and 5 (Very High). This might characterize the subjective level of impact or likelihood the organization wants to assign to a particular risk event. In assigning these subjective values, you must also decide how they relate to each other, yielding an overall risk calculation. In other words, given likelihood values of 1 (Very Low), 2 (Low), 3 (Medium), 4 (High), and 5 (Very High), and identical values for impact, what would the overall risk level be when these two dimensions of risk are viewed together? How do their values affect each other? NIST Special Publication 800-30 offers a good example of how risk is calculated using qualitative analysis.



NOTE NIST SP 800-30 refers to numerical scales as semiquantitative values since they are numerical values that can be used in calculations but are still subjective in nature (in other words, they cannot be independently derived or repeated and are based upon informed opinion).

In Figure 4-1, taken from NIST SP 800-30, you can see how the relationships of likelihood and impact affect different risk levels. The values of each are correlated, and a qualitative risk determination results. For example, according to this figure, a *moderate* level of likelihood combined with a *very high* level of impact results in a level of risk determined as *high*. The determination of what constitutes a likelihood of moderate and what is required for an impact level of very high is subjective but should be defined within the organization for consistency and standardization.

Combining Quantitative and Qualitative Techniques

If you are thinking that a qualitative or quantitative assessment alone may not be enough to adequately capture the different elements of risk and develop an overall risk determination, you're absolutely right. While there are instances where each of these techniques can be used alone, in a majority of situations they are used together, to varying degrees. Each technique is good at producing a valuable piece of the puzzle, but sometimes you need both a quantitative perspective and a qualitative perspective on risk. For example, in the scenario we described earlier for quantitative risk, say you have numerical values for AV, EF, SLE, and ALE. These values account primarily for impact. However, suppose you don't have enough solid information for a calculation of likelihood. You might have to give it a "best guess" that comes from a reasonably well-thought-out analysis, using anecdotal data or another type of data that can't necessarily be quantified, but is a fairly accurate predictor. You may have to assign likelihood values that are semiquantitative or the subjective High, Medium, and Low values. There also might be other subjective factors that contribute to these values, so you would not have a purely quantitative assessment. Suppose you added "customer confidence" or "reputation" into the discussion on

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Figure 4-1 Qualitative assessment of risk (courtesy of NIST SP 800-30)

impact or loss to the company, for instance. Those would almost have to be qualitative values, so the assessment couldn't always be expressed in exact numerical terms that are easily repeatable or defendable.

In practice, most risk assessments are usually qualitative with some quantitative elements to them, or vice versa. There are usually few purely quantitative or entirely qualitative assessments performed. You should understand the elements and characteristics of both, however, for the exam and your profession.

Exercise 4-1: Performing Qualitative and Quantitative Assessments

Using the quantitative and qualitative techniques described earlier, go through the basic process of performing assessments with each technique. Use realistic assets and values from your organization or fictitious values and assets. What additional factors should you include that may affect these values? Do you find that some values can't be quantified using numerical values?

Other Analysis Techniques

Now that you know the basics of qualitative and quantitative techniques, there are a few specific techniques, based upon both of these methods, which we will discuss here so you are familiar with them for the exam. Note that there are dozens of different techniques that professionals have developed over the years to assess risk; you'll find that a majority of them fall into either the qualitative or quantitative methodology. The ISO/IEC 31010:2009 standard we briefly described earlier lists more than 30 such techniques in its appendixes. Some of them approach assessments from different directions, but most of them have several things in common. We'll discuss just a few of these in the next sections.

Fault- and Event-Tree Analysis

A fault-tree analysis is a method where the analyst starts with a risk event and looks for all possible causes of the event. This is diagrammed as a tree, with the risk event at the root and the causes extending away as branches. This analysis is used to discover all of the potential causes of the event (threats and threat actors in this case) so that they can be further analyzed for likelihood. Similar to the fault tree, the event-tree analysis is also diagrammed as a tree structure but takes the opposite approach (bottom-up as opposed to top-down). In event-tree analysis, an initiating event is at the root of the tree, with all possible consequences (impacts) diagrammed from the root as branches (as opposed to causes of the event in fault-tree analysis). Both fault tree and event tree are predictive analysis tools; in other words, they seek to predict relationships between causes, events, and consequences. Figures 4-2 and 4-3 show examples of both fault-tree and event-tree analysis diagrams, respectively.

In Figure 4-2, a risk event (in this case, a firewall failure) is shown, with the potential causes shown as no rule configured, a firewall appliance failure, and unknown or unusual traffic. Note that the risk event itself is the root of the tree. Conversely, in Figure 4-3, an event-tree diagram, the risk event (in this case, a break-in to a corporate facility) is also at the root, but the branches leading away are the potential consequences, not the causes.

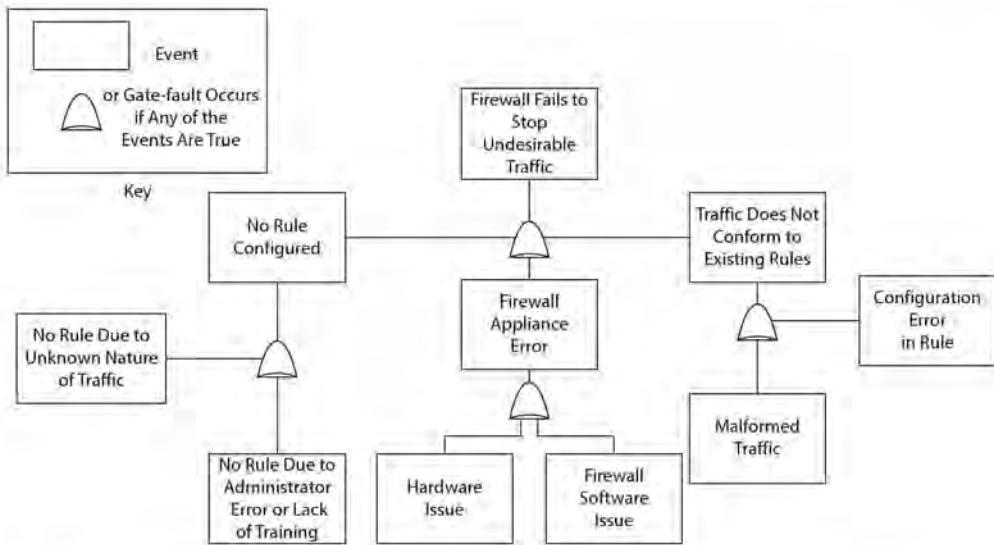


Figure 4-2 An example of a fault-tree analysis diagram

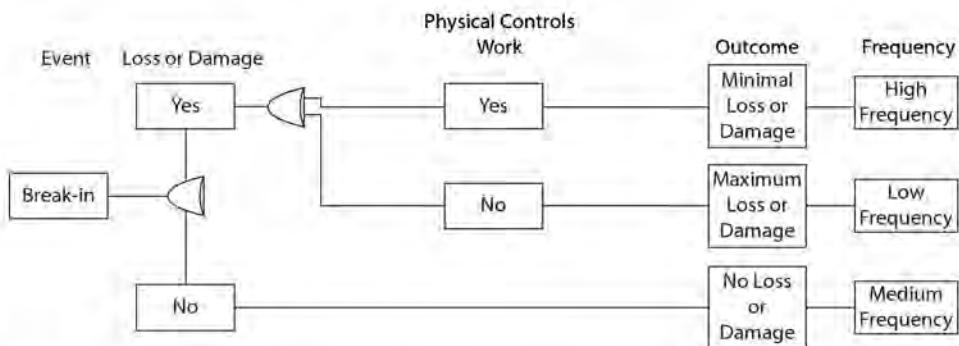
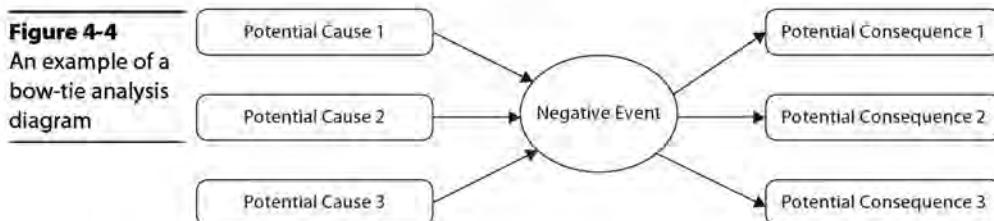


Figure 4-3 An example of an event-tree analysis diagram

Bow-Tie Analysis

A bow-tie analysis uses diagrams to analyze and explain relationships between various elements of risk, from causes (threats) to events and then to impacts (consequences). It is similar to both the fault-tree analysis and the event-tree analysis since it looks at the various causes of a risk event (fault tree) and also analyzes the consequences of the event (event tree). The difference, however, is that the bow-tie analysis looks at the intervening characteristics of the events and causes, such as the path by which the cause leads to the event and then the consequences. Figure 4-4 illustrates a bow-tie diagram. In this figure, the negative event is shown as the center of the bow tie, with potential causes on the left and possible consequences on the right.



Other Methods

As mentioned, there are too numerous other methods that exist to perform the different types of assessments to mention here. Some of these methods focus on data collection, while others emphasize different group analysis techniques. All are, again, some variation of either the qualitative or quantitative method and may require looking at specific aspects of data to determine various elements of risk. Other examples of these techniques include the Delphi method, which centers on expert opinion from questionnaires; the Bayesian analysis method, which uses data distribution and statistical inference to determine risk probability values, checklists, scenario analysis, and business impact assessment (briefly described in Chapter 2); root-cause analysis (discussed further in Chapter 6); and various collaborative techniques, such as brainstorming. You won't be expected to know all of these methods for the exam, but you should be familiar at least with the concepts of qualitative and quantitative analysis and some of the techniques that use each. For further knowledge on various assessment and analysis techniques, consult with ISO/IEC 31010:2009.



EXAM TIP You will not have to know any particular risk assessment method in detail for the exam, but you should understand how the qualitative and quantitative methods work.

Risk Analysis

Now that you've assessed impact and likelihood (using any of several qualitative or quantitative methods), it's time to perform the risk analysis. Risk analysis is just an extension of what you've been doing all along so far; a risk analysis looks at impact and likelihood values and determines what the level of risk is for a particular system, an asset, or even the entire organization. Part of risk analysis involves discussing findings with risk and control owners, as well as senior managers in the organization. During this discussion, you may discover other factors that influence the levels of likelihood and impact or even affect threats, vulnerabilities, and assets. You'll also look at the existing controls and determine how effective they really are in meeting risk, as well as recommend additional controls. Finally, after this process is complete, you will report risk analysis results to senior managers and generate a risk report. We'll discuss all of these topics in more detail in this section. Figure 4-5 shows a familiar variation of the 5x5 likelihood and impact

Likelihood	Impact				
	Very Low	Low	Medium	High	Very High
Very High	Very Low	Low	Medium	High	Very High
High	Very Low	Low	Medium	High	Very High
Medium	Very Low	Low	Medium	Medium	High
Low	Very Low	Low	Low	Low	Medium
Very Low	Very Low	Very Low	Very Low	Low	Low

Figure 4-5 Likelihood and impact are evaluated together to produce a risk level.

table, demonstrating how different levels of likelihood and impact are evaluated together to produce a qualitative risk level.

Control Analysis

In this section, we will discuss control analysis in detail. You'll also receive some more in-depth information on controls in the next three chapters, focusing on different aspects of how controls are designed, implemented, and used to respond to risk. It's important to understand how controls fit into the overall risk analysis process; you perform a control analysis before actually determining risk since existing controls that are already in place may be effective to varying degrees in mitigating risk. Simply examining threats, vulnerabilities, assets, impact, and likelihood without taking into account existing controls and protections in place doesn't do justice to the risk analysis process. Not accounting for existing controls would dramatically skew risk assessments and render an unrealistic risk determination. The goal here is to examine existing controls, determine how effective they are, and use that determination in analyzing the impact to assets if threats exploit vulnerabilities, as well as the likelihood of that exploitation. Typically, results of your documentation, observation, interviews, and testing will likely also be part of your control analysis. We'll look at different aspects of control analysis in the next few sections.

Evaluating Existing Control Effectiveness

As we stated earlier, part of risk analysis involves evaluating the effectiveness of existing controls. The reason for this is that risk doesn't exist in a vacuum filled with only threats, vulnerabilities, and assets. Almost all assets have some type of controls that serve to protect them from harm. These controls may not be sufficient enough to protect against certain threats. In some cases, however, a control may be implemented that significantly lowers the risk to an asset by decreasing the likelihood of a threat exploiting a vulnerability or by protecting the asset sufficiently enough to reduce the impact in the event a threat is realized. This is part of the risk assessment and analysis process, which involves not only identifying and prioritizing assets and performing threat and vulnerability assessments but also determining what controls exist and how effective they are in protecting against identified risk.

As previously described, controls fall into three broad categories: administrative, technical, and physical or operational controls. We've also described how controls can be categorized based upon function, classifying them as preventive, deterrent, detective, and

other critical control functions. When identifying controls that apply to a given resource, process, asset, or system, you should look at all of these different categories to determine exactly what controls exist. Administrative controls will be in the form of policies or procedures and can serve to protect an asset by detailing requirements that users must abide by. Technical controls can serve to protect assets by providing logical protections, which might include strong authentication, restrictive permissions, and other access controls. Physical and operational controls can provide asset protection in the form of operational procedures and physical barriers, which separate unauthorized persons from the asset and prevent them from physically accessing the asset. Consider all these different categories of controls when attempting to identify any controls that may be providing protection for assets.

Once you have identified all the different controls that are protecting a given asset, you should determine what functions they are required to serve and how well they're performing that function. Controls are designed to perform different security functions (in some cases only one but often many different functions). Economy of use is one important aspect of applying controls to assets; organizations that are able to use fewer controls to cover more security functions are able to reduce costs and more effectively use the resources they have.

Just as threats and vulnerabilities are often paired together, controls are often identified that match up with specific threats or vulnerabilities. While we discuss the value of performing threat and vulnerability assessments, seemingly as separate activities, often they are conducted simultaneously, along with control analysis, to get a better idea of how these three elements balance with each other. Threats exploit vulnerabilities; however, controls can reduce the likelihood of threat exploitation, as well as mitigate the weaknesses that vulnerabilities provide. So, there is a relationship between these three elements, making it valuable to sometimes look at all three of them simultaneously in a concerted effort.

In assessing control effectiveness, you should examine how well a particular control protects against a given threat or reduces a particular vulnerability. This can be a subjective process but can be more objective if performed as part of an in-depth penetration test (discussed in Chapter 6). For example, a threat assessment may give you only the potential threat events that could affect a given asset, and a vulnerability assessment may tell you only what potential vulnerabilities exist on the system. Neither tells you how effective a control may actually be in reducing the effects of the threat or vulnerability, unless you actually attempt to exploit the vulnerability during penetration testing. Only then will you truly know how effective the control really is; if a given vulnerability isn't easily exploitable, then realistically the control may be more effective than a cursory review would indicate. Likewise, a penetration test may indicate that a control is not as effective as you might have originally thought. Remember that vulnerability assessments describe theoretical weaknesses, whereas penetration tests actually attempt to exploit vulnerabilities and can give more realistic estimates of how effective controls really are.

When evaluating controls, you may report them as part of a risk analysis as ineffective, partially effective, or effective in reducing impact or likelihood. You also might use a semi-quantitative scale that indicates control effectiveness from a range of numerical values.

AC-5 SEPARATION OF DUTIES

Control: The organization:

- a. Separates [Assignment: organization-defined duties of individuals];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	Low Not Selected	MOD AC-5	HIGH AC-5
----	------------------	----------	-----------

Figure 4-6 The AC-5 control from NIST SP 800-53

Often, different control frameworks also provide guidance on assessing the effectiveness of the controls in that particular framework. For example, the catalog of controls found in NIST's Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," is supplemented by an assessment methodology found in its companion volume, Special Publication 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," which describes how to assess and report the effectiveness of each control. Figure 4-6 shows an example of a NIST control, from SP 800-53, and Figure 4-7 shows the corresponding assessment guidance for the same control in SP 800-53A.



EXAM TIP Control analysis includes identifying controls, determining their required function, determining whether they are effective in meeting that function, and identifying gaps between the desired and end states of how well controls protect assets.

Control Gaps

A control gap is a situation where existing controls are not sufficient to provide adequate protection for an asset, reducing either impact or likelihood (and thereby risk) to an acceptable level. In this situation, after the lack of effectiveness of the control is established, the organization has to look at remediating the situation. We won't go too much in-depth on remediation here; that's really the subject of the Risk Response domain that

AC-5	SEPARATION OF DUTIES							
ASSESSMENT OBJECTIVE: <i>Determine if the organization:</i>								
AC-5(a)	AC-5(a)[1]	<i>defines duties of individuals to be separated;</i>						
	AC-5(a)[2]	<i>separates organization-defined duties of individuals;</i>						
AC-5(b)	<i>documents separation of duties; and</i>							
AC-5(c)	<i>defines information system access authorizations to support separation of duties.</i>							
POTENTIAL ASSESSMENT METHODS AND OBJECTS:								
Examine: [SELECT FROM: Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system access authorizations; information system audit records; other relevant documents or records].								
Interview: [SELECT FROM: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties; organizational personnel with information security responsibilities; system/network administrators].								
Test: [SELECT FROM: Automated mechanisms implementing separation of duties policy].								

Figure 4-7 Assessing the AC-5 control, from NIST SP 800-53A

you'll read about in the next chapter. However, during your analysis, you must identify control gaps and may even make recommendations as to possible response options that would close those gaps. You may identify gaps in physical, technical, or administrative controls, even when there are other types of controls present that perform some security and protection functions. For example, if an organization is implementing account management processes, such as creating accounts in a standardized fashion, verifying identities before user accounts are created, and so on, then it has operational and technical controls in place that help provide secure account management. However, if the organization has no written policy in place that actually requires this process and dictates that it be performed in a consistent manner, how can the organization be assured that these procedures will always be followed uniformly and in a secure manner? If there is no policy, then the organization leaves it up to individual account operators to perform this function as they want, regardless of how "most people do it." In this case, a control gap would be that although the organization is applying some level of control over this process, there is no written policy ensuring that it is standardized.

Control Recommendations

Once you've identified existing controls, determined how effective they are, and identified gaps between the current and desired end states of controls, you should be in a position to make sound, risk-based recommendations to senior managers on how controls should be supplemented, added, or changed. Recommending controls is in itself

a risk-based process; remember that there is risk that you are trying to minimize, but you must balance this between control functionality and economy of resources. There are several considerations to keep in mind when making control recommendations.

- What more could be done to supplement or change existing controls to close the gap between current and desired end states of risk?
- Should new or different controls be applied to replace existing ones?
- What are the costs involved in applying additional controls, and do they exceed the value of the asset or the costs to replace it?
- Would additional controls require retooling or significantly changing the infrastructure, processes, or asset itself?
- Would additional controls require new personnel or training for current personnel?
- Can additional controls be implemented that also reduce risks in other areas (economy of use)?

The answers to these questions, at least some of them, will determine how you make the recommendations to management about closing the “control gap.” Both the cost of implementation and the return on investment received from implementing new controls or strengthening existing ones are going to affect management’s acceptance of the recommendations. The asset value, or impact if it were significantly damaged or lost, will also affect how well the recommendation is received. Implementing a costly control to protect an asset that is worth less in terms of impact is not usually an economically sound decision. Organizational levels of risk appetite and tolerance will also affect control recommendations since any new or additional controls must reduce risk enough to fall within those levels. In general, when recommending ways to close the control gap, whether it is by introducing new controls, modifying existing ones, or modifying the infrastructure to reduce likelihood or impact, you should do the following:

- Try to leverage existing controls that can be used across the board to include additional assets.
- Look for “quick wins” first—controls that are easily and inexpensively implemented (such as policies, training, procedure changes, and so on).
- Prioritize control recommendations with risk; the greater the risk, the more attention that should be paid to those particular control gaps.
- Be realistic in your recommendations: You can’t reduce risk to absolute zero, you don’t have all of the resources you would like at your disposal, and you don’t have to offer a 100 percent solution. Sometimes a 70 percent solution is better than a 0 percent solution.
- Provide alternatives to your primary recommendation for each control gap. Give management alternatives based on cost, level of risk reduction, and effectiveness.

Considering Risk and Control Ownership

Risk and control ownership are issues that must be taken into account during a risk analysis. Depending upon how the organization is structured and how the risk management strategy has been developed, risk ownership may be assigned to one or several different managers, spanning multiple functional areas. This is because the risk that affects one area likely affects other areas as well, so many different people may have responsibility over affected areas and be required to deal with and respond to risk. Control ownership is also something that should be examined; often controls that provide protections for a given asset or a number of systems may not fall under the operational purview of the risk owner. Some controls span the entire organization and protect multiple assets, rather than only a specific system. These are referred to as *common controls*, and the responsible entity for these controls is the *common controls provider*. For example, consider physical security controls. There may be a physical security officer for the organization that is in charge of guards, personnel security, and access to secured areas. They may also be responsible for locks, closed-circuit televisions (CCTVs), and physical intrusion detection systems and alarms. All of these controls serve to protect information systems and data assets that might be in a secure data center. Risks may be presented to the person who is responsible for information systems in the data center, but the controls that serve to protect them may belong to the physical security functional area. This will require some coordination between the different functional areas if controls managed by one functional area are insufficient to protect assets managed by another area. This may also affect organizational structures, budget, and allocation of resources.



CAUTION Risk, asset, and control owners are not always the same person, functional area, or even organization. It's important that you identify these particular owners early in the assessment process and maintain careful coordination and communication between these and other relevant stakeholders, within the boundaries of your authority and assessment scope. Different types of owners can result in politically sensitive issues that revolve around resourcing, responsibility, accountability, and, sometimes, blame.

Reporting Risk Assessment Results

After the risk assessment is performed, the results are reported to the key managers in the organization. Most organizations have their own methods for generating formal reports, which may include detailed reports that describe technical deficiencies or simply high-level reports or briefings that describe risk on a generalized basis. Some risk reports may also map IT risk to business processes in order to communicate exactly how IT risk affects business operations. In any case, determining risk and framing it in such a manner that senior executives and managers can understand, particularly in terms of business cases, is a key part of communicating the results of risk assessment. We discuss communicating the results of the risk analysis, as well as documenting risk and updating the risk register in the next few sections.

Risk Determination

How risk is determined and defined largely depends upon the organization's risk management strategy, on the methodology used, and, to an extent, on the organization's risk culture, appetite, and tolerance. Some organizations may want to see risk expressed as bottom-dollar figures relating to the cost of remediation; the risk assessor's job is also to determine and express risk as an impact on business processes. More often than not, the risk determination will be reported as both qualitative and quantitative values since cost is only one of the measurements of risk.

Risk should be determined based upon impact and likelihood values after existing controls are taken into account. The risk that is calculated at this point must be responded to by accepting it, mitigating it, transferring it, or avoiding it. After a viable risk response option is selected, there will still be risk left over; remember that this is called *residual risk* and will always exist. The organization must determine whether the residual risk falls within the organization's ranges for risk tolerance and appetite. Risk determination, and the processes that support it, should be communicated to management as well, to give them a better understanding of the scope and scale of risk.

Communicating Risk Analysis

Communicating risk results can be one of the most difficult parts of the entire process. Frequently, the risk assessor is charged with briefing not only their own managers but also managers and executives within the entire organization. This can be challenging simply because, unless their daily duties involve risk management, many of the people receiving this information won't quite understand the purpose for the assessment, the methodology used, and how significant the findings really are. They also likely won't understand how risk is determined. What they should understand, however, is how IT risk relates to any impact on their business processes and operations. That's part of what should be communicated to the different stakeholders in the organization since IT risk is a subset of, and directly impacts, business risk. IT risk should be communicated in such a way that the different asset, risk, and control owners are made aware of how it affects the confidentiality, integrity, and availability of the information systems and data to support their business processes. This may require a bit of education for the stakeholders on the part of the risk assessor. While everyone may not agree with the risk assessment or like the fact that it will cost them resources to respond to it, they should be able to completely understand it and not make decisions based upon ignorance. Stakeholders should also be educated on the different risk response options available since often they will be responsible for resourcing these options from their own budgets and implementing them.



NOTE Most organizations have formal risk reporting and communication procedures, and sometimes these also require restricting access to risk results and other information. Understand your communication requirements and restrictions before the risk assessment begins so you will know with whom, how, and how much you may communicate about these subjects.

Results Documentation

Documenting the results of a risk assessment involves carefully and accurately recording the process of assessing risk for the organization, as well as the results of that process. Documentation includes presenting an executive summary and briefly describes the risk of analysis results, as well as the general aspects of the assessment itself, including scope, limitations, delimitations, assets assessed, information owners, risk owners, and control owners. The general aspects of the assessment may also discuss timeframes and the methodology involved in the assessment. The key of this part of the assessment is that you are trying to communicate supporting information to the right people so that they have the information they need to make risk-based decisions supporting risk response. Documentation could also produce detailed technical findings, such as those that might result from threat or vulnerability assessments. Normally these are included as appendices to the risk assessment report. In some reports, risks and findings are also mapped to controls as part of a formal risk management or compliance monitoring effort.

Documentation also involves updating the risk profile for the organization, which usually details characteristics of risk at the organizational level, as well as at the lower levels involving processes, systems, and other resources or assets. Normally, all of this documentation is reviewed by senior management, as well as the appropriate risk or control owners. Note that documentation should be carefully controlled; only appropriate people within the organization who have a valid need to know should be able to access this information, and it should be considered sensitive information for the organization.

Updating the Risk Register

Because the risk register is a living document, it should be periodically updated as risk conditions change. Obviously, risk assessments will provide updated information that should be included in the risk register, as well as information about ongoing risk response actions applied to the risk. Whether the risk register is in the form of an electronic database, spreadsheet, or other type of document, it should be easy to read and readily accessible by managers or risk owners so they can stay updated on the current risk posture of the organization. As mentioned previously, it also should be considered a sensitive, access-controlled document. Table 4-3 shows a risk register and some sample entries.

Risk Description	Likelihood	Impact	Risk Owner	Resources Required		Estimated Completion Date	Actual Completion Date	Current Status	Comments
				(Hours, Dollars, etc.)					
Data theft from malicious user (via risk assessment in April 2015)	Medium	High	Engineering department	\$10,000 for new DLP system		January 2016		Assessing DLP vendors	Purchase and different implementation by December 2015
Loss of primary accounting server data	High	High	Accounting department	\$15,000 for backup system		October 2015	September 2015	Vendor selected	Final purchase and installation in August 2015

Table 4-3 Sample Entries in a Risk Register

Exercise 4-2: Assessing Risk

Using one of the risk assessment frameworks or standards described previously, go through the basics of a mock risk management process for your organization, using all of the steps outlined in the supporting framework's publications. Since this is only a paper-based exercise, notionally go through the different steps for characterizing systems, identifying threats, identifying vulnerabilities, and so on. Record your responses. After you have finished, review the process and your responses. Were you able to complete all steps?

Chapter Review

Risk assessments include risk identification, evaluation, and assessment. While identification involves developing risk scenarios by identifying threat agents, threat and vulnerability pairs, and the affected assets, risk evaluation looks at the likelihood and impact variables, which indicate how likely a threat and vulnerability pair is to occur, causing a significant impact to an asset. Analysis also looks at controls and rolls the assessment up into a comprehensive risk determination for the organization. In this chapter, we also further reviewed different risk management and assessment frameworks and standards, including NIST RMF, OCTAVE, the ISACA Risk IT Framework, and the ISO/IEC standards.

We also reviewed the basic generic steps of conducting a risk assessment, including risk identification, threat and vulnerability assessments, asset identification, categorization and prioritization, and control analysis. We discussed key aspects of assessment that include evaluating likelihood and impact and their relationships to the other risk elements.

We discussed the value of both qualitative and quantitative assessment methods. Quantitative techniques primarily use quantifiable numerical values, such as cost and statistical analysis, as factors in assessing likelihood and impact. Qualitative values are subjective and are not easily definable or repeatable. Qualitative values might include a range of values or designations such as High, Medium, and Low. Most risk assessments use a combination of these techniques.

Finally, we looked at other aspects of risk analysis, including control evaluation and gaps, as well as recommending additional controls for risk response. We discussed risk and control ownership and communicating risk to these stakeholders. Reporting risk and updating the risk register are also key parts of the assessment process, as are maintaining risk profiles and monitoring risk on a continual basis.

Review Questions

1. What is the first step in risk management?
 - A. Risk evaluation
 - B. Risk classification
 - C. Risk identification
 - D. Risk response

2. Which of the following steps in the four-step NIST risk assessment guidance should be accomplished after identifying threat sources and events?
 - A. Determining magnitude of impact
 - B. Identifying vulnerabilities and predisposing conditions
 - C. Determining likelihood of occurrence
 - D. Determining risk
3. Which two of the following factors are the primary focus during risk evaluation? (Choose two.)
 - A. Likelihood
 - B. Impact
 - C. Threat
 - D. Vulnerability
4. Which of the following techniques uses subjective terms for its evaluation?
 - A. Statistical
 - B. Quantitative
 - C. Asset valuation
 - D. Qualitative
5. Which of the following quantitative formulas is used to express the annualized loss expectancy (ALE)?
 - A. EF × SLE
 - B. AV × ARO
 - C. AV × EF
 - D. SLE × ARO
6. Given an asset value (AV) of \$20,000 and an exposure factor (EF) of 0.5, what is the annualized loss expectancy (ALE) where a specific negative event is expected to occur once every two years?
 - A. \$10,000
 - B. \$20,000
 - C. \$5,000
 - D. \$2,500
7. Which of the following assessment methodologies uses a workshop methodology and is specifically intended for large organizations?
 - A. OCTAVE Allegro
 - B. OCTAVE-S
 - C. OCTAVE
 - D. The ISACA Risk IT Framework

8. Which of the following evaluation processes in the ISACA Risk IT Framework is concerned with analyzing risk?
- A. RE1
 - B. RE2
 - C. RG3
 - D. RR1
9. Which of the following data collection methods is the *most* subjective?
- A. Documentation reviews
 - B. Interviews
 - C. System observations
 - D. System security testing
10. You have a system administrator who you're working with during a risk assessment. The system administrator insists that adequate permissions are assigned to system files. Which of the following methods could you use to visually confirm the system administrator's assertion?
- A. Documentation review
 - B. Fault-tree analysis
 - C. Interviews
 - D. System observations
11. Which of the following must be examined after threats, vulnerabilities, assets, likelihood, and impact are taken into consideration in order to adequately analyze risk?
- A. Controls
 - B. Threat actors
 - C. Risk ownership
 - D. Risk profiles
12. Which of the following types of analysis examines an event strictly from the cause perspective?
- A. Bow-tie analysis
 - B. Event-tree analysis
 - C. Fault-tree analysis
 - D. Brainstorming
13. Which of the following standards is primarily concerned with risk assessment?
- A. ISO/IEC 31000
 - B. ISO/IEC 27005
 - C. ISO/IEC 31010
 - D. ISO/IEC 27000

14. Which of the following terms describes the difference between how controls are currently functioning and the level they need to be functioning at?
- A. Control enhancements
 - B. Supplemental controls
 - C. Control effectiveness
 - D. Control gap
15. Which of the following terms describes an entity responsible for controls used across several different assets and systems within the organization?
- A. Common controls provider
 - B. Risk owner
 - C. Asset owner
 - D. Control owner
16. Once a risk assessment is completed and recommended controls are put into place, at what level should residual risk fall?
- A. Below the level that it costs to replace an asset
 - B. Within risk appetite and tolerance levels for the organization
 - C. Below the level of the priority of the asset
 - D. Within a range of values predetermined before the risk assessment
17. Which of the following is the most critical point to convey to managers when communicating the results of a risk assessment?
- A. The risk assessment methodology used
 - B. How impact and likelihood values are calculated
 - C. How much it will cost to remediate discovered risks
 - D. How IT risk relates to any impacts on business processes and operations
18. Who should a risk assessor communicate the results of a risk assessment to?
- A. All senior executives
 - B. Senior executives and designated senior managers
 - C. The board of directors only
 - D. Only those personnel who have been formally designated and approved to receive the information by senior management
19. Which of the following should be updated after a risk assessment, especially if and when risk conditions change? (Choose two.)
- A. Risk management strategy
 - B. Risk register
 - C. Risk profiles
 - D. Asset documentation

20. When performing a control analysis, which of the following is the main concern?
- How much control costs to maintain
 - If the control could be replaced or reduced
 - How effective a control is at providing protection for an asset
 - How many personnel it takes to support the control

Answers

- C. Risk identification is the first step in risk management.
- B. “Identify vulnerabilities and predisposing conditions” comes immediately after “Identify threat sources and events” in the NIST assessment guidance.
- A, B. Likelihood and impact are the primary factors focused on during the risk evaluation stage of risk management.
- D. Qualitative techniques use subjective terms, such as High, Medium, and Low, for their evaluations.
- D. Annualized loss expectancy (ALE) is a product of the single loss expectancy (SLE) and the annualized rate of occurrence (ARO).
- C. \$5,000 is correct, given $\$20,000 \text{ (AV)} \times 0.5 \text{ (EF)} = \$10,000 \text{ (SLE)}$ and $\$10,000 \text{ (SLE)} \times 0.5 \text{ (ARO)} = \$5,000 \text{ (ALE)}$. Note that the ARO is expressed as an *annual* value, although the scenario in this question states that the negative event occurs once every *two* years, instead of per year.
- C. The original OCTAVE uses teams performing in workshops and was designed for large organizations with more than 300 employees.
- B. RE2, “Analyze risk,” is the process step used for risk analysis in the Risk IT Framework.
- B. Interviews are by far the most subjective data collection method since people may offer opinion or mistaken or false information.
- D. Directly observing the system in operation, including examining the permissions on sensitive system files, would be one way to confirm the system administrator’s claim.
- A. Existing controls must be examined to determine how well they reduce likelihood or impact to a system in the event a threat actually occurs.
- C. Fault-tree analysis focuses on an event and all of its potential causes.
- C. ISO/IEC 31010 primarily focuses on risk assessment processes and methodologies.
- D. The difference between the level at which a control is currently functioning and its desired level is the control gap.
- A. A common controls provider is responsible for controls that aren’t specific to a particular asset but are used across the organization for various assets and systems to provide general protection.

16. **B.** Residual risk levels should fall within acceptable ranges, given the organization's risk appetite and tolerance levels.
17. **D.** The one important point to convey when communicating the results of a risk assessment to senior managers and executives is how IT risk impacts business processes and the business operations of the organization.
18. **D.** Only approved personnel should receive information regarding the risk assessment results since it is sensitive information.
19. **B, C.** Both risk registers and risk profiles should be updated after the assessment since changing risk affects the current risk posture of the organization.
20. **C.** During control analysis, the primary concern is how well the control provides protections for an asset, reducing the likelihood of a threat occurring or reducing the impact to the asset if a threat does occur.

Risk Response and Mitigation

In this chapter, you will:

- Learn about the risk response process
- Understand risk response options and how to align choices with business objectives
- Become familiar with risk response standards and frameworks
- Understand how risk appetite and tolerance affect risk response choices
- Understand risk response action plans and how they are developed
- Understand how controls are designed, implemented, and executed
- Develop better project management skills to more effectively execute risk response plans
- Learn methods to document and assess risk responses
- Determine how to best train personnel on risk responses

In this chapter, we will review the concepts that comprise Certified in Risk and Information Systems Control (CRISC) Domain 3, which is focused on risk response and mitigation. There is a natural progression from the risk assessment discussions in previous chapters that covered CRISC Domains 1 and 2, to the discussion on risk response in this chapter; you will see that many of the outputs from those processes lead directly to this chapter because an organization generally wants a positive response to any risk assessment findings. After discussing how risk responses are chosen, we will discuss how to implement those risk responses, including how to design, develop, and adjust controls.

The CRISC exam objectives covered during this chapter include the following task statements:

- 3.1 Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions
- 3.2 Consult with, or assist, risk owners on the development of risk action plans to ensure that the plans include key elements (e.g., response, cost, target date)

- 3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level
- 3.4 Ensure that control ownership is assigned to establish clear lines of accountability
- 3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution
- 3.6 Update the risk register to reflect changes in risk and management's risk response
- 3.7 Validate that risk responses have been executed according to the risk action plans

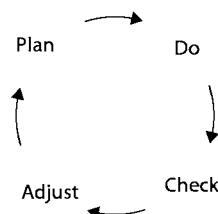
Risk Response

Every organization has risk. The leaders of smart organizations, however, have determined how they will deal with that risk appropriately for their business context. Will they accept all risks? Will they transfer some risks to a third party, such as an insurance company? These are some questions that need to be considered within the risk response process, discussed in this chapter.

We will also discuss the major risk frameworks within the field and how they incorporate risk response determination and implementation. Please note that risk is different for every organization; risk within an educational context is different from a financial context, which is different from a government context. Also keep in mind that IT risks are different from business or mission-oriented risks. It's important to note that the mission of the organization helps to shape risks and responses as well. This is why it's so important that organizations conduct a thorough risk analysis and understand and prioritize the response options that are right for them. You should also remember that the risks to the business, the business goals and objectives, and the systems supporting those functions should all be considered throughout the risk response process. It's easy as an IT professional to forget that the business objectives are the top priority, but to maximize efficiency and effectiveness (and especially to pass the exam), you should keep that in mind.

It's a good idea to think about this risk response action plan in a Plan-Do-Check-Adjust (PDCA) life cycle, as shown in Figure 5-1. The PDCA model (often referred to as the Plan-Do-Check-Act or Deming cycle) promotes continuous improvement.

Figure 5-1
Plan-Do-Check-
Adjust cycle



In this case, you are planning (designing), doing (implementing), checking (assessing), and adjusting (adjusting and creating documentation) the quality controls that will respond to risk.

Risk Response Standards and Frameworks

Standards and frameworks help provide a standardized, industry-accepted approach toward managing risk. While they're certainly not perfect, they provide a baseline for an organization to recognize the key steps toward understanding and categorizing the risks to their business, implementing the appropriate security controls to lower risk to an acceptable level, and continually monitoring the residual risk and report status to the management. Each standard and framework has its own pluses and minuses, and we will discuss three of the most commonly used: the National Institute of Standards and Technology (NIST) Risk Management Framework, the ISACA Risk IT Framework, and the ISACA Control Objectives for Information and Related Technology (COBIT). Keep in mind that while we discussed these three frameworks in Chapter 1, our discussion there served only to introduce you to the frameworks. In this chapter, you will look at them from the perspective of risk response in particular.



NOTE You can find more general information on standards, frameworks, and best practices (and the differences between the three) in Chapter 1.

NIST Risk Management Framework

NIST Special Publication 800-37, revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems,” along with other supporting publications from NIST (part of the U.S. Department of Commerce), makes up the defining volumes of the Risk Management Framework (RMF). The RMF is comprised of six steps, as shown in Figure 5-2.

1. Categorize information systems.
2. Select security controls.
3. Implement security controls.
4. Assess security controls.
5. Authorize information systems.
6. Monitor security controls.

Security categorization requires the information systems and associated information to be categorized based on an impact analysis. When selecting a set of security controls, the security categorization, as well as any previous assessments of risk, must be taken into account. Following this step, you implement the security controls that were previously selected and then assess their effectiveness and the overall success of the controls of lowering the risk to the accepted level. Finally, the security controls need to be continually

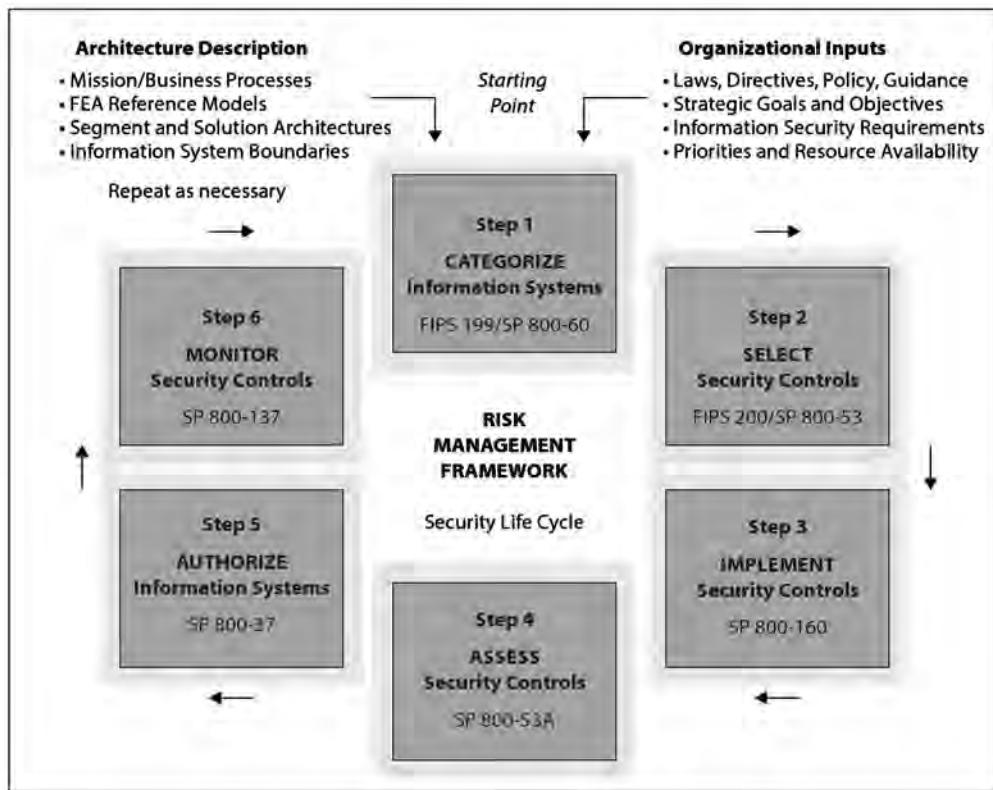


Figure 5-2 The NIST Risk Management Framework (courtesy of NIST, from Special Publication 800-53, revision 4)

monitored to be sure they continue to operate as intended, as well as considering any changes that come into effect across the organization (think location, mission, security classification, or other underlying factors).

You will notice many additional concepts within NIST Special Publication 800-37 that are germane to the CRISC exam; for example, the first two steps of the RMF discuss categorizing and selecting appropriate security controls (which we will discuss later in this chapter), while steps 3, 4, and 6 map cleanly to the implementation, assessment, and continuous monitoring of controls (covered throughout this book). For these reasons alone, it's a great idea to read this document to understand how the steps work together and how they are similar to (and sometimes different from) other frameworks.

From a response perspective, the key point that you need to understand about the NIST RMF, and what makes it so revolutionary within the Department of Defense (DoD) and associated organizations, is that risk response starts with steps 4 and 5 of the RMF. This is where authorizing the system (based upon the responsible authority's

acceptance of risk levels) and continuous monitoring take place. Continuous monitoring within the RMF context means near-real-time risk management through the implementation of a comprehensive set of controls that provide an up-to-date status of the current security posture of the organization. To achieve these ends, the RMF encourages automated mechanisms (such as Tenable Security Center and the McAfee Host-Based Security System, for example) to be implemented to support rapid analysis and reporting to management, and for organizations under the mandate of the standard, the RMF establishes a level of accountability and responsibility for the controls selected and implemented within supporting information systems.

Risk response is also covered in NIST Special Publication 800-39, “Managing Information Security Risk,” and the different response options are discussed in Chapter 3 of that publication. They include risk acceptance, transfer, avoidance, sharing, and so forth, which make it a great reference document. They are similar to what the next framework, the ISACA Risk IT Framework, discusses in terms of risk response. We’ll discuss the risk response options in more depth later in this chapter.

ISACA Risk IT Framework

Published in 2009, the ISACA Risk IT Framework is another common risk management framework that you should be aware of. ISACA looked to create a framework that merges the traditional IT models with a more risk-focused mind-set. Within the ISACA model, the activities considered key are grouped into processes, which are grouped into three domains, as described in Table 5-1.

There are three main domains to consider within the ISACA Risk IT Framework: Risk Governance, Risk Evaluation, and Risk Response. You will see many of the same concepts that you’ll find within this book (and even this chapter), so it’s definitely a worthwhile model to review. The Risk Governance domain discusses risk appetite, risk tolerance, and communicating risk to leadership (this should sound familiar!). The Risk

Domain Name	ISACA Description	Associated Processes
Risk Governance	Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return	Integrate with Enterprise Resource Management, Make Risk-Aware Business Decisions, Establish and Maintain a Common Risk View
Risk Evaluation	Ensure that IT-related risks and opportunities are identified, analyzed, and presented in business terms	Analyze Risk, Maintain Risk Profile, Collect Data
Risk Response	Ensure that IT-related risk issues, opportunities, and events are addressed in a cost-effective manner and in line with business priorities	Manage Risk, React to Events, Articulate Risk

Table 5-1 Domains and Associated Processes Within the ISACA Risk IT Framework

Evaluation domain includes an understanding of the impacts to the business and the risk scenarios, developed through the inclusion of internal and external environmental factors, risk management capability, IT capability, and IT-related business capability.

Since we've already given you a general overview of the other domains of this framework in Chapter 1, we'll focus on risk response in particular here. The Risk Response domain covers the risk response definition, risk response prioritization, and key risk indicators (KRIs). KRIs are those that show a potential for risk that is beyond the organization's risk appetite level, and we will cover them in much more depth in Chapter 6. The framework also describes risk response options such as risk avoidance, risk mitigation, risk sharing and transfer, and risk acceptance. If these sound familiar to you, they are the same options described in NIST, as we mentioned earlier. Again, we'll go into depth on them later in the chapter.



TIP Understand the relationships between the Risk Governance, Risk Evaluation, and Risk Response domains; even though the Risk IT Framework is not covered on the CRISC exam, the framework provides a useful foundation of the concepts.

You'll see many areas of similarity between the ISACA Risk IT Framework and the CRISC exam, so it definitely wouldn't hurt to include it in your study plan.

COBIT

While ISACA's COBIT doesn't focus solely on risk, it's still important for you to have a cursory understanding of the framework and its supporting processes, inputs and outputs, and activities. Again, ISACA authored both the CRISC and COBIT frameworks, so you will see many of the same concepts interwoven across the two (as well as within the Risk IT Framework discussed previously, which is quite complementary and often grouped with the other two).

To refresh your memory, COBIT was designed to help businesses take advantage of IT assets, increase compliance levels, and manage risk through an integrated framework. This framework includes processes that have general inputs and outputs, objectives and activities, and associated measures. The most recent version, COBIT 5, was released in 2012, with two updates published in late 2012 and 2013, respectively covering information security and assurance. This should tip you off to the fact that while many IT professionals are familiar with the COBIT framework, it is not meant to be IT-centric or IT security-centric and was developed with organizational governance in mind as its primary goal. Within COBIT, the activities considered key are grouped into domains, which are broken down into processes, as described in Table 5-2.

The COBIT processes associated with risk response are Monitor and Evaluate and are used to ensure that risk response options are implemented and are consistent with the organization's desired strategy for dealing with risk. Remember that with COBIT, we are talking governance, so this supports the governance perspective more so than an IT risk perspective. These processes could be used to fulfill governance and regulatory requirements with regard to risk response.

Domain Name	ISACA Description	Associated Processes
Plan and Organize	Provides direction to solution delivery and service delivery	Define strategic plans, manage quality control
Acquire and Implement	Provides the solutions and passes them to be turned into services	Identify areas for automation, implement change management
Deliver and Support	Receives the solutions and makes them usable for end users	Define service levels, identify costs
Monitor and Evaluate	Monitors all processes to ensure that the direction provided is followed	Ensure compliance with regulations, monitor and assess IT performance

Table 5-2 Domains and Associated Processes Within the ISACA COBIT Framework

Understanding Risk Response Options

Having developed your understanding of risk, you should also develop an understanding of the corresponding risk response options. These options will help you bring your risk levels down to that vaunted level of risk tolerance that your organization can accept. Within this section, consider how you would recommend that your organization respond to risk effectively but with a balanced approach.

Evaluating Risk Response Options

Avoidance, mitigation, sharing, and acceptance are all valid options that you should consider using (sometimes at the same time) to lower the risk level you face. The key is to use these options together; you want to balance risk and reward to maximize the benefits. These benefits can be financial or some other, perhaps difficult to quantify (for example, morale, partnerships, long-term strategy), benefit. We'll discuss the different risk response options in the next few sections.

Risk Mitigation

Risk mitigation generally involves the application of controls that lower the overall level of risk by reducing the vulnerability, likelihood of the threat exploit, or impact to the asset if the risk were to be realized. Mitigation actions come in a number of forms; a policy requiring nightly off-site backups of critical data can mitigate the risk of data loss, for instance. Similarly, applying a newly released web browser patch can mitigate the risk of exploitation. The goal is to get the risk down to a level considered acceptable by the organization's leadership. For the CRISC exam, you need to understand four main types of controls: managerial, technical, operational, and preparedness. The following are examples of each.

Managerial

- Requiring an acceptable use policy to dictate IT usage within the organization
- Starting a risk management program to identify, lower, and monitor unacceptable risk levels within the organization

Technical

- Implementing additional firewalls to protect internal (non-public-facing) systems
- Adding 802.1X port-based network access control to deter unapproved assets being added to the network
- Installing an intrusion detection system/intrusion prevention system (IDS/IPS) to monitor for malicious activities or violations of policy

Operational

- Implementing delegation/separation of duties procedures to assure that one person does not have the sole control over key duties
- Mandating security training and certification requirements to increase the baseline knowledge of IT security-related issues and concepts

Preparedness

- Executing a tabletop exercise of the Continuity of Operations Plan to test its effectiveness and identify gaps that should be addressed



TIP Remember that you're looking for low-cost, high-reward solutions to offset risk. Sometimes this is just a plan you implement or a process improvement, rather than an expensive piece of hardware!

Risk Sharing

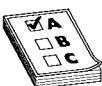
Risk sharing (often referred to as *risk transference*) entails the use of a third party to offset part of the risk. Risk sharing can involve the outsourcing of some activities to a third party to reduce the financial impacts of a risk event in many cases. Sharing off-site (co-location) assets and contractual obligations with other entities is one way that organizations implement risk sharing; a cloud service provider can be used within this scenario. The cloud provider might be contractually obligated to assume part of the financial impact in the event of a breach, but be aware that there is a potential loss of brand goodwill or other intangible assets that can be difficult to offload. Another example of risk sharing is the use of an insurance service to cover the financial impacts (at least partially) of a breach; however, the intangible losses mentioned previously would still be present.



EXAM TIP Don't forget that use of a risk-sharing scheme does not totally absolve an organization of its responsibilities; there may still be legal liabilities involved.

Risk Acceptance

There will always be some level of residual risk, no matter how many controls you implement or the amount of insurance you purchase. Again, the goal is to get the risk down to a level considered acceptable by the leadership. Risk acceptance occurs when the active decision is made to assume the risk (either inherent or residual) and take no further action to reduce it. The word *active* is critical here; risk acceptance is different from being risk ignorant in that the risk is identified, alternatives are considered, and a conscious decision is made to accept it. A good example of this is when a person intentionally drives alone in the carpool lane during the hours where multiple people are required to be in the vehicle; if that person is pulled over and ticketed for their lawlessness, that would incur a financial impact. However, they knowingly took the risk of this action, understanding the consequences if caught and accepting it anyway. Similarly, a company might choose to willfully ignore government-mandated control implementation that would incur fines or other financial penalties, assuming that the financial cost incurred would be less than the controls would be to implement. Another common situation is an organization choosing to work in a developing country, knowing there is a high level of risk; the financial rewards of being adopted early could outweigh any potential losses.



EXAM TIP It's important to note that risk acceptance doesn't insinuate ignorance; it's an active acknowledgment and conscious decision to accept risk as it is.

Risk Avoidance

Risk can be avoided through a number of methods. Can you remove the source of risk by making a different choice? Perhaps you don't need to conduct the activity at all. Avoiding risk can mean anything from eliminating risk associated with a particular activity through the careful analysis of risks and subsequent changes to a plan to the complete avoidance of a risk by not performing a planned activity. Risk avoidance is the option taken when, after controls have been considered, the level of risk is still not acceptable. An organization might choose not to take on a proposed project because of the probability of failure and subsequent loss of capital, for example. Another scenario might be the organization choosing to not adopt a cloud solution because of the level of sensitivity of information that would be stored within the cloud.

Selecting Risk Response

Selecting a risk response entails more than just blind luck or uncanny good fortune. In selecting a risk response, you should consider all of the factors we've discussed previously, such as cost (both of the response and of the potential cost of not responding), organizational context and associated missions, risk tolerance, and the simple ease of implementation. Within this section we will discuss some of these considerations and how they should affect your final decision.

Risk Response Parameters

Cost is obviously a large factor in response determination. When you think about cost, think about not only the financial impacts of any decision but also the less easily quantified aspects such as loss of goodwill, loss of brand status, and other hard-to-define attributes. You also need to consider the cost to maintain the responsive mitigation over its required life span. For example, if you are required to apply a costly IT solution into your architecture to load balance and you don't have an IT professional who is skilled or knowledgeable in that area, you may be required to hire a new professional or train an existing staff member. That also brings up your ability to plan for contingencies; is one person enough to complete this task? You may need more personnel in general to maintain your new security posture or to cross-train existing personnel as an alternative to hiring new people. Maintenance is a huge consideration that should not be shrugged off.

The ability (also defined as *capability*) for the organization to implement the response should also be considered. How mature is your company's ability to implement the response? Do you have a small, untrained, ad hoc team (perhaps that sounds cynical, but it happens)? In that case, a more sophisticated measure might not be appropriate; perhaps you need a new team! In contrast, a sharp, well-trained, experienced team can handle more complicated mitigation measures and processes.

How effective will the response be? *Effectiveness* can be measured as the extent to which the response reduces the likelihood or the impact of the risk event to the organization. If the effectiveness of the response activity is in question, that's a strong reason to consider that path questionable as well. You should also consider the efficiency of a response. *Efficiency* can be described as the ability for a risk response to cover one or more objectives that our organization sets in front of them. Quite simply, solutions are more efficient if they lower more risks than if they lower only one risk. Consider low-cost, highly effective solutions your "nirvana" and work from there. You want to obviously avoid high-cost, ineffective solutions, but it's shocking how often you will encounter them!

We will talk about prioritizing risk responses in the following section, and these concepts go hand-in-hand.

Prioritizing Risk Responses

Now that you have a better understanding of what your risk response options are and how you will select them, you need to understand how they should be prioritized. Have you ever worked for a company that had too much money to spend on its security program? (Here's a hint... we haven't.) It's unlikely that you'll have the resources to complete all of your proposed risk mitigation and response strategies, so knowing the proper priority is important. This will drive how you spend the money and apply the human resources that will lower your overall risk to an acceptable level. Figure 5-3 depicts the rankings of how you'd generally prioritize risk response options, and we'll discuss that ranking in more depth within the next section.

Figure 5-3
Prioritizing risk response options



Risk Response Prioritization Options

There are three prioritization options that you need to be aware of for the CRISC exam. They are *quick wins*, *business cases*, and *deferrals*. We will discuss each of these in this section and provide examples of both the options and the alternatives.

Quick wins are actions that can be taken that really are winners; as we discussed earlier, you are looking to select risk responses that are high reward and low cost and that are both effective and efficient. Quick wins are just that; they meet those criteria and address a medium to high risk and look good doing it! You should always be looking for a quick win to address a scenario, though that's easier said than done. Consider a scenario where an organization is having difficulties maintaining source code integrity across multiple teams of software developers. The developers are overwriting each other's work and causing havoc with old or untested code being pushed into production. It's a nightmare but one that happens regularly! An example of a quick win is the development of a configuration management board that immediately begins discussing and making decisions on source code changes and cross-pollinating projects among teams. The team might exist happily on its own, or the team might look at incorporating source code control software to force a developer to "check in" and "check out" software before it's changed. This facilitates logging and improves the ability to track and roll back from catastrophic implementations. A quick win is almost obvious in nature; why wouldn't you want to take advantage of it?

In contrast, making a business case is more difficult than pitching a quick win. A business case for a particular risk response must be made if the response can't be quickly or easily implemented without a significant cost or change to the organization or the system. These changes might include processes, infrastructure, architecture, or design, and they are significant enough to warrant a business case to respond to a risk issue. A business case for a risk response justifies the expense and work required to make the response function properly. When you make a business case for a risk response, you must take a number of factors into account. For example, what projects are currently in the pipeline? Is there something that would conflict with your proposed response option, make it irrelevant, or make it more costly? How's the business doing? If the bottom line is weak, it will be harder to sell any risk response solution that is costly, even if

it would significantly improve the baseline level of risk. When a business case needs to be made, generally the risk response option is more costly in general, whether it is costly in terms of financial or personnel resources. It also might be attempting to address a low or medium risk that doesn't have the attention of the leadership in the way a high risk would. Even an efficient and effective response to a low risk must be questioned and prioritized appropriately.

Finally, you choose to defer when risk response options simply don't make good business sense. A deferral is the polar opposite of the quick win; whereas a quick win is almost obvious in its ability to address a medium or high risk in an efficient and effective way, a deferral is the choice when you have a high cost of response associated with a low risk, one where even a business case can't be made. In the scheme of prioritization, deferrals will be at the bottom of the list. We choose to accept risk, perhaps until the cost is reduced, or choose risk acceptance as our permanent measure.

At the end of the day, your prioritization should take into account a number of concerns. These include the regulatory mandates that are applicable to your organization, the impact to the business through implementation of the proposed measure (including costs both financial and nonfinancial), the market conditions you find yourself in, the culture and the climate of the organization (including the inherent resistance to change), and the ability to optimize resources.



EXAM TIP Always remember that low-cost responses to high-risk scenarios are the goal of risk response prioritization.

Identifying Business Opportunities

Businesses of all types and markets are looking to create business opportunities. With opportunities, however, comes risk. Risk is not always a bad thing; in some cases, it allows you to get out ahead of your competitors and capitalize on forward-thinking ideas that may be out of your comfort zone. An example that we'll use frequently is a business looking to move into a developing country; the risk is high, but the reward could also be great. We'll identify these opportunities here and explore how they can be leveraged.

Identifying business opportunities during the selection of risk responses requires the organization to understand its risk appetite and risk tolerance. As we discussed in Chapter 1, risk appetite is how much risk an organization is willing to deal with in any given endeavor, while risk tolerance is the acceptable level of deviation in risk for a particular endeavor or business pursuit. Remember, there's a certain amount of risk in every business enterprise or pursuit, but the organization may not be able or willing to tolerate large deviations from what it considers its acceptable level of risk on an endeavor. The selection of risk responses will inevitably change the risk appetite/risk tolerance calculation within the organization, and any risk response should be examined against these guiding factors.

When the organization is able and willing to take a risk, it can be considered a business opportunity, and to identify those opportunities, you need to understand the areas that can withstand the risks. Cloud computing is a great example of an opportunity that

many organizations consider worth the risk based on the rewards; operating within a difficult business area such as a developing country is another we discussed previously. In the end, to identify business opportunities, remember to look for areas of opportunities that can be leveraged through the creation of a competitive advantage or increased synthesis of activities and processes.

Risk Mitigation

Hooray! You've selected your risk responses carefully and prioritized them appropriately. You're feeling good about how you're going to positively capitalize on good risk and minimize bad risk, and you're going to do it efficiently and effectively. You're a risk response rock star! Alas, now comes another challenge: implementing those risk response options. In this section, we will talk a bit about how controls are implemented, as well as the concepts of exception management and residual risk. Even the best-laid risk response plan will need to account for these concepts.

Have you ever seen a manager act with a knee-jerk reaction to a sudden problem that ends up costing more time and money implementing a solution than the actual issue itself would have? Implementing risk responses properly should consider a few key components, such as the ability to measure its success, proper documentation, and appropriate training.

Earlier, we discussed a number of different risk response options, such as risk avoidance, risk sharing (or transference), and risk acceptance. In this chapter, we will focus on risk mitigation. Risk mitigation incorporates *controls* of varying types across an enterprise to lower risks to an appropriate level. These controls can be anything from a written document to a sophisticated, comprehensive technical solution, but they should all be designed to most effectively and efficiently mitigate the risk they are associated with. At the end of the day, control should provide the organization with some level of assurance that they can meet their business objectives and deal with any events that occur in a manner that is acceptable to the leadership of the organization.

Risk Response Action Plans

Quite simply, the risk response action plan lists the risk responses that have been chosen and charts their progress and associated timeline, with an appropriate action owner. This ownership piece is critical because you need a "belly button" to push if things are not going as quickly or as smoothly as they should be. Without a proper risk response action plan, you will likely end up losing sight of where your risk responses are in their progress, if they've made any progress at all. Risk response action plans can contain any number of data points inside of them, but at a minimum, they should list the prioritized risk responses, their associated costs, a timeline for their implementation, the associated cost, and the owner of the risk response. The plan should be formally accepted by senior leadership, monitored continuously, and reviewed at regular intervals to ensure it does not deviate from a risk or response perspective. Any deviation should be reported immediately to the senior leadership.

Control Development

So, what is a control anyway? Quite simply, a control is some sort of measure, be it a document, a technical solution, a procedure, or some other remediation that is put into place to improve the overall security posture of your organization through correcting a gap or making up for a shortfall in another control. Controls can be technical solutions, such as firewalls or intrusion detection systems, but they can also be processes, procedures, policies, or physical controls. We talked in Chapter 1 about the types of controls (administrative/managerial, technical/logical, and physical/operational), but controls also can be grouped in different families: access control, auditing, configuration management, contingency planning, personnel security, and so on. So, how do you determine new controls to apply to your system or whether your existing controls are good enough? We will discuss this in more depth in the following sections.

Control Types

As you may have gathered by now, there are many types of controls to choose from. However, you can generally group these controls into a number of broad categories by their intended function; the most common are compensating, corrective, detective, deterrent, directive, and preventative. You may notice some significant overlap between these categories, and that is why some experts do not distinguish between, for example, deterrent controls and preventative controls. Table 5-3 lists each control type, its definition, and an example control.

Control Function	Definition	Control Example
Compensating controls	Compensates for weaknesses or inherent flaws within other controls or a lack of controls	Regular third-party review of logs based on an inability to enable proper separation of duties across system administrators
Corrective controls	Corrects a situation back to a “known-good” or improved state	Regularly rotated and tested backups of critical data to limit the time a critical database is offline
Detective controls	Detects and characterizes events or irregularities as or after they occur	External or internal audits conducted on an unscheduled, irregular basis
Deterrent controls	Deters and discourages an event from taking place	Cameras around the building, continuously monitored by personnel
Directive controls	Written direction for how security measures will be conducted within the organization	Policy requiring two-person opening of sensitive areas within the building
Preventative controls	Prevents events or irregularities from occurring	Laptops locked to desks to prevent them from being walked away with

Table 5-3 Controls Categorized by Function

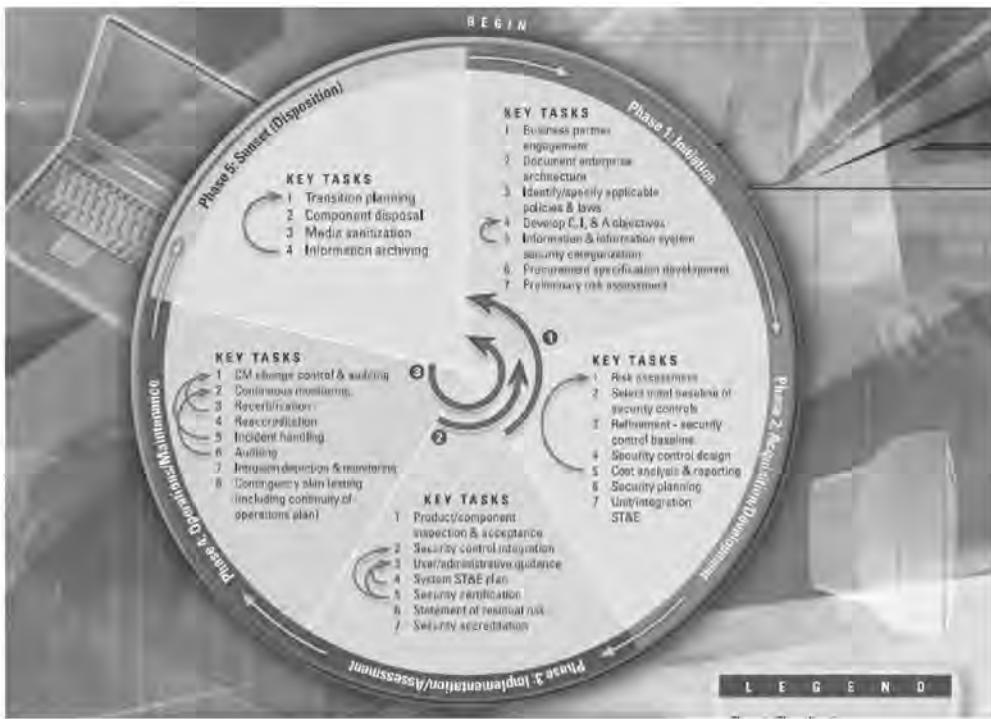


Figure 5-4 NIST 800-53 security controls identifiers and family names (courtesy of NIST, from Special Publication 800-53, revision 4)

NIST 800-53

NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” is a key catalog of controls to be aware of if you are doing business in the U.S. government but is also a great resource even if you’re not. With its latest revision (revision 4, as of this writing), it includes controls for assuring privacy as well as security and is meant to be policy and technology neutral, meaning that the controls are broad enough to be applied to any architecture. If you’re looking for a document to tell you the steps of how to configure your router securely, this isn’t the document for you; it’s perfect, though, if you’re looking for a comprehensive view of the scope and magnitude of a system-level control solution. Figure 5-4 lists the families of security controls and their unique identifiers from NIST 800-53.

ISO 27002

While NIST 800-53 is used heavily within the U.S. government, International Standards Organization (ISO) 27002 is used much more widely internationally. Much like 800-53, 27002 groups controls into families, such as the following:

- Human resource security
- Asset management

- Access control
- Cryptography
- Physical and environmental security
- Operation security
- Communication security
- System acquisition, development, and maintenance
- Supplier relationships
- Incident management
- Business continuity management

Since its birth, versions of 27002 specific to different industries, such as healthcare, have been developed that are tailored to their specific contexts, laws, and regulations.

Designing Effective Controls

The first step in designing an effective control is to determine who exactly owns the control; this is key because it will determine who actually designs the control, who tracks its care and feeding, and who creates the documentation that will follow the control well into its implementation and eventual disposition. This individual or group should be the party responsible for determining the security categorization (SC) of the system or environment into which the control will be applied. NIST 800-53 recommends the determination of the SC of an information system as an equation, as described here:

$SC = \{(confidentiality, impact), (integrity, impact), (availability, impact)\}$, where the acceptable values for potential impact are low, moderate, or high

Using this equation, a low-impact system would need to have most or all the confidentiality, integrity, and availability (CIA) elements with a low impact; a moderate-impact system would have a mixture of low and moderate and potentially high elements; and a high-impact system would have most or all of the CIA elements with a high impact. Note that higher-impact systems will usually have more controls applied to them, reflecting their higher sensitivity and criticality within the organization, and these controls will normally be applied with a higher degree of effort or rigor. It is important to understand the SC because it will help you determine how much money, time, and other resources you want to devote to any particular control. As discussed earlier, you are looking for low-risk, high-reward controls. Understanding the impact of the system allows you to plan and design more cost-effective controls.

After determining your security category, you will want to understand the *common controls*. These are controls that are common across your organization and are shared between more than one information system. For example, you may have more than one information system being housed within the same server room in your headquarters building. Perhaps a previously accredited system review already ensured that you have a strong lock and a heavy door between those servers and the rest of the world. This would be a common control between the old system and your new system. Other possibilities

could be continuity of operations, policies, and procedures; guards at entrances; biometrics; and so on. These should have already been documented in a plan (we hope!), so a great place to start is to review the security plans for other systems within your organization. Don't forget the advent of the cloud has created situations where you are sharing data and systems among more than one organization, often supported by another third-party organization, so you may have common controls among all of your organizations that need to be considered. Also, be constantly aware that any common controls that do not meet your specific requirements (let's say there's a strong door but no lock) will require you to add a compensating control to meet your standards.

Selecting the appropriate controls for you and developing them often depend on your context (for example, government, healthcare, banking, or some other specific context that mandates a certain regulatory or legal standard for your security). Further, you already developed your security category, as discussed earlier, so you know the impact of the system if it was lost for a period of time. After determining the common controls, you now know where the gaps between the two points are. Now is the time to begin documenting those gaps in the risk response action plan. Don't forget, if you are dealing with a third party or cloud-based provider, you should also be considering any service level agreements or other legal documentation that will need to be drawn up as part of your risk response action plan.

Control Implementation and Adjustment

Now that you've selected the appropriate controls for your system, it's time to implement them. You have unlimited time, money, and personnel available, so this shouldn't be an issue, right? In a perfect world, that would be the case; however, we all know that we have to deal with constraints on a daily basis, so we will discuss how to deal with control implementation as a project using project management tools later in this chapter.

This is a great time also to consider any current or future technology knowledge that you may want in your organization. Are the areas you are applying controls to grossly out of date? Or are they stable and still widely used, causing your leadership to have an "if it ain't broke, don't fix it" approach to phasing them out? Consider how you could enable change in the organization through implementing new technologies. This could be anything from upgrading your core network infrastructure to implementing biometrics at critical entry points.

Don't forget to do a thorough review of your existing controls that are in place and how they may need to be adjusted. This will need to be factored into your project plan, both for time and for resources.

Risk Response Assessment

Security controls should be tested before the system is authorized or credited and at irregular intervals afterward. You *assess* a program or a project to determine whether it is meeting your specified objectives and to determine whether the controls you have selected to protect the system are performing their desired function to the level you need them to. Conducting an assessment early in the life cycle of control implementation allows for issues with the control to be determined and remediated as appropriate. Based on the rules and regulations that your organization must adhere to, you may be able to

do an internal audit of your controls, or you may be required to use a third-party agency or other testing authority. Either way, be mindful that an assessment should be thorough, technical (as appropriate), and independent. Anyone conducting an assessment should be impartial, as free of bias as possible, and preferably not in the same part of the organization as the personnel charged with implementing the controls. You will often see two types of testing discussed within the community; developmental testing/evaluation is conducted in parallel with the development of a system (or in this case the controls for the system), and operational testing/evaluation is conducted before the system is released into final production (or operation). While both types of testing are required in some segments (such as major government systems), some organizations that do not require developmental testing and evaluation fail to get elected, to their own peril. Quite simply, the time and money spent to assess iteratively along the life cycle of the project will save you dividends in the end. Just imagine the headache you will have if you find out that a major control you were betting on to reduce the risk of external breaches does not play well with your network infrastructure. You would have found that out much earlier if testing occurred sooner. Either way, you should have an assessor, inspector, agent, or other authority assigned to assess your system to detail any flaws found and allow you to better fill the gaps.

So, what exactly occurs during control assessment? If you are using a formal set of controls, such as the NIST framework discussed throughout this chapter, you can expect each family of controls to be decomposed into specific requirements that can be assessed in a variety of ways. For example, if continuity of operations is one of the controls you have implemented, you could expect a review of your continuity of operations documentation, a visit to your off-site facility (as appropriate), and perhaps even a test of your backup solution. Another example is the door and lock combination that we discussed previously in this chapter; any assessor worth his or her salt will be checking to make sure you have a lock on all doors but that they are also adequate to meet the requirements to lower your organization's risk posture. There will be a mixture of documentation review, technical assessments, and interviews that are conducted to determine whether you have adequately covered all the controls required. Table 5-4 lists some common assessment techniques. If you've done your due diligence in preparing for an assessment (through adequate documentation, thorough implementation, and appropriate analysis of the actual controls required), this should be no sweat. However, if formal assessment is required for an authorization or accreditation action and you did not diligently pursue these activities, you could be in for a major headache when you receive your results.

Ever thorough, NIST has a guide to security assessment that aligns well with its other documents covering risk management. NIST Special Publication 800-115, "Technical Guide to Information Security Testing And Assessment," was written with four points of focus: helping organizations establish an information security assessment policy, implementing a repeatable and documented assessment methodology, determining the objectives of the security assessment, and analyzing the findings and developing risk mitigation techniques to address weaknesses.

Documentation Review	Technical Assessment	Physical Assessment	Interviews
Backup and restoration procedures	Source code review	Check for working locks on doors	System administrators
Disaster recovery plan	Wireless scans	Examine and test fire extinguishers	IT security staff
Rotation of duties policy	Network sniffing	Review sensitive area access control logs	Senior leaders
Employee training and awareness documentation	System configuration review	Review security guard procedures	Users
Privileged user agreements	Log review	Review video surveillance tapes	Developers

Table 5-4 Control Assessment Options

An alternative to the NIST framework is the Open-Source Security Testing Methodology Manual (OSSTMM) from the Institute for Security and Open Methodologies (ISECOM). Currently in its fourth revision, the goal of the OSSTMM is to create a standard for thorough and practical security testing across the community with the following goals:

- Quantifiable
- Consistent and repeatable
- Valid beyond the “now” timeframe
- Thorough
- Compliant to individual and local laws and the human right to privacy

Even if you do not intend to use the OSSTMM framework, it is a useful reference document that contains handy rules of thumb for gauging testing time and sample rules of engagement.

Documentation

Risk response options must also be thoroughly documented, with a clear owner defined, whether it is a new process, control, team, policy, or any other solution. Just imagine a risk being uncovered that requires a set of procedures for storing, handling, and destroying sensitive information. The procedures are developed and put on a shelf until an incident occurs. In the meantime, the procedures go stale (locations change, for example), and no clear owner was defined to be responsible for maintaining the documentation. The procedures, in this event, are as good as useless. Substitute any situation where documentation is not only helpful but necessary, and you can quickly see why this is so important.

By this point, you've no doubt made a number of changes to your organizational security posture, and these changes should be documented within your security plan. You should write security plans assuming that the personnel who are currently active within your organization could leave at any time (the old story about someone being hit by a bus and was the only one who knew how to perform a specific function), so it's best to always prepare for contingencies such as this by having your security plan as heavily documented as possible. You need to make sure to include a functional description of all controls that were applied to the system, any decisions that were made leading to these controls being implemented, any interdependencies, and any other relevant information. Finally, you also want to include any documentation from testing that occurred and remediations that were made based on testing results.

Any risk response planning should outline a rough timeline for implementation, a rough estimate of costs, who is responsible for the implementation, and any required tools (such as software, hardware, and so on) required to complete the tasks. More detail is always better! A lack of clarity is not your ally, especially if the plan is handed over to a team that wasn't involved in the initial planning process.

Finally, you'll want to track the status of your risk response implementation. This is usually done using a risk register, discussed previously in Chapter 3. To recap, the risk register is a document that tracks various elements of the identified risks, such as the risk name, risk impact, risk probability, risk mitigation, action owner, and action suspense date. This risk register can be used to track the implementation of the mitigations and assure that timelines are met.

Do you have any metrics in place that can determine the success of the risk response? Metrics help you quantify the effectiveness of your implemented risk response over its life. Monitoring comes into play here because it facilitates your ability to understand your performance against the metric. Monitoring can be done through a tool, through a team, or through a combination of both.

Exception Management

It's easy to say that your risk response options should always be implemented. You carefully considered the risks to the organization through the risk analysis process, selected appropriate responses, and monitored your risk levels diligently. How could you possibly not implement a control? That would be crazy! However, there are exceptions, and you need to have a process in place to manage those exceptions and keep them minimized. Consider the situation where an operating system patch cannot be applied because of a legacy application that's critical to the organization's mission. This mitigation is important but less important than the legacy application and its associated mission. What to do? *Exception management* comes into play here; you need to document this as an accepted exception to the policy and track it. Perhaps the patch can be implemented in the future, or another mitigation could come along and make the exception moot. This is another aspect of risk acceptance; you are asking management to accept an ongoing risk, as an exception, because the response cannot be implemented for whatever reason. Either way, keeping a close eye is key to not letting these exceptions slip through the cracks.



NOTE Don't forget to track exceptions and remove any that aren't valid! It's easy to let them slip through the cracks.

Reporting the Risk Response Activities

What are the reporting requirements for your organization? Are they bound by government regulations, international business partnerships, or other binding agreements? Understanding what is required of your organization is absolutely critical for your reporting requirements. You also need to understand what you should report in any of these contexts. For example, it is a good idea to report any issues you have ongoing, the status of any ongoing remediation actions, how your controls performed, any ongoing incidents, and how your overall risk response activities are performing, essentially the “Bottom Line, Up Front” of your risk response action plan.

Along with understanding the underlying operational environment, it is key to understand your stakeholders and what their needs are. For example, your board of directors might want a high-level, quarterly presentation on compliance levels relative to the previously discussed operational environment, as well as performance relative to business goals and objectives. The risk committee, conversely, might want a much more “deep dive” into the individual risks identified previously, the new risks that could potentially come to the forefront, and how different business units are supporting the risk management program across the entire organization. It’s important that you understand how these different stakeholders need different reporting mechanisms and tools and that you identify clearly (preferably in writing) how they expect you to support them through timely and relevant reporting.

When reporting, you can include a few standard items, such as measured control effectiveness (which can be rolled up to a higher level, as necessary, for management), any ongoing issues, any perceived gaps, the status of any remediation actions, any incidents or risk events that have occurred since the last report, and the overall trending status of the effectiveness of the risk management process. Also, identify ahead of time whether your report will be included as an input to a greater enterprise report and work to include any appropriate information needed to facilitate that enterprise-level view. This will help garner support for the risk program supporting the business goals and objectives.

You should review the results of any third-party analysis or audit that has taken place and incorporate the findings into your understanding of the organization’s risk posture. Has your organization conducted any type of internal audit or self-assessment? These will be important to review and to take a look at how they affect the risk profile and where they will need to be mapped. We’ll discuss the risk tolerance in many places throughout this book, so suffice it to say that the risk tolerance should be considered throughout the reporting process as a key input.



NOTE Chapter 1 has more information on the concept of risk tolerance and how it relates to risk acceptance.

Training

After all is said and done and the controls have been implemented and documented, it is important that you conduct regular and traceable training that covers a number of aspects. On top of the usual cyber security, privacy, and acceptable user training that most organizations (should) have in place, it is imperative that the employees responsible for the care and feeding of your controls are properly trained on both the content of the controls and the context of the controls. What does this mean? Content means that a network administrator in charge of your infrastructure, and the subsequent controls, understands the latest evolutions and revolutions in both current threats and vulnerabilities. Context means that the same network administrator in a highly sensitive government environment (think missiles, space, and so on) should know that they should be extra prudent and consider the limitations inherent to their systems and how they interact with other systems (if not the larger Internet). Without both of these, content and context, as part of the training portfolio for all personnel charged with implementation of controls, you may well likely find that one or the other is neglected.

System Development Life Cycle

There are many assorted control-related life cycles; some deal with systems, and some are more specific to software or other project types. In this section, we'll discuss a system development life cycle (SDLC), which is a generic framework used within NIST 800-64, "Security Considerations in the System Development Life Cycle." The NIST SDLC has five phases: initiation, acquisition/development, implementation/assessment, operations/maintenance, and sunset (otherwise known as disposition). Be on the lookout in this section at how well many of these particular steps align with the concepts covered previously. You should see how important it is that controls are developed and implemented within each phase of this life cycle. In fact, NIST states that "an integrated security component (composed of milestones, deliverables, control gates, and interdependencies) that specifically addresses risk management...enables security to be planned, acquired, built-in, and employed as an integral part of a project or system." Figure 5-5 depicts the SDLC covered in NIST 800-64.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Figure 5-5 NIST 800-64 System Development Life Cycle (courtesy of NIST, from Special Publication 800-64)

Initiation

In the initiation phase, the need for a system is determined, and its purpose is documented formally. Within the initiation phase, it is critical to consider your control development and integration early and often. In fact, you will save yourself many headaches, time, and eventually money by considering your controls at every step along the way. Within the initiation phase, security is often expressed as a business risk or a risk to project completion or the business itself. Outputs for the initiation phase could include the following:

- Documentation of security roles and responsibilities
- Documentation of controls required by regulation, law, or other guidance
- Schedule of control activities or decisions throughout the project timeline

Acquisition/Development

Within the acquisition/development phase, the risk assessment is often conducted, along with any security testing and development of documentation for system certification and accreditation (as required). Risk assessment is covered in-depth in Chapter 2, but just note that an effective risk assessment is built on the initiation phase having been conducted appropriately and thoroughly. This is also the phase where the bulk of your control development will occur.

Implementation/Assessment

Within the implementation/assessment phase, the system is installed in its new environment and evaluated for its readiness, both operational and security. Here you do a final certification and accreditation review, and the authorizing official or other accrediting authority will take responsibility for the security posture of the system. Any documentation to connect the system to any external entity should be completed within this phase. Outputs for the implementation/assessment phase could include the following:

- Accreditation package
- System authorization
- System security plan

Operations/Maintenance

Within the operations/maintenance phase of the SDLC, the system is actively operating, so you can leave it alone here, right? Not likely. You need to constantly be looking for ways to improve and enhance the system, and any improvements or enhancements need to be considered for their security ramifications. Furthermore, the system must be assessed periodically based on regulatory, legal, or other guidelines to ensure that it continues to maintain a risk level that aligns with the company's risk tolerance. Outputs for the operations/maintenance phase could include the following:

- Updated plans of actions and milestones
- Change control board documentation
- Renewed accreditation and authorization documentation

Sunset (Disposition)

Every good thing must come to an end, and systems are no exception. The final phase of the SDLC requires a system to be disposed of properly, and in doing this you need to be aware of the controls required for securely disposing of a system and any corresponding data or other artifacts. As NIST points out, there is usually not a definitive end to a system; it is often merely rolled into the next generation of systems, and any data and associated requirements become the province of that group of personnel tasked with the care and feeding of the new shiny solution. However, you do need to be aware that, if required, it is important to have an orderly and safe disposal process on hand that includes migration of data or archival solutions as appropriate. Outputs for the implementation/assessment phase could include the following:

- Logs of hardware and media sanitization/destruction
- Transition plan

Project Management

Risk responses should be implemented in a controlled, defined, and monitored manner as discussed previously. One tried-and-true way to do this is through the tenets of project management. The Project Management Body of Knowledge (PMBOK), a publication of the Project Management Institute, defines a project as “a temporary endeavor to create a unique product, service, or result.” Project management, then, is “the application of knowledge, skills, tools, and techniques to project activities to meet project requirements.” Note that a project in this context is indeed temporary in nature, with a defined beginning and end. Risk management is distinct from project management on this point because project management incorporates concepts to lower project risk but ends with the project, while risk management activities can continue indefinitely.

Project management is a great concept to know as a professional because it can be helpful in completing any set of tasks, but for the CRISC exam, you obviously need to keep your risk hat on. In this section, we will discuss the most common project management frameworks and the vital concepts you need to understand for the exam. We’re not advocating for a particular standard to be adopted; in fact, you’ll notice a great deal of similarity among all of the major frameworks. Most importantly, you need to understand that implementing controls is like any other project, in that, as the PMBOK states, it is “the application of knowledge, skills, tools, and techniques to project activities to meet project requirements.” The project activities are the activities you are conducting to meet the project requirement: a set of controls implemented and functioning properly.

Project Management Frameworks

As we’ve said, a framework can be described as a set of laws, best practices, policies, procedures, and processes, all wrapped up in an implementable, established format. Project management frameworks help provide that standardized, industry-accepted approach toward managing projects. While all project management frameworks differ in their content (and sometimes context) slightly, they all contain basic steps comprising the project

initiation, the design and planning phases of the project, the execution of that plan, the tracking of the progress (or monitoring), and project closeout. Each of these phases will have risks that need to be addressed, and some frameworks even have their own specified areas that address risk. An example is tracking the risks (perhaps using a risk register) alongside the project goals and objectives to ensure that all are kept within organizationally accepted tolerance levels.

PMI-PMBOK

The Project Management Institute (PMI) Project Management Body of Knowledge is perhaps the most recognized project management framework internationally. The PMBOK divides project management into process groups, knowledge areas, and associated processes. The five process groups are as follows:

- Initiating
- Planning
- Executing
- Monitoring and Controlling
- Closing

Within the Initiating phase, you conduct your project kickoff. This is where you get authorization to move forward with the project, and you create the project charter. Next, you conduct the Planning phase, where the work plan is developed. The Executing phase is where all your hard work planning pays off; you implement your plan and watch it come to life. Monitoring and Controlling covers the critical points of tracking progress against established milestones, goals, and objectives, and conducting remediation actions as necessary. Finally, as discussed previously, all projects have a definite life span and must be closed out in the Closing phase, with appropriate lessons learned documented.

There are also a number of certifications associated with the PMBOK framework, including the Project Management Professional (PMP), the Certified Associate in Program Management (CAPM), and the Program Management Professional (PgMP). While you don't need to know about these certifications within the scope of the CRISC exam, it's good to be aware of their existence because they are some of the more widely held and respected credentials within the Project Management field.

CMMI

The Capability Maturity Model Integration (CMMI) framework is an internationally recognized standard for improving processes within organizations. Developed by Carnegie Mellon University, the CMMI is used to gauge the process maturity within the organization and to place it within a "maturity level." There are CMMI frameworks for a number of sectors, including CMMI for Acquisition (CMMI-ACQ), CMMI for Services (CMMI-SVC), CMMI for Development (CMMI-DEV), Data Management Maturity (DMM), and the People CMM. You'll see many large companies boasting about their CMMI level; it's considered to be a solid gauge of the process maturity within an organization. Why does this matter? If you want to, for example, hire an

external software developer to create and maintain an enterprise-wide budget tool, their CMMI rating would give you insight of how they deal with processes such as change management.

The maturity levels range from 1 through 5.

- **Level 1 (Initial)** Processes are poorly controlled and managed
- **Level 2 (Repeatable)** Processes are repeatable, sometimes even with consistent results
- **Level 3 (Defined)** Defined processes that can be improved over time
- **Level 4 (Quantitatively Managed)** Finding ways to adapt without significant loss
- **Level 5 (Optimizing)** Focus on continual improvement of processes

CMMI doesn't discuss risk as overtly as the PMBOK, but you can see the same overarching elements of processes being used to manage the different aspects of a project, including the tracking and optimization. CMMI puts particular value on the concept of process improvement, and organizations operating at CMMI level 5 are actively reviewing and improving their processes—including dealing with risk—on a regular basis.

Agile

Agile project management frameworks have been used within the software development sector for some time. The Agile methodologies look to improve—you'll never guess—agility by improving collaboration, reducing bureaucracy and red tape, and facilitating ad hoc groups creating products in a rapid fashion. The Agile Manifesto, released by the Agile Alliance, reflects the following principles:

- The highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
- Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
- Businesspeople and developers must work together daily throughout the project.
- Build projects around motivated individuals. Give them the environment and support they need and trust them to get the job done.
- The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
- Working software is the primary measure of progress.
- Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
- Continuous attention to technical excellence and good design enhance agility.

- Simplicity—the art of maximizing the amount of work not done—is essential.
- The best architectures, requirements, and designs emerge from self-organizing teams.
- At regular intervals, the team reflects on how to become more effective and then tunes and adjusts its behavior accordingly.

Within this manifesto, you notice the concepts of welcoming change (not common within many project management frameworks) and a self-organized team (as opposed to having a project manager formalize team membership). Finally, the concept of iteration—from the team members reflecting regularly on their own effectiveness and tuning accordingly to the delivery of regular products—is central to the Agile mind-set. While its more flexible, ad hoc project management methodology might not be ideal for every organization, you can definitely see how it would appeal to a certain subset of company such as a startup.

The Agile framework (as well as the Lean framework, discussed in the next section) differs from the PMBOK and the CMMI in its approach and rigidity. Both Agile and Lean value the ability to make quick changes and the ability to be more ad hoc through the use of self-organizing teams. There is much less emphasis on tracking through the use of metrics, and a discussion of project risk is almost nonexistent. Still, in an organization using these project management frameworks, risk should be considered and incorporated into the project processes from beginning to end.

Lean

The Lean mind-set is derived from the manufacturing sector and is looking to “lean” organizations through less waste; in this context, it means less waste within projects. Waste can be found within too much unnecessary time spent on a project or unnecessary personnel involved who could be utilized elsewhere. Anything that does not bring value to the project is a target for “leaning” or improving, perhaps even removal. Value should be defined early in the project by the end customer and often means what they will be willing to pay in the end for any segment or part. Lean project management differs from other frameworks by focusing efforts on improving processes to compress the overall project schedule to reduce the project cost and improve the profitability of the project.

A common tool used within Lean projects is the value stream map (VSM). Within the process of creating the VSM, the team will detail the steps, information flows, and any delays currently resident within existing processes. This will allow the team to better understand the current state of the processes within the company and look for areas to reduce waste. At this time, another, updated VSM is created to depict the leaner process.

Project Management and Risk Management

So, you’ve learned a good bit about project management within the previous sections, but how does it really interact with the discussions of risk? Remember, project management covers a defined project from start to finish and is looking to cut costs (time, scope, and overall project cost), and managing risks can often create new costs. However, as you read through the major frameworks, you’ll see a few concepts that are really central to

effective risk response management: understanding the project requirements, tracking project progress, improving processes, and creating value. Look at how these align with the overall risk-focused mind-set. You understand the requirements for tracking risk so that you know the organizational contexts and values, overarching laws and regulations, and existing policies that you must consider when determining how you will approach risk management. You track the progress in implementing your chosen risk responses (and track exceptions to the policies using your exception management process). You improve the fundamental organizational processes by incorporating a calculation of risk throughout all of your projects. Finally, understanding risk creates real value for the leadership because no project should be considered if the overall risk of failure, for example, outweighs the reward of success. Risk management helps your leadership succeed by helping quantify these concepts in a way that honest assessments can be made.

Chapter Review

In this chapter, we covered the risk response process from top to bottom. We discussed three major risk frameworks, the NIST RMF, the ISACA IT Risk Framework, and the ISACA COBIT. The NIST process is comprised of six steps: security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring, and it has an important consideration of continuous monitoring. The ISACA IT Risk Framework has three domains: Risk Governance, Risk Evaluation, and Risk Response. COBIT is not risk-centric or IT security-centric but is largely focused on governance. These frameworks all differ in their scope and content but have the same underlying goal of helping identify, deal with, and monitor risks within an organization. We discussed how risk response is an essential topic within all three frameworks.

We then covered the risk response process that includes the selection of risk response options, the prioritization of risk response options, and the implementation of the risk response plan. Each of these facets contains a number of key steps involving analysis, proper communication, and consideration of the organizational risk tolerance and risk appetite.

We then developed an understanding of the different risk response options, including risk avoidance, risk mitigation, risk sharing or transference, and risk acceptance. Each one of these options has advantages and disadvantages. We also discussed how risk responses should be selected and appropriately prioritized. This requires an understanding of whether a response is a quick win (a situation where the response is high benefit and low cost), requires a business case to be made, or necessitates a deferral (where the risk does not outweigh the potential cost). Each risk response choice requires careful consideration of these options to determine the best course of action; also, when it's time to implement the risk responses, knowing how to incorporate metrics, document thoroughly, and manage exceptions to the plan is key.

We also discussed how to implement the risk mitigations after they've been chosen, through the use of frameworks, both for controls and for the overarching project management. You learned how risk responses are assessed, through documentation review,

technical assessment, and interviews. We discussed how to properly document risk responses and any exceptions and report the activities to leadership. Finally, we covered training for both content and context as a regular, repeatable activity for personnel charged with implementing any controls.

Review Questions

1. Which of the following is *not* part of the risk response process?
 - A. Reviewing the results of the risk analysis
 - B. Implementing change management
 - C. Prioritizing risk response options
 - D. Implementing the risk reaction plan
2. Which of the following options can be considered a risk avoidance option? (Choose two.)
 - A. Not opening operations within countries that are considered high risk
 - B. Deploying intrusion detection systems (IDSs) across the enterprise
 - C. Choosing to turn down an opportunity to partner on a new technology project based on the poor performance of previous attempts
 - D. Purchasing insurance to cover financial losses in the event of a breach
3. What is phase 4 of the SDLC?
 - A. Sunset (disposition)
 - B. Implementation/assessment
 - C. Acquisition/development
 - D. Operations/maintenance
4. Which of the following would you choose if you had an expensive risk response option to a relatively low risk?
 - A. Develop a quick win
 - B. Conduct more research
 - C. Develop a business case
 - D. Defer
5. The SC of a system includes which of the following? (Choose all that apply.)
 - A. Confidentiality
 - B. Impact
 - C. Integrity
 - D. Availability

6. Which of the following is *not* a valid risk response option?
 - A. Risk avoidance
 - B. Risk acceptance
 - C. Risk prediction
 - D. Risk transference
7. Risk mitigations are developed to reduce which of the following? (Choose two.)
 - A. The acceptance of risk
 - B. The avoidance of risk
 - C. The likelihood of risk
 - D. The impact of risk
8. Which of the following is considered a managerial activity?
 - A. Development and implementation of an enterprise acceptable use policy
 - B. Implementation of an antivirus tool across the organization
 - C. Implementation of mantraps at all major business entrances
 - D. A tabletop exercise of the business continuity plan
9. _____ testing and evaluation is conducted before the system is released into final production.
 - A. Operational
 - B. Production
 - C. Essential
 - D. Final
10. What process would help you deal with risks that require an exemption to policy?
 - A. Exception management process
 - B. Risk acceptance process
 - C. Risk mitigation process
 - D. Risk management process
11. The _____ framework is not IT security–centric and was developed with organizational governance in mind.
 - A. ISACA IT Risk Management
 - B. COBIT
 - C. NIST 800-37, revision 1
 - D. CRISC

12. When monitoring the risk, you need to assure that the organization accepts the responsibility for operating within the _____ level.
- A. Risk acceptance
 - B. Risk management
 - C. Risk exposure
 - D. Risk tolerance
13. A business knowingly decides it wants to capitalize on an opportunity that contains a level of risk deemed within its acceptable levels of risk. No controls are applied to lower the risk further. In this case, the approach would be best defined as which of the following?
- A. Risk tolerance
 - B. Risk mitigation
 - C. Risk acceptance
 - D. Risk avoidance
14. _____ provide written direction for how security measures will be conducted within an organization. (Choose the best answer.)
- A. Corrective controls
 - B. Preventative controls
 - C. Deterrent controls
 - D. Directive controls
15. What are the three domains within the ISACA Risk IT Framework? (Choose three.)
- A. Risk Governance
 - B. Risk Response
 - C. Risk Evaluation
 - D. Risk Mitigation
16. A business wants to look at expanding into a developing country where the risks are high along with the rewards. The business needs to understand which of the following? (Choose two.)
- A. Risk response
 - B. Risk tolerance
 - C. Risk appetite
 - D. Risk strategy

17. What is the open source alternative for thorough and practical security testing?
- A. NIST 800-64
 - B. NIST 800-115
 - C. ISACA COBIT
 - D. OSSTMM
18. Which of the following is a technical control?
- A. Creation of a demilitarized zone within the enterprise architecture
 - B. Implementation of a physical security policy
 - C. Mandating two people to open secure areas together
 - D. Requiring segregation of duties across sensitive duty areas
19. _____ help(s) you quantify the effectiveness of your implemented risk response over its life.
- A. Leaders
 - B. Reports
 - C. Automation
 - D. Metrics
20. While the NIST 800-53 control catalog is used predominately within the United States, the _____ is used more widely internationally and has specific versions tailored for different types of industry.
- A. ISACA COBIT
 - B. Risk Management Framework
 - C. ISO 27002
 - D. ISACA Risk IT Framework

Answers

1. B. While change management is important, it is not a formal step of the risk response process.
2. A, C. Choosing to avoid risk often means not taking advantage of opportunities that are determined to be riskier than is acceptable.
3. D. Phase 4 of the SDLC is the operations/maintenance phase, where a system (and associated controls) is put into operation and continuous monitoring takes place.
4. D. In the event you have an expensive risk response option to a relatively low risk, you would ideally choose to defer. Always be on the lookout for low-cost options for high-risk scenarios.

5. **A, B, D.** The security category (SC) of a system must consider the confidentiality, integrity, availability, and impact of a system where the acceptable values for potential impact are low, moderate, or high.
6. **C.** Risk prediction is not an accepted risk response option.
7. **C, D.** Risk mitigations are developed to reduce the likelihood and impact of risk.
8. **A.** The development/implementation of an enterprise acceptable use policy is a managerial control.
9. **A.** Operational testing/evaluation is conducted before the system is released into final production (or operation).
10. **A.** The exception management process helps you deal with exemptions to your risk response process.
11. **B.** COBIT was not developed to be IT security–centric; it has an organizational governance approach.
12. **D.** The risk tolerance level is the acceptable level of risk that can be operated within.
13. **C.** The company would be exercising risk acceptance in making a risky decision without a strategy to mitigate or avoid the risk.
14. **D.** Directive controls provide written direction for how security measures will be conducted within an organization.
15. **A, B, C.** The three domains within the ISACA Risk IT Framework are Risk Governance, Risk Evaluation, and Risk Response.
16. **B, C.** A business looking to identify opportunities to capitalize on risk should understand its risk tolerance and risk appetite.
17. **D.** The Open-Source Security Testing Methodology Manual (OSSTMM) from the Institute for Security and Open Methodologies was created as a standard for thorough and practical security testing across the community.
18. **A.** A demilitarized zone is technical in nature.
19. **D.** Metrics help you quantify the effectiveness of your implemented risk response over its life.
20. **C.** While NIST 800-53 is used heavily within the U.S. government, International Standards Organization (ISO) 27002 is used much more widely internationally, and versions of 27002 specific to different industries, such as healthcare, have been developed that are more tailored to their specific contexts, laws, and regulations.

This page intentionally left blank

Control and Risk Monitoring

In this chapter, you will:

- Learn about types of control testing and assessment
- Discover tools and techniques used to conduct different types of control testing and assessment
- Understand and define key performance indicators
- Understand and define key risk indicators

In this chapter, we will review the concepts that comprise CRISC Domain 4, which is focused on risk control monitoring and reporting. In the previous chapters, we discussed the elements of risk and information system controls, and this chapter shows you how to most effectively and efficiently monitor those elements for maximum impact.

The CRISC exam objectives covered during this chapter include the following task statements:

- 4.1 Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk
- 4.2 Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile
- 4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making
- 4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance
- 4.5 Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls
- 4.6 Review the results of control assessments to determine the effectiveness of the control environment
- 4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making

Control Monitoring

In Chapter 5, we discussed the development and implementation of controls to help you reduce risks within your organization. In this section, we will discuss how you can assess and monitor the efficiency and effectiveness of those controls. Understanding how controls are operating within your organization is an important input to your risk management strategy.

Control Testing and Assessment

The controls you've put into place in your organization are always under constant threat from physical and logical intruders, poor security practices, and just general badness that seems to occur on a daily basis. Never mind how much money you spend and how many people you have devoted to the cause; there are always flies in the ointment. This is what keeps a good system administrator awake at 3 A.M. (other than the incessant calls from the help desk).

Many tools are available to assess the effectiveness of your controls; be aware, however, that these tools are also available to anyone who wants to cause harm to your organization. By taking a proactive approach to monitoring your controls and dealing swiftly with any concerns that are found, you can reduce the risk that someone might successfully exploit vulnerabilities within your organizational structure before you can remediate them.

Testing and Assessment Types

There are a number of ways to test your controls depending on the level of fidelity you are interested in achieving, as well as the amount of capital you are willing to spend to test those controls. Do you feel satisfied with having an internal team check your control effectiveness? Would you prefer to have an external team execute scans from an outside location and submit reports directly to you? Or, would you like the whole enchilada with a "real-world" test that accurately depicts the security posture of your organization? Finally, what are the legal and regulatory requirements for testing and assessing your controls? These are all critical questions you need to ask yourself before committing to a test or assessment methodology. Internal testing works from the inside of the network; the test team "plugs" into the internal network and attacks from within, thoroughly testing internal controls. Conversely, external testing involves the team attacking the perimeter first and working their way into the organization; this allows the team to test the external controls prior to the internal controls. We discussed testing and assessment in Chapters 4 and 5, but we'll go more in-depth on some different types in the following sections.

Threat Assessment

Threat assessments determine how threats, both of the natural and human-made type, might harm your systems and, subsequently, the data residing on those systems. Remember from Chapter 1 that a threat is a danger of harm that can be enacted on an asset. The asset has to be in danger from this threat; theoretically, if there is no danger, then there is no threat. Threats exploit specific vulnerabilities, as discussed in the following section.

A threat must have a matching weakness in a system that it can exploit, or act upon, if it is to be an effective threat. Threat assessments, then, are often conducted to identify matching threat and vulnerability pairings, as well as the threat agents that could exercise a threat. Like a vulnerability assessment, the assessment does not have to necessarily be part of but can definitely support risk management. Threat assessments are conducted using a wide variety of data, including historical trends, statistical analysis, industry data, and other information from sources including the government, vendors, and even the organization itself. A threat assessment entails gathering as much information on the potential organizational harms, similarly to what a threat agent (or something or someone who causes or initiates a threat against a vulnerability) would do. There are a number of sources for this data, including law enforcement and counterintelligence organizations, that are resident experts on your particular geographic area, industry, industrial, or technological specialization. Quality information regarding threats is also often available from historical or statistical information that may apply to your particular industry or area. Larger organizations often have their own threat or intelligence units that are tracking threats to their domain. Threat assessments should consider, at a minimum, the following:

- Natural disasters, such as flood, fire, or earthquake, that cause physical damage to assets
- Equipment malfunction, from normal wear and tear to catastrophic failure
- Employees, both malicious users and those with poor practices
- Intruders/hackers, unauthorized people attempting to compromise controls to gain access or even damage assets

It's important that a threat assessment consider the organization you work for, the particular industry you reside within, and what the particular targets within your organization would be. One example is healthcare, where specific threats might target both personal and protected health data that could be used for a number of malicious ends; information concerning these threats can be gathered from other healthcare organizations or government agencies. Another industry that might be targeted is education, where an educational institution is conducting applied research in conjunction with the defense industry. This happens quite frequently for cutting-edge technologies, which are just the type of thing an adversary would be deeply interested in. In this situation, an intelligence entity might be able to supply information on foreign intelligence services and their collection priorities, the likelihood of industrial espionage, and other relevant threats. Your organization must use the expertise it has at its disposal in order to determine to what level and how these threats would affect its infrastructure and data.

Vulnerability Assessments

In Chapter 1 we discussed vulnerabilities, and you'll recall that vulnerabilities are weaknesses in a system, operation, or facility that would make these resources susceptible to being exploited by a threat. Vulnerabilities can exist in the way a system processes, transmits, or stores data; they can also exist in the technologies that make up a system or even

in its design. Vulnerability assessments are designed for a (generally) third party to come into an organization, take stock of the assets that will be covered within the scope of the assessment, conduct scans and other tests against those assets, and provide a report of the vulnerabilities that have been found. Often, a report recommending possible remediation measures is also included within the deliverables. Vulnerability assessments often occur from an internal point looking across the organization; the team will host its equipment within the network to get the best look at the vulnerabilities without the interference of the perimeter protections, such as firewalls. Many vulnerability assessment teams also have the benefit of administrator or root credentials, rather than basic user credentials. This allows an “open kimono” look at the patches that are missing, incorrect configurations, and other flaws in the system that should be corrected to improve the control set. A vulnerability assessment is commonly included within a risk assessment.

Penetration Testing

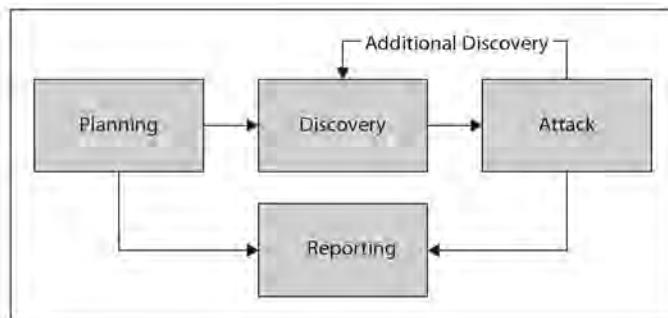
Penetration tests, unlike vulnerability assessments, are designed to actually exploit weaknesses on a system. Penetration tests take a vulnerability assessment a step (or ten) further in that they tell you all of the actual vulnerabilities based on their having been exploited, not just the probability. While vulnerability assessment is largely nonintrusive, becoming intrusive only when a scan brings a system down because of a misconfiguration or other situation causing a reboot or a crash of the system, a penetration test attempts to bypass security controls and exploit any vulnerability that is identified. If a vulnerability is indeed identified, the tester will attempt to “own” the system, often leaving a marker showing that they were there. The really high-speed, real-world tests will even attempt to conduct a denial-of-service attack or steal data, just like an attacker would do. The results from penetration tests can be used to better determine how to protect the system, by mitigating the vulnerabilities that the tester was actually able to exploit.

There are a couple of different types of penetration test that you should understand. A *black-box* test, or *blind* test, means that a penetration test is performed with no prior knowledge about the system design and architecture, personnel and organizational structure, and other attributes that could shed light on inherent weaknesses. In the same manner as a malicious actor, the tester would have to use reconnaissance activities to determine weaknesses.

Another type of penetration test is the *gray-box* test, in which the tester has some knowledge, albeit limited, of the organization and its infrastructure. This could be limited to just information that can be found in certification and accreditation or other sensitive internal documentation. Finally, there’s the *white-box* test, where the tester has full knowledge of the network, access to diagrams of the network, information in detail of hosts and services on the network, and potentially documentation from previous testing events.

Within a black-box (blind) test, as noted, the testers do not have prior access to the information regarding the organization and its infrastructure. In a *double-blind* test, those charged with defending the network are unaware of the testing and are tested on their ability to react and defend as if a real-world attack were taking place. Figure 6-1 shows the NIST SP 800-115 penetration testing cycle. As NIST points out, this is an example of how the penetration process can be divided into phases. However, there are

Figure 6-1
The NIST SP 800-115 four-stage penetration testing methodology



many acceptable ways of grouping the actions involved in performing penetration testing, and other models are available for your use.

Within the planning phase, the rules of engagement are set, and management approves the testing parameters. Without the due diligence in the planning phase, you could have any number of disastrous situations, from a lack of management support to overstepping boundaries because of a lack of agreement. The discovery phase includes reconnaissance, or information gathering, as well as vulnerability analysis. Vulnerability analysis requires the systems—and their resident operating systems and software—to be scanned, generally using automated tools, and compared to accepted vulnerability databases.

The attack phase can be delineated into steps: gaining access to the system, elevating privileges to gain administrator (or root) access, browsing the system, and installing additional tools. At any point in time, a new system could be discovered, and the cycle would loop back; this is depicted in Figure 6-2.

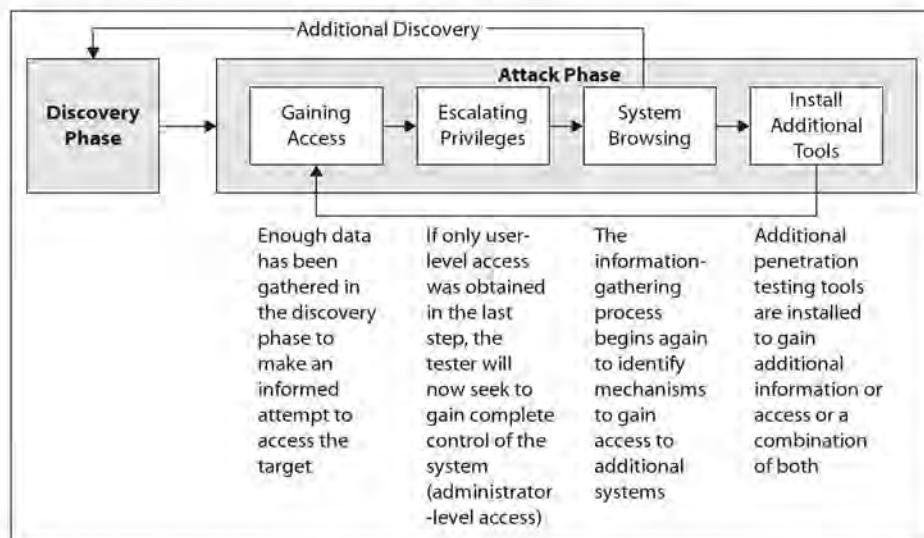


Figure 6-2 The NIST SP 800-115 attack phase steps with loopback to discovery phase

Finally, reporting is occurring continuously throughout the process; the reporting requirements are often laid out within the rules of engagement or management approval documentation. Generally there is a big final report at the end that details all the findings, but there could be weekly, or even daily, reports that are required, as well as “spot reports” in the event of an incident or a major finding. Be sure you detail what is expected for reporting up front!

Control Testing and Assessment Tools

In the previous sections, we discussed some different methods of conducting assessments and tests against the controls you’ve put into place. In this section, we will discuss the tools and techniques that are often used to conduct those assessments and tests. These are only a smattering of the most basic available tools; there are far more sophisticated and advanced tools available to professionals, both friend and foe.

Passive vs. Active Tools

It’s important to understand the difference between passive and active tools because they can have a big effect on your test. *Passive* tools are used when you desire no interference with daily activities. Passive tools listen for network traffic or monitor the hosts they reside on quietly and with little to no impact on the ongoing operations. This is good and bad! Defenders are fans of passive tools because they can conduct these activities during business hours with no negative performance effects; conversely, malicious entities use passive tools because they’re often hard to detect.

At the opposite end of the spectrum, *active* tools interact actively with a system, and this has pros and cons as well. These tools can often give you a more realistic perspective of vulnerabilities and the overall control effectiveness but can cause performance issues, sometimes even denials of service, driving system administrators straight toward the headache medication. Testing professionals often tread carefully with active tools, most carefully within a production environment, to avoid issues they’re trying to protect against. However, active tools produce extremely valuable results and cannot be thrown out of the toolkit. We will discuss some active tools later in this chapter.

Protocol Analyzer

A *protocol analyzer* is often known as a *sniffer* and is dedicated hardware or software that collects network traffic for the purposes of examination, either to determine network issues or to capture plain-text usernames, passwords, or other sensitive information being sent in the clear. Encryption helps protect against the malicious use of a protocol analyzer; while the data can still be captured, the encrypted data is gibberish until it’s unencrypted.

Port Scanner

A *port scanner* allows the tester to determine which ports on the system are listening for requests; this is a crucial step in determining what can be exploited. There are a standard set of ports, including 65,535 TCP ports and User Datagram Protocol (UDP) ports, available for running services on a system. The first 1,024 are *well-known* or common ports, such as FTP (21), SMTP (25), DNS (53), HTTP (80), and HTTPS (443). After the first

Table 6-1	Service	TCP/IP Port Number
TCP/IP Services and Port Numbers	HTTP	80
	FTP (Data)	20
	FTP (Control)	21
	DNS	53
	DHCP	67
	SMTP	25
	SNMP	161
	Telnet	23
	POP3	110
	IMAP	143
	NTP	123
	NNTP	119
	SSH	22
	LDAP	389

1,024 ports are port ranges used by applications, services, and other devices. Table 6-1 lists the most common services and their corresponding TCP/IP ports.

Vulnerability Scanner

When a tester has determined which systems are available on the network, the next step is to determine the associated vulnerabilities. A *vulnerability scanner* is a piece of software designed to scan a system to determine what services the system is running and whether any unnecessary open ports, operating systems and applications, or back doors can be exploited because of a lack of patching or other flaw. Administrators commonly use the same tools to test and remediate any flaws existing within the system. Vulnerability scanners can include previously mentioned tools within their kit, such as port scanning, network scanning and mapping, and operating system and application server scanning, and can include a database of known weaknesses vulnerabilities. The scanner will execute one or more of those tools against the targets to determine whether any of the vulnerabilities listed in its database exist.

False Positives and Negatives

False positives and false negatives are two different types of findings you should be aware of when looking at the results generated by your tools. A false positive is when a vulnerability is reported that isn't actually legitimate. An example of that might be when a Windows patch is reported missing on a Unix system. That's easy because the patch isn't required or even possible. A false negative, on the other hand, can be much more serious. A false negative is when a vulnerability isn't detected when it does actually exist. This is a great reason to use a number of tools to analyze your controls and not rely on just one that could let you down in the end.

Indicators

Now that you understand the tools that can be used to test control performance, you can move toward the indicators associated with measuring and reporting that performance and come up with current risk levels accurately and efficiently. You will often hear indicators referred to as metrics, and in this book, those terms are interchangeable for our purposes. However, the types of indicators and what they measure differ. *Key performance indicators* (KPIs) are used to understand and enable the measurement of control performance. Control performance can be anything from how often your firewall blocks malicious incoming traffic to how often your continuity of operations plan is exercised. The level of “performance” can be different for each organization; it’s important that you not solely borrow the KPIs from another organization as a whole but really focus on how they meet your organizational objectives and what your risk appetite is. Risk indicators are metrics, much like KPIs, that are used to determine whether and when the organization has a high probability of risk that exceeds the defined risk appetite. Not all risk indicators, however, are key. *Key risk indicators* (KRIs) are considered to be highly probable indicators designed to accurately predict important levels of risk based on defined thresholds.

So, why do you need indicators? How do you know whether you’re doing well or poorly? Do you trust your risk team, hoping that they have some sort of reporting mechanism that will scratch the stakeholder itch? At the end of the day, you want to be able to monitor and analyze those indicators to track trends and determine the effectiveness and efficiency of the controls and to make decisions for creating new controls, ditching others, and sounding the alarm when risk has passed a predefined threshold.

Defining Key Performance Indicators

Understanding what a key performance indicator means to your organization requires you to ask yourself a few questions. What is your organization’s mission? Are you a research organization attempting to develop a new cryptographic algorithm? Or are you a bakery that is trying to create a new frosting recipe? What are the things that are important to your organization? Do you want to have availability above all other attributes and the ability to conduct business through any fire, storm, hacking attempt, or any other scenario that can be thrown your way? Perhaps you instead value secrecy in lieu of any other consideration, wanting to keep that frosting recipe as top-secret as the recipe to build a stealth bomber. All joking aside, these are questions you need to ask yourself when developing key performance indicators. Remember, these key performance indicators help you understand how controls are performing to enable all of these attributes. You want to make sure that controls are performing at the level you find tolerable, so as discussed previously, the level of performance can be different and cannot be wholly borrowed from any other organization.

We covered the differences between qualitative and quantitative methods in Chapter 1, but to recap, qualitative methods involve using subjective scales. These scales could consist of a numerical scale of one to ten or have subjective values of High, Medium, and Low, for instance. Qualitative KPIs, then, can be measured using historical trend analysis, experience, expert opinion, existing internal and external environmental factors, governance, and other inputs that are not always necessarily quantifiable but exist and are important nonetheless. Conversely, quantitative methods use concrete (nonsubjective)

numerical values and statistical analysis to calculate the likelihood and impact of risk. Quantitative analysis uses numerical values such as dollar figures, statistical numbers, and any other hard-core numerical assignments. For our purposes, we will err toward quantitatively measured KPIs because they are more objective as opposed to subjective (like qualitative measurements can sometimes be).

KPIs should be S.M.A.R.T. to be most effective. This stands for the following:

- Specific
- Measurable
- Attainable
- Relevant
- Timely

When a KPI is S.M.A.R.T., it is tailored to the organization and the area being measured. Are you attempting to measure availability? And you may want to look at a metric that measures how often your systems go down or, the converse, the percentage of time that your systems are up. Measurable KPIs can be measured somehow, in a way that can be assured that it is accurate. In the instance of the availability measurement, how would you measure this accurately? Perhaps you would determine how often the systems went down based on the uptime command in the Unix operating system. However, there are other ways to measure this such as “When a KPI is attainable, it is readily achievable.” While it is admirable to shoot for the stars, you wouldn’t want to, for instance, shoot for 100 percent uptime in a situation where you have an entirely new staff, new equipment, new management, and so on. Perhaps 85 percent is more achievable, and then you can work toward that 100 percent mark. KPIs that are relevant matter to your organization. If you’re in a situation where time is of the essence, such as stock trading, availability is essential. Without availability, your systems cannot buy or sell stocks, and your user base will quickly move on to another organization that values availability as much as they do. However, other contexts, such as educational institutions, may not care so much about availability. Usability might be the word of the day, or it might be the ability to access content via mobile applications or other cutting-edge technologies. Think about what’s important or relevant to your organization when determining your KPIs. Finally, timely KPIs allow the data to be collected when needed to quickly determine the performance of your measured initiative. Data should be able to be obtained relatively easily from existing sources and repositories.

A number of academic institutions have done some really great work on KPIs and metrics that is useful for anyone looking to define solid KPIs. For example, Cornell University has conducted research on the business of KPIs and has determined that KPIs should include the following attributes:

- **Objective** Goal or objective that the metric supports (for example, business process)
- **Description** What the metric is about; why the metric is useful

- **Data source** Where the data was obtained (and often by what means), how the metric is calculated, and quality of the data
- **Metric owner** Individual responsible for providing the metric
- **Reporting period** Period for which the metric is applicable or relevant
- **Reporting frequency** Frequency in which the metric is measured
- **Present value** Current or present value of the metric as most recently measured
- **Previous value** Value of the metric from the last measurement period
- **Baseline** Normally expected value for a metric (an average for example); may also include lowest and highest possible values for the metric
- **Trend** Direction the metric is moving; should indicate if increased or decreased values are better and the progress (improving, getting worse, and so on)
- **Thresholds** Expected ranges of the metrics; this determines where the metric is with respect to target values (determines acceptable values for “green” status) and danger values (determines unacceptable values; generally the delineation between “yellow” status and “red” status)

The Oak Ridge Institute for Science and Education has also published questions that can help you determine the quality of your metrics.

- Is the metric objectively measurable?
- Does the metric include a clear statement of the end results expected?
- Does the metric support customer requirements, including compliance issues where appropriate?
- Does the metric focus on effectiveness or efficiency of the system being measured, or both?
- Does the metric allow for meaningful trend or statistical analysis?
- Have appropriate industry or other external standards been applied?
- Does the metric include milestones or indicators to express qualitative criteria?
- Are the metrics challenging but at the same time attainable?
- Are assumptions and definitions specified for what constitutes satisfactory performance?
- Have those who are responsible for the performance being measured been fully involved in the development of this metric?
- Has the metric been mutually agreed upon by you and your customers?

NIST also has some great information on performance measurement within its Special Publication 800-55, revision 1, “Performance Measurement Guide for Information Security.” In this document, NIST lists three types of measures: implementation measures,

effectiveness/efficiency measures, and impact measures. NIST states that implementation measures are used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures. Effectiveness/efficiency measures are used to monitor if program-level processes and system-level security controls are implemented correctly, operating as intended, and meeting the desired outcome. Finally, impact measures are used to articulate the impact of information security on an organization's mission. To that end, NIST 800-55 lists the following security requirements that are a great basis for lowering risk within an organization and an excellent basis for KPIs:

- **Access control (AC)** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise.
- **Awareness and training (AT)** Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the information security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the information security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- **Audit and accountability (AU)** Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions.
- **Certification, accreditation, and security assessments (CA)** Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- **Configuration management (CM)** Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective information system development life cycles; and (ii) establish and enforce information security configuration settings for information technology products employed in organizational information systems.

- **Contingency planning (CP)** Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
- **Identification and authentication (IA)** Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- **Incident response (IR)** Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
- **Maintenance (MA)** Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- **Media protection (MP)** Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
- **Physical and environmental protection (PE)** Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
- **Planning (PL)** Organizations must develop, document, periodically update, and implement system security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
- **Personnel security (PS)** Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established information security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational information security policies and procedures.

- **Risk assessment (RA)** Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
- **System and services acquisition (SA)** Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ information system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate information security measures to protect information, applications, and/or services outsourced from the organization.
- **System and communications protection (SC)** Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and information systems engineering principles that promote effective information security within organizational information systems.
- **System and information integrity (SI)** Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Defining Key Risk Indicators

Now that you've determined indicators to measure the performance of the controls that you put into place, you need to determine ways to indicate the risk that your organization is subject to. KRIs are related to but separate from KPIs, in that KRIs are all about how the metric predicts current and future risk, rather than past performance of a specific control or set of controls. KRIs are linked to specific risks and provide an early warning alarm that a risk is emerging, allowing leadership to be proactive and deal with that risk sooner rather than later.

ISACA's Risk IT Framework includes the following criteria to select KRIs:

- **Impact** When a risk indicator has a high impact, it is likely to be a KRI.
- **Effort to implement, measure, and report** When all is equal, the easiest indicator to measure from is the best.
- **Reliability** The indicator reliably predicts an outcome.
- **Sensitivity** The indicator accurately indicates variances in the risk.

Similarly to the determination of KPIs discussed earlier, KRIs should be S.M.A.R.T. and should drill down to the root cause and not just focus on the symptoms that are immediately evident. KRIs should include lagging indicators, or indicators that determine current risk after an event has occurred; leading indicators, which indicate the controls in place to prevent an event from occurring; and trends, as discussed previously, which consider patterns in the data that indicate risk. Root-cause analysis is also important here, as discussed within KPIs, to determine the root cause for any risk, not just the symptoms.

Root-Cause Analysis

Finally, it is important to use indicators that measure the root cause of any issue and don't focus on the symptoms themselves. Root-cause analysis (RCA) has its roots in rocket science, and NASA has used it to determine faults within its programs. Essentially, RCA looks to establish a causal relationship between the root cause (or causes) and the problem as it has manifested itself. While we won't get into the details (or even basics) of rocket science, it is easier to understand how the culture of space exploration, and attempting to lower risk in such a complex environment, helps you to understand the importance of digging deep for the root cause. For example, the tragic Challenger shuttle disaster manifested itself with an explosion 73 seconds after liftoff. That is the problem, with a loss of seven crewmember lives, but the root cause is deeper and must be critically analyzed. In the end, root-cause analysis showed that a rubber O-ring failed, causing the disintegration of the spacecraft and the loss of all lives. Understanding that root cause has saved dozens of lives in subsequent space missions because of redesigns and modifications that were made as a result.

Collecting and Analyzing Data

Now that you've determined what your indicators will be – whether KPI or KRI – you need to determine what data to collect. You have a number of sources at your disposal for useful measurement. One might be previously reported results, both internal and external. Internal reporting might be internal audits or internal risk assessment results, for example. Logs are another rich source of data to use for measurement. Logs can contain valuable information on past and ongoing activities and, when handled properly, can be timely. However, don't fall into the trap of thinking that logs are the end-all and be-all of metrics generation. For example, it's easy to believe that an indicator such as "frequency of successful compromise of an organizational asset" is a useful metric. What if you don't know you've been successfully compromised? It's easy to assume that your logs (or people) are infallible and that if you don't determine that a compromise has taken place, you're good as gold. What does that metric mean, however, if it's determined that you have had a prolonged compromise years down the road? You simply don't know what you don't know. Another trap to avoid is too much data from too many sources; with an influx of data, sometimes at the terabyte level, it's easy to miss significant individual events. You need to work hard to focus in on the points of data that are indeed important.

You also need to be on the lookout for any trends that might indicate risk is moving in an upward pattern. A one-time blip, even if it's significant, is less relevant to your

organization's risk profile than an upward trend proactively indicating a serious increase in the organization's risk. This is what you're looking for when you attempt to determine an upward trend, and you need to make sure that the data you're collecting helps you find trends, rather than one-time events. Be aware of patterns that might be emerging within your data, particularly those that indicate a downward slope in efficiency or effectiveness of the controls you've put into place.

Reporting

At the end of the day, risk professionals need to make sure they have a clear understanding of the exposures their organization faces, the active mitigations for those exposures, and the indicators that are being used to measure the success or failure of the control set, as well as the current risk posture as measured against the risk appetite. This all needs to be communicated to the stakeholders. Articulating risk should not be underestimated; this is the place where you win hearts and minds through improving the bottom line by reducing negative risk and capitalizing on positive risk. Responsible reporting involves helping leadership understand the risks to the organization and how critical it is to support their reduction through compliance with appropriate controls, as well as identifying business opportunities in areas that can withstand risk. This needs to be done in the most clear and concise manner possible, understanding the concepts of risk, the indicators that have been chosen, and the current statuses that allow leadership to make the best-informed decisions possible. Without the best possible information, you cannot expect leadership to make informed decisions. You also need to interpret technical findings and perhaps portray information in a manner that is less technical and more "business speak." What does this mean? When is the last time that you heard a senior leader within your organization use purely technical jargon to describe ongoing business performance? Maybe if you are at a tech company, this is normal, but for the rest of us, we need to still place this information in a format that is understandable for leadership. By doing this, you will not only make the point that the risk program is useful and worthwhile and is supporting business goals and objectives but also identify opportunities for the risk program (and associated reporting) to integrate throughout the enterprise more cleanly.



NOTE Communicating clearly will help you receive more useful guidance from your organization's leadership; while that may sound like a drag, in fact, it will facilitate all of those previous "good news" opportunities.

No communication is complete without thoroughly understanding and depicting both the worst-case and most probable scenarios involved with a risk event. A risk event could mean many potential losses take place, not only those affecting the company's financial bottom line. There could be losses to the company's goodwill, including any brands associated. Think about major security breaches in previous years, including Target, TJ Maxx, and Sony. The result of their losses was both tangible (financial) and intangible (brand associated with a major breach), and this is difficult to quantify.

This is also the time to include any other information that would be pertinent to supporting the recommendations you've made, such as situations where a financial gain could be made (through exploiting an opportunity) or any outlying legal or regulatory concerns you might have.

Chapter Review

In this chapter, we discussed how you can assess and monitor the efficiency and effectiveness of controls and risk. We discussed different types of testing and assessment, including threat assessment, vulnerability assessment, and penetration testing. Threat assessments determine how threats, both of the natural and human-made type, might harm your systems and, subsequently, the data residing on those systems. Vulnerability assessments are designed, often by a third party, for an organizational inventory that includes scans and other tests against those assets and includes a report of the vulnerabilities that have been found. Penetration tests, unlike vulnerability assessments, are designed to actually exploit weaknesses on a system. Penetration tests take a vulnerability assessment a step further in that they tell you all of the actual vulnerabilities based on their having been exploited, not just the probability of them. Black-box tests, or blind tests, mean that penetration testing is performed with no prior knowledge about the system design and architecture, personnel and organizational structure, and other attributes that could shed light on inherent weaknesses. The gray-box test differs in that the tester has some knowledge, albeit limited, of the organization and its infrastructure. Finally, there's the white-box test, where the tester has full knowledge of the network and access to diagrams of the network, information in detail of hosts and services on the network, and potentially documentation from previous testing events.

We then covered the tools that are often used to conduct those assessments and tests, both passive and active. Passive tools are used when you desire no interference with daily activities and listen for network traffic or monitor the hosts they reside on quietly and with little to no impact on the ongoing operations. At the opposite end of the spectrum, active tools interact actively with a system, which has pros and cons as well. These tools can often give you a more realistic perspective of vulnerabilities and the overall control effectiveness but can cause performance issues, sometimes even denials of service. We subsequently detailed a sampling of tools, including protocol analyzers, port scanners, and vulnerability scanners.

We then covered indicators associated with measuring and reporting performance and current risk levels accurately and efficiently. Key performance indicators are used to understand and enable the measurement of control performance. Key risk indicators are considered to be highly probable indicators designed to accurately predict important levels of risk based on defined thresholds. Both KPIs and KRIs should be specific, measurable, attainable, relevant, and timely, and the root cause should be taken into account to ensure that indicators measure the root cause of any issue and don't focus on the symptoms themselves. We then discussed the need to determine what data you can collect to help measure indicators effectively.

Review Questions

1. _____ are often conducted to identify matching threat and vulnerability pairings.
 - A. Vulnerability assessments
 - B. Threat assessments
 - C. Penetration tests
 - D. Gray-box tests
2. _____ often occur from an internal point looking across the organization to get the best look at the vulnerabilities without the interference of the perimeter protections.
 - A. Threat assessments
 - B. Penetration tests
 - C. Vulnerability assessments
 - D. Black-box tests
3. _____ are designed to exploit weaknesses on a system.
 - A. Threat assessments
 - B. Penetration tests
 - C. Vulnerability assessments
 - D. White-box tests
4. A _____ means that a penetration test is performed with no prior knowledge about the system design and architecture, personnel and organizational structure, and other attributes that could shed light on inherent weaknesses.
 - A. Clear test
 - B. White-box test
 - C. Gray-box test
 - D. Blind test
5. In a _____ test, those charged with defending the network are unaware of the testing and are tested on their ability to react and defend as if a real-world attack were taking place.
 - A. Double-blind
 - B. Gray-box
 - C. White-box
 - D. Penetration

6. Jim wants to conduct a scan using a tool that can be used during business hours with minimum disturbance to operations. Which is the most likely to support his needs?
- A. Active tools
 - B. Impact tools
 - C. Penetration tools
 - D. Passive tools
7. A _____ is dedicated hardware or software that collects network traffic for the purposes of examination, either to determine network issues or to capture plain-text usernames, passwords, or other sensitive information being sent in the clear.
- A. Port scanner
 - B. Protocol analyzer
 - C. Vulnerability scanner
 - D. Penetration tester
8. A _____ allows the tester to determine which ports on the system are listening for requests.
- A. Port scanner
 - B. Protocol analyzer
 - C. Vulnerability scanner
 - D. Penetration tester
9. A _____ is a piece of software designed to scan a system to determine what services the system is running and whether any unnecessary open ports, operating systems and applications, or back doors can be exploited because of a lack of patching or other flaw.
- A. Port scanner
 - B. Protocol analyzer
 - C. Vulnerability scanner
 - D. Penetration tester
10. John is reviewing the results of a vulnerability assessment on his Unix-based network and finds a Windows patch missing. What is the likely finding?
- A. False positive
 - B. False negative
 - C. False flag
 - D. False vulnerability

11. _____ are used to understand and enable the measurement of control performance.
- A. Key performance indicators
 - B. Key control indicators
 - C. Key risk indicators
 - D. Key monitoring indicators
12. _____ are considered to be highly probable indicators designed to accurately predict important levels of risk based on defined thresholds.
- A. Key performance indicators
 - B. Key control indicators
 - C. Key risk indicators
 - D. Key monitoring indicators
13. _____ measurements can be derived from historical trend analysis, experience, expert opinion, existing internal and external environmental factors, governance, and other inputs that are not always necessarily quantifiable.
- A. Quantitative
 - B. Objective
 - C. Solid
 - D. Qualitative
14. _____ methods use concrete (nonsubjective) numerical values and statistical analysis to calculate the likelihood and impact of risk. (Choose the best answer.)
- A. Quantitative
 - B. Objective
 - C. Solid
 - D. Qualitative
15. When a KPI is S.M.A.R.T., it is which of the following? (Choose all that apply.)
- A. Short
 - B. Measurable
 - C. Right
 - D. Timely
16. What NIST SP 800-55 security requirement requires organizations to limit access to authorized users?
- A. Awareness and training
 - B. Audit and accountability
 - C. Access control
 - D. Configuration management

17. What NIST SP 800-55 security requirement states that organizations must establish and maintain baseline configurations and inventories of organizational information systems?
- A. Awareness and training
 - B. Audit and accountability
 - C. Access control
 - D. Configuration management
18. ISACA's Risk IT Framework includes which criteria? (Choose two.)
- A. Impact
 - B. Meaningfulness
 - C. Reliability
 - D. Efficiency
19. The process of _____ helps to determine a causal relationship between a cause and the manifested problem.
- A. Causal analysis
 - B. Root-cause analysis
 - C. Indicator analysis
 - D. Exploratory analysis
20. _____ can contain valuable information about past and ongoing activities and, when handled properly, can be timely.
- A. Metrics
 - B. Accreditations
 - C. Indicators
 - D. Logs

Answers

1. **B.** Threat assessments are often conducted to identify matching threat and vulnerability pairings, as well as the threat agents that could exercise a threat. Like a vulnerability assessment, the assessment does not have to necessarily be part of but can definitely support risk management.
2. **C.** Vulnerability assessments often occur from an internal point looking across the organization; the team will host its equipment within the network to get the best look at the vulnerabilities without the interference of the perimeter protections, such as firewalls. Many vulnerability assessment teams also have the benefit of administrator or root credentials, rather than basic user credentials.

3. **B.** Penetration tests, unlike vulnerability assessments, are designed to actually exploit weaknesses on a system. Penetration tests take a vulnerability assessment a step further in that they tell you all of the actual vulnerabilities based on their having been exploited, not just the probability.
4. **D.** A black-box test, or blind test, means that a penetration test is performed with no prior knowledge about the system design and architecture, personnel and organizational structure, and other attributes that could shed light on inherent weaknesses.
5. **A.** In a double-blind test, those charged with defending the network are unaware of the testing and are tested on their ability to react and defend as if a real-world attack were taking place.
6. **D.** Passive tools are used when you desire no interference with daily activities.
7. **B.** A *protocol analyzer* is often known as a *sniffer* and is dedicated hardware or software that collects network traffic for the purposes of examination, either to determine network issues or to capture plain-text usernames, passwords, or other sensitive information being sent in the clear.
8. **A.** A port scanner allows the tester to determine which ports on the system are listening for requests.
9. **C.** A vulnerability scanner is a piece of software designed to scan a system to determine what services the system is running and whether any unnecessary open ports, operating systems and applications, or back doors can be exploited because of a lack of patching or other flaw.
10. **A.** A false positive is when a vulnerability is reported that isn't actually legitimate.
11. **A.** Key performance indicators are used to understand and enable the measurement of control performance.
12. **C.** Key risk indicators are considered to be highly probable indicators designed to accurately predict important levels of risk based on defined thresholds.
13. **D.** Qualitative measurements can be determined using historical trend analysis, experience, expert opinion, existing internal and external environmental factors, governance, and other inputs that are not always necessarily quantifiable.
14. **A.** Quantitative methods use concrete (nonsubjective) numerical values and statistical analysis to calculate the likelihood and impact of risk.
15. **B, D.** KPIs should be S.M.A.R.T. to be most effective. This stands for Specific, Measurable, Attainable, Relevant, and Timely.
16. **C.** Access control requirements state that organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise.

17. **D.** The principles of configuration management state that organizations must establish and maintain baseline configurations and inventories of organizational information systems.
18. **A, C.** ISACA's Risk IT Framework includes the following criteria to select KRIs: impact; effort to implement, measure, and report; reliability; and sensitivity.
19. **B.** Root-cause analysis looks to establish a causal relationship between the root cause (or causes) and the problem as it manifested itself.
20. **D.** Logs can contain valuable information about past and ongoing activities and, when handled properly, can be very timely.

Information Systems Control Concepts

In this chapter, you will:

- Learn the basic concepts of controls
- Examine different control frameworks

We've discussed controls throughout this book so far, but always from a risk identification, assessment, analysis, and response perspective. There's a lot more to be learned about security controls and how they are designed and implemented. In this chapter, we will begin to change direction a bit and focus on controls from those perspectives. We will review some basics regarding controls, and you will learn about how you select them to perform specific functions in protecting systems and data. We'll also review a few key control frameworks in detail, including the National Institute of Standards and Technology (NIST) control catalog, COBIT, and Val IT.

The CRISC exam objective covered in this chapter includes coverage of the following task statement:

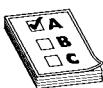
- 3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.

You'll find that this chapter only begins to cover this objective; coverage on control design and implementation is also the focus of Chapter 8. This chapter essentially covers the prerequisite knowledge on controls that you should have before an in-depth discussion on their use in managing risk, as well as in designing and implementing controls. Control selection, as well as their use in mitigating and managing risk, is discussed further in Chapter 8 and has also already been briefly touched on in Chapters 4 and 6.

Additionally, you'll find that this chapter covers much more material than you might find on the exam; this is for two important reasons. First, it's important that you understand foundational and conceptual knowledge about controls and some of the relevant control frameworks you will find both on the exam and in the real world as a risk and control assessor. Second, this book is intended to be not only a study guide for the exam but also a comprehensive reference you will use even after you have passed the CRISC exam.

Information Security Control Concepts

Before getting too deeply involved in control frameworks, it's helpful to understand what a control is. Although we've discussed controls throughout the book, we haven't really defined some of the finer points of controls. *Controls* are fundamentally defined as measures implemented to ensure that processes are performed to a certain standard, degree, or depth; they offer detailed guidance relevant to a specific requirement. There are different contexts for controls; for example, you may have financial controls that regulate how transactions are securely processed, ensuring correct balances. In terms of information security (and the corresponding risk context), they are used to specify what measures should be taken to ensure security and reduce risk. Controls should be directly relevant to the risk at hand; usually controls are defined and implemented in terms of addressing a specific vulnerability or deficiency in asset protection. Often, controls directly address a known risk or vulnerability in a given system, environment, or program, such as health-care or financial IT systems and environments.



EXAM TIP Controls are measures implemented to reduce the likelihood and impact elements of risk and may target specific vulnerabilities in an asset or be used to generally protect several assets.

Control libraries or catalogs are defined sets of controls that can be used in a given set of circumstances, market, or area. Controls are often tied to governance directives and frameworks, but this isn't always the case. Sometimes different regulations or even process frameworks reference controls only to the extent that a control framework is required, but not to specify which control catalog must be used. The Health Insurance Portability and Accountability Act (HIPAA) is a good example of this scenario because HIPAA requires security and risk controls, but it does not specify which control set must be used (although HIPAA guidance does recommend the NIST control catalog). As another example, while references to controls are specifically called out in the ISACA Risk IT Framework (RR 2.1, "Inventory Controls," and RR 2.4, "Implement Controls"), the framework itself does not give any clear guidance on how controls are defined, selected, or implemented. The assumption is that implementing the framework will show you how to use and evaluate whichever control set you choose, especially if it's the COBIT 5 or Val IT control sets, which are also associated with ISACA. The NIST Risk Management Framework (RMF), in contrast, does provide guidance on how its controls are constructed, used, and assessed, devoting two entire publications to this subject.

Specific product or market environments may require the use of specific controls that are context-related, as indicated in Table 7-1.

Controls in a given framework are often organized according to a particular area or context, usually by functionality or relevance. For instance, NIST controls are broken down into *families*, which are categories that apply to a specific context. As an example, Physical and Environmental Protection (PE) controls address physical and environmental concerns such as physical access control and environmental factors (lighting, humidity, and temperature), while the Program Management (PM) control family addresses management processes that often appear as administrative controls, such as formally

Area or Environment	Governance	Corresponding Control Set
U.S. federal government	Federal Information Security Management Act (FISMA)	NIST Special Publication 800-53, revision 4
Healthcare	HIPAA Security Rule	Various, but NIST Special Publication 800-53, revision 4, is recommended
Finance	Gramm–Leach–Bliley Act (GLBA), Sarbanes–Oxley Act (SOX)	PCI-DSS, COBIT
Private/commercial	Various	NIST Special Publication 800-53, COBIT 5, and so on

Table 7-1 Examples of Environments That Use Various Control Frameworks

appointing a responsible information security officer, for example. Most other control frameworks discussed in this chapter similarly categorize controls, usually by process area or other relevant aspect of context.



TIP You'll find that most control libraries similarly group controls into specific categories based upon function or context, and most use specific identifiers for each control.

Which controls from the various frameworks are used by an organization depends on several factors, including governance, market segment or area, level of regulation, and internal factors such as risk tolerance, appetite, and maturity of risk management processes. We cover more of how controls are selected, designed, implemented, and used later in this chapter and in the next chapters, but suffice it to say for now that controls are usually developed and applied to specific risk scenarios. These risk scenarios are developed by the organization or industry as part of their risk identification process. They describe threats, threat actors, events, time, and other circumstances, but of course, control assignment and use may be required by legal or regulatory governance, as well as the needs of the organization that intends to employ them. It's also fairly common that an organization will use more than one control set or framework because it may apply differently to various aspects of the business or mission areas in an organization. For example, a hospital may use NIST controls for some areas but may also be required to use PCI-DSS controls because it may process payments from credit cards as patients pay for medical services.

In examining the various control frameworks, you'll also find that there are many similarities between controls in some instances; often a control in one framework has a close equivalent in another framework. For example, COBIT control PO7 loosely maps to the NIST training control, AT-1, but describes a more generic process than the equivalent NIST control. There will also be controls that have no matching control or even context in another framework; these are often controls that deal with specific instances of risk or security requirements unique to a particular environment.



NOTE Most control catalogs have controls that can be easily mapped to controls in other catalogs, although in some cases, this mapping may be imprecise, may not be as detailed, or may even map to multiple controls in another control library.

Control Classification

We discussed in earlier chapters how different controls are classified and categorized, and those different categorizations are worth repeating here. The first way of categorizing controls is in terms of their application to different aspects of security. We often categorize controls in terms of administrative, technical, and physical controls. Administrative controls, if you remember correctly, are those that apply to policies, procedures, personnel, training, and so on. For example, a formally documented policy detailing how often backups should be made, to what type of media, and under what circumstances would be considered an administrative control. Related to that would be a technical control, which would be the backups themselves since data is backed up, preventing its loss. Obviously, the physical control aspect in this particular example would be the physical protection of the backup media, in terms of physical access, storage, and transport.

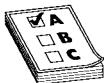


EXAM TIP The most common classifications of controls are as follows: administrative (sometimes also referred to as managerial), technical (also sometimes referred to as logical), and physical (which may also cover or be referred to as operational controls).

Yet another way of categorizing controls that we have discussed is according to function. Previously we identified several different functions that controls can fulfill and noted that some controls may serve more than one function at a time. Typically, these functions are normally considered to be deterrent, preventative, detective, corrective, compensating, and recovery. Note that different security texts and frameworks may categorize these functions differently. A deterrent control is one that prevents an action or issue from occurring, as does a preventative control. The difference here, however, is that a deterrent control must be known to someone in order to prevent an action. For example, a firewall rule that prevents someone from sending sensitive data outside the organization will work regardless of whether someone realizes the rule is in place. This would be considered a preventative control in this case. A deterrent control, however, is designed to keep an individual from even attempting to do so. A deterrent control in this case might be simply a warning message that pops up when someone attempts to send a specific type of sensitive data outside the network, in an e-mail, for example. A preventative control will work regardless of whether the individual is aware of it. A deterrent control relies on knowledge of the control in order to perform its deterrent action but may still prevent the action from taking place.

Detective controls serve to alert the proper individuals and management that a security issue has occurred. An example would be an intrusion detection system or a building alarm. Corrective controls typically are used to remediate an immediate or temporary

deficiency or weakness; you may see them put into place if a regular or permanent control is not performing its function sufficiently. Similar to a corrective control is a compensating control. A compensating control is used to make up for a deficiency in an established control. Corrective and compensating controls may be temporary in nature, until a more permanent solution can be found, either by strengthening the existing control or by completely replacing it with a better solution. Often, the same solution that was considered a corrective or compensating control, once it is considered permanent, may be considered simply a deterrent or preventative control, for instance. A recovery control is one that is used to recover the organization, system, or data to its previous state in the event of an incident. Restoring a system from backup might be considered a recovery control, even though actually backing up the data in the first place would be considered a preventative control. As previously mentioned, controls could be considered to be fulfilling several different functions simultaneously, so how you would categorize control with regard to these functional areas would depend upon the context in which you're discussing it.



EXAM TIP Controls may be categorized by function, which include preventative, deterrent, detective, corrective, compensating, and recovery controls. Often controls can serve more than one function simultaneously and may be difficult to completely categorize as one particular function or another.

Control Selection

Controls are applied to a system, data, process, or even organizational element to address a weakness or vulnerability or to counter a specific threat. Often, controls are applied to address a specific risk response strategy, such as risk reduction/mitigation, transference, avoidance, and acceptance. Controls are applied to reduce the impact and likelihood elements of risk, as follows:

- Reduce the likelihood of a threat agent initiating a threat (deterrence, preventative, and detection controls are examples)
- Reduce the likelihood of threat exploiting a vulnerability (preventative and detection controls)
- Reduce the impact to the organization or asset if a threat exploits a vulnerability (corrective, compensating, recovery controls)
- Reduce the vulnerability (deterrent, preventative, corrective, and compensating controls all could perform this action)

Note that none of the scenarios listed earlier describes a case where a control prevents a threat or a threat actor. Threats and threat actors exist, and controls can't really prevent their existence. Controls can, however, affect how they interact with vulnerabilities and assets. Also note that all these strategies may be pursued simultaneously in the case of

controls that are well designed and effective, using the concept of economy of scale and multiple use of controls.



EXAM TIP Remember that controls can affect the likelihood or impact risk elements only by reducing vulnerabilities or protecting assets. They cannot eliminate or reduce threats or threat actors; they only serve to reduce likelihood or impact resulting from an attempted or successful exploitation of a vulnerability by a threat.

Control Frameworks

Now that we've covered some generalities about controls, it's time to look at various control frameworks that you might use in your professional career. Keep in mind that some control frameworks go more in-depth than others on their controls; some controls in a given framework may treat a particular subject area lightly, while others may go into detail on a particular subject area. Also keep in mind that some control frameworks are geared toward specific environments or areas, and not all frameworks are necessarily geared toward security specifically; some frameworks apply to a broad general business or risk management area but may have security controls built into them for specific needs or direct security actions from a higher level. Not all control frameworks are technical in nature either; some frameworks apply to security and risk from a business process perspective rather than a technical perspective. The control frameworks we'll describe in the following sections are just some of the more popular ones that you may encounter in your professional career. You'll also see that we spend more time talking about the NIST control catalog than we do the others; this is because it is simply one of the more popular frameworks and one of the more comprehensive. It's also applicable to a wide variety of risk management programs and efforts. It's flexible, lending itself to almost any type of management framework an organization could use. However, we will also describe some of the other control frameworks you will encounter.

NIST

The U.S. Department of Commerce's NIST has produced several documents, some of which we have already discussed, that relate to risk management. The entire Risk Management Framework, and all of its different components, spans several documents. We will provide a comprehensive review of the framework and its related documents in Appendix A, but for now we'll examine a particular piece of the framework, the controls catalog. NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," is the control catalog supporting the RMF. The NIST controls are a comprehensive set of security measures and processes intended to mitigate and reduce risk from an IT security perspective.

The NIST control catalog is divided into 18 control groups, called *families*, each related to a particular aspect of IT security. Table 7-2 lists these families.

Control Family	Control Designation	Number of Controls in Family
Access Control	AC	25
Awareness and Training	AT	5
Audit and Accountability	AU	16
Security Assessment and Authorization	CA	9
Configuration Management	CM	11
Contingency Planning	CP	13
Identification and Authentication	IA	11
Incident Response	IR	10
Maintenance	MA	6
Media Protection	MP	8
Physical and Environmental Protection	PE	20
Planning	PL	9
Program Management	PM	16
Personnel Security	PS	8
Risk Assessment	RA	6
System and Services Acquisition	SA	22
System and Communications Protection	SC	44
System and Information Integrity	SI	17

Table 7-2 The NIST Control Families

As you can see, the NIST control families span a great deal of subject areas. Also note that each family has several controls in it; there are smaller families (such as the Awareness and Training family, for example) that may have as few as five controls, but there are others that have many different controls that go into great detail on security measures; an example is the System and Communications Protection (SC) control, with 44 controls. One thing to keep in mind about the numbers of controls for each family is that often, as the control catalog goes through editing or revisions, some controls may be merged with others or withdrawn entirely; this does not change the control numbering in subsequent revisions for backward compatibility and reference purposes. So, for example, the SC family, with 44 controls listed, actually has only 41 controls because three have been “withdrawn,” but their numerical placeholder remains to avoid confusion with later versions.



NOTE NIST also has 8 control families in addition to the 18 mentioned in Table 7-2 that specifically deal with privacy rather than security. Although not listed here, it's a good idea to become familiar with those controls as well, because the risk management profession is increasingly dealing with privacy and data breach issues. You can find NIST privacy controls in Appendix J of NIST Special Publication 800-53.

NIST controls have different elements or attributes that tell an organization how to apply them, in regard to data sensitivity and security baselines. Without going into great depth on all of these different attributes, we'll explain a few of these entries to help you understand how and when the control is applied. Figure 7-1 shows an example of a control, as listed in Special Publication 800-53.

Note that there are several elements to a control listing. The first element is the control number, in this case, AC-7. This indicates the family control number, along with the title of the control. There's also a description of the control, as well as supplemental

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

- a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and
- b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements:

- (1) **UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK**
[Withdrawn: Incorporated into AC-7].

- (2) **UNSUCCESSFUL LOGON ATTEMPTS | PURGE/WIPE MOBILE DEVICE**

The information system purges/wipes information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging/wiping requirements/techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13.

References: None.

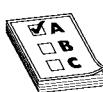
Priority and Baseline Allocation:

P2	LOW AC-7	MOD AC-7	HIGH AC-7
----	----------	----------	-----------

Figure 7-1 An example of a NIST control (AC-7), from NIST Special Publication 800-53

guidance that helps to further detail the control and amplify what the control is about. Some controls also have *control enhancements*, which serve to further refine or restrict the controls, typically in environments that require a higher-level security or more in-depth application of the control. Control enhancements get into the finer details and are more specific than the basic control. There may also be, where appropriate, references that apply to the control; usually these are from other publications or sources that give further guidance on the logic and reasoning behind applying the control, or even best practices associated with it. Many of these references are NIST-related or other types of publications. The last parts of the control that we will cover are the priority and baseline elements. All controls are assigned a particular priority, from P0 through P5, which indicates the relative order in which a control should be applied. Controls marked as a P1, as the highest priority, given budgetary, resource, or environmental constraints, should be applied prior to controls that have a lower-priority rating, such as a P2 or P3. Controls marked as P0 are actually the lowest priority. In the case of the example in Figure 7-1, this control is considered a P2.

The baseline is considered a select level of security or assurance based upon the earlier step in the RMF of security categorization (discussed further in Chapter 8). Properly done, security categorization indicates the level of sensitivity or level of security at which the asset should be protected. These baselines, in NIST, are designated as low, moderate, and high. Sets of controls are assigned to one or more levels of security baselines. In the case of the example in Figure 7-1, the AC-7 control should be applied to all three security baselines, although other controls in other instances may be applied only to medium or high baselines, depending upon the security categorization of the data asset or the needs of the organization. All controls listed in the NIST catalog have these elements; this control is actually one of the simpler examples since many controls have many more control enhancements and may also belong to different levels of security baselines. You should take the time to review and try to understand how controls are laid out in NIST Special Publication 800-53.



EXAM TIP You will likely not be tested on any specific NIST controls; however, it's a good idea to have this knowledge in order to differentiate among the different control frameworks you may see on the exam, as well as for real life.

Along with a comprehensive controls catalog, NIST provides an assessment method for assessing the effectiveness of these controls. NIST Special Publication 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," focuses on how to examine each of the controls from the catalog and how to determine the effectiveness of each. Special Publication 800-53A uses a similar methodology to the one described in Chapter 4; it makes use of interviews with key personnel, examination of documentation, testing, and system observation. It also decomposes each control into manageable, defined subparts, which can be assessed individually. Figure 7-2 shows an example of how to assess a NIST control from the catalog.

AC-6 (10)	LEAST PRIVILEGE PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS						
	<p>ASSESSMENT OBJECTIVE: <i>Determine if the information system prevents non-privileged users from executing privileged functions to include:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;">AC-6(10)[1]</td><td><i>disabling implemented security safeguards/countermeasures;</i></td></tr> <tr> <td>AC-6(10)[2]</td><td><i>circumventing security safeguards/countermeasures; or</i></td></tr> <tr> <td>AC-6(10)[3]</td><td><i>altering implemented security safeguards/countermeasures.</i></td></tr> </table> <p>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</p> <p>Examine: [SELECT FROM: Access control policy; procedures addressing least privilege; information system design documentation; information system configuration settings and associated documentation; list of privileged functions and associated user account assignments; information system audit records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system developers].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing least privilege functions for non-privileged users].</p>	AC-6(10)[1]	<i>disabling implemented security safeguards/countermeasures;</i>	AC-6(10)[2]	<i>circumventing security safeguards/countermeasures; or</i>	AC-6(10)[3]	<i>altering implemented security safeguards/countermeasures.</i>
AC-6(10)[1]	<i>disabling implemented security safeguards/countermeasures;</i>						
AC-6(10)[2]	<i>circumventing security safeguards/countermeasures; or</i>						
AC-6(10)[3]	<i>altering implemented security safeguards/countermeasures.</i>						

Figure 7-2 An example of how to assess a NIST control (AC-6(10)), from NIST Special Publication 800-53A

COBIT

COBIT (previously known as Control Objectives for Information and Related Technology but now typically referred to by its acronym) is a management and governance framework developed and used extensively by ISACA in its various risk management and business process frameworks. COBIT version 5, the current version, has incorporated other ISACA-related frameworks, such as the Risk IT Framework and Val IT. COBIT controls cover various areas, including auditing, compliance, information assurance, IT operations, and security risk management, but typically from a higher-level perspective than you might see in the NIST framework. As a governance and management control framework, COBIT focuses more on the process level, rather than the implementation details. We presented some basic information about COBIT in Chapter 1, but to refresh your memory, the following are the COBIT governance and management domains:

Governance Processes: Evaluate, Direct, and Monitor (EDM)

- EDM01: Ensure Governance Framework Setting and Maintenance
- EDM02: Ensure Benefits Delivery
- EDM03: Ensure Risk Optimization
- EDM04: Ensure Resource Optimization
- EDM05: Ensure Stakeholder Transparency

Management Domain: Align, Plan, and Organize (APO)

- APO01: Manage the IT Management Framework
- APO02: Manage Strategy
- APO03: Manage Enterprise Architecture
- APO04: Manage Information
- APO05: Manage Portfolio
- APO06: Manage Budget and Costs
- APO07: Manage Human Resources
- APO08: Manage Relationships
- APO09: Manage Service Agreements
- APO10: Manage Suppliers
- APO11: Manage Quality
- APO12: Manage Risk
- APO13: Manage Security

Management Domain: Build, Acquire, and Implement (BAI)

- BAI01: Manage Programs and Projects
- BAI02: Manage Requirements Definition
- BAI03: Manage Solutions Identification and Build
- BAI04: Manage Availability and Capacity
- BAI05: Manage Organizational Change Enablement
- BAI06: Manage Changes
- BAI07: Manage Change Acceptance and Transitioning
- BAI08: Manage Knowledge
- BAI09: Manage Assets
- BAI10: Manage Configuration

Management Domain: Deliver, Service, and Support (DSS)

- DSS01: Manage Operations
- DSS02: Manage Service Requests and Incidents
- DSS03: Manage Problems
- DSS04: Manage Continuity
- DSS05: Manage Security Services
- DSS06: Manage Business Process Controls

Management Domain: Monitor, Evaluate, and Assess (MEA)

- MEA01: Monitor, Evaluate, and Assess Performance and Conformance
- MEA02: Monitor, Evaluate, and Assess the System of Internal Control
- MEA03: Monitor, Evaluate, and Assess Compliance with External Requirements

You may notice some similarities to the NIST framework described earlier; controls are broken down into relevant areas, similar to NIST families, and numbered appropriately. Like NIST, these controls have subcategories with lower-level breakdowns. For instance, APO12: Manage Risk breaks down into subprocesses that include the following: APO12.01, Collect Data; APO12.02, Analyze Risk; APO12.03, Maintain a Risk Profile; and so on. While there's no one-to-one matching of COBIT controls to NIST, obviously there are some generalities that could be considered equivalent. In the previous example, COBIT's APO12: Manage Risk process might map loosely to the NIST Risk Assessment (RA) family of controls.



EXAM TIP Remember that COBIT 5 has integrated both Val IT (discussed in the upcoming section) and the Risk IT Framework and serves as the "parent-level" framework for implementing both of these frameworks.

Val IT

A discussion of Val IT may be a moot point in this chapter regarding control frameworks, but it's worth mentioning because it is part of COBIT and works closely with the Risk IT Framework. Val IT is a governance and management framework developed by the IT Governance Institute. Previously used in more of a stand-alone context, it has primarily been absorbed as part of COBIT 5. It consists of three main domains: Value Governance (VG), Portfolio Management (PM), and Investment Management (IM). While its purpose is to obtain business value from IT investments and infrastructures, it can be used as the logistical and mechanical business process and governance framework used to justify control implementation and security programs that affect IT and business risk. It can also be used as guidance in managing IT portfolios and programs, including the security aspects of those programs. The three domains in Val IT are broken up as follows:

Value Governance (VG)

- VG1: Establish informed and committed leadership
- VG2: Define and implement processes
- VG3: Define portfolio characteristics
- VG4: Align and integrate value management with enterprise financial planning
- VG5: Establish effective governance monitoring
- VG6: Continuously improve value management practices

Portfolio Management (PM)

- PM1: Establish strategic direction and target investment mix
- PM2: Determine the availability and sources of funds
- PM3: Manage the availability of human resources
- PM4: Evaluate and select programs to fund
- PM5: Monitor and report on investment portfolio performance
- PM6: Optimize investment portfolio performance

Investment Management (IM)

- IM1: Develop and evaluate the initial program concept business case
- IM2: Understand the candidate program and implementation options
- IM3: Develop the program plan
- IM4: Develop full life-cycle costs and benefits
- IM5: Develop the detailed candidate program business case
- IM6: Launch and manage the program
- IM7: Update operational IT portfolios
- IM8: Update the business case
- IM9: Monitor and report on the program
- IM10: Retire the program

As you can see from the domain processes, Val IT seeks to derive and monitor value from IT; it also closely corresponds with other processes discussed throughout this book that help to control and minimize both IT and business risk, such as the system development life cycle (SDLC) and portfolio and project management processes.



EXAM TIP While you won't be expected to know Val IT's domains and breakdowns in detail, it's a good idea to at least have a basic understanding of the framework and its purpose.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security requirements levied on merchants that process credit card transactions. The standard was developed jointly by the major payment card industry players, including Discover, Visa, MasterCard, and American Express. The standard was developed in an effort to impose security requirements and controls on retailers (merchants and service providers) to reduce credit card fraud and identity theft. Note that PCI-DSS is not a law; rather, it is an effort by the credit card industry to self-regulate. While not a law, it does have the

Control Objective	Requirement
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Table 7-3 PCI-DSS Control Objectives and Requirements

effect of being mandatory governance requirements; retailers must comply with PCI-DSS to be allowed to process credit cards from the major industry brands. A few U.S. states, however, have codified into their laws the use of PCI-DSS standards.

The PCI-DSS (currently in version 3.1 as of this writing) is a set of 6 control objectives, broken down into 12 major requirements, which are further broken down into subrequirements. Table 7-3 lists the basic PCI-DSS requirements.

On the surface, these objectives and requirements don't seem to go much in depth. Understand, however, that PCI-DSS further decomposes the requirements into detailed processes and procedures. The standard also provides guidance for testing at the control level. For example, requirement 5, "Protect all systems against malware and regularly update anti-virus software or programs," breaks down into four subrequirements, some of which break down even further. Requirement 5.1.2, continuing the example, specifies continuous monitoring and evaluation of hosts for malware threats. All in all there are actually more than 200 subrequirements, the equivalent of controls.



EXAM TIP You likely won't be asked any control-specific questions on the exam, but you should keep in mind where it's applicable: to merchants and retailers that process credit card transactions. You can find more detailed information on the PCI-DSS standards at the website of the PCI Security Standards Council at https://www.pcisecuritystandards.org/security_standards/.

Other Control Frameworks

We've only scratched the surface of the many different control sets and frameworks available to risk practitioners and organizations. In some cases, an organization may settle on one control framework, but this usually isn't the case. Many times an organization will have additional control sets it must use to meet a variety of governance requirements or to apply to specific parts of its business. Hospitals, for example, must abide by HIPAA regulations, which recommend (but do not require) the use of NIST controls. Simultaneously, they may also be subject to PCI-DSS controls since they likely use credit cards to process financial transactions for patient billing. Other governance may require that they adhere to other control frameworks, such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standards. Obviously, we can't cover all the potential control sets and frameworks you will encounter in the field, but we've covered the major ones and will touch upon a few others of significance in the following sections.

ISO/IEC Controls

Although we've primarily discussed different control sets that originate in the United States (such as PCI-DSS and NIST), most of the various control frameworks map to, and in some cases, originate from standards used worldwide and developed by internationally respected governing bodies. In Chapter 4, we briefly mentioned some of these standards, including those from ISO and IEC. The ISO and IEC produce information technology standards that are used internationally, including several that apply to information security and risk management. You may see individual standards prepared by each of these organizations, but you may also see combined standards, usually indicated as ISO/IEC for those standards that are jointly developed. We discussed standards that applied more specifically to risk assessments in Chapter 4, but there are also ISO/IEC standards that are essentially control requirements. Two examples are ISO/IEC 27001, "Information Technology—Security Techniques—Information Security Management Systems—Requirements," and ISO/IEC 15408, "Information Technology—Security Techniques—Evaluation Criteria for IT Security" (more widely known as the Common Criteria).

In addition to the mapping that the NIST Cybersecurity Framework provides to different control sets and requirements (discussed in an upcoming section), NIST Special Publication 800-53, the NIST control set, provides a convenient mapping as well to both ISO/IEC 27001 and 15408 control sets in its appendixes. Figure 7-3 shows a snippet mapping NIST controls to ISO/IEC 27001, and Figure 7-4 shows the reverse mapping. Figure 7-5 illustrates the mapping of ISO/IEC 15408 to the NIST 800-53 controls. All three figures were taken from NIST Special Publication 800-53.

In examining these control mappings, a few points should stand out. First, there's not necessarily a straight one-to-one mapping of controls. In some cases, the requirements for a given control in a control set may map to one, many, or even none of the other control set's controls. Second, controls tend to follow similar patterns and requirements, such as acceptable use, password requirements, media storage, encryption, and so on. Most controls from the various control sets have these commonalities because all of them

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.6.1, A.11.7.1, A.11.7.2, A.12.3.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.2, A.11.5.5, A.11.5.6
AC-3	Account Enforcement	A.7.2.2, A.10.6.1, A.10.7.3, A.10.7.4, A.10.8.1, A.10.9.1, A.10.9.2, A.10.9.3, A.11.2.2, A.11.5.4, A.11.6.1, A.12.4.3, A.15.1.3
AC-4	Information Flow Enforcement	A.7.2.2, A.10.7.3, A.10.8.1, A.11.4.5, A.11.4.7, A.12.5.4
AC-5	Separation of Duties	A.10.1.3
AC-6	Least Privilege	A.11.2.2, A.11.4.1, A.11.4.4, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Logon Attempts	A.11.5.1
AC-8	System Use Notification	A.6.2.2, A.11.5.1, A.15.1.5
AC-9	Previous Logon (Access) Notification	A.11.5.1
AC-10	Concurrent Session Control	None
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5

Figure 7-3 NIST controls mapped to ISO/IEC 27001 (from NIST Special Publication 800-53)

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
<i>Note: An asterisk (*) indicates the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>	
A.12.3 Backup	
A.12.3.1 Information backup	CP-9
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	AU-3, AU-6, AU-11, AU-12, AU-14
A.12.4.2 Protection of log information	AU-9
A.12.4.3 Administrator and operator logs	AU-9, AU-12
A.12.4.4 Clock synchronization	AU-8
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	CM-5, CM-7(4), CM-7(5), CM-11
A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.12.6.2 Restrictions on software installation	CM-11
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	AU-5*
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.1.2 Security of network services	CA-3, SA-9

Figure 7-4 ISO/IEC 27001 control requirements mapped to NIST 800-53 controls (from NIST Special Publication 800-53)

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FAU_GEN.2	Security Audit Data Generation User Identity Association	AU-3	Content of Audit Records
FAU_SAA.1	Security Audit Analysis Potential Violation Analysis	SI-4	Information System Monitoring
FAU_SAA.2	Security Audit Analysis Profile-Based Anomaly Detection	AC-2(12)	Account Management <i>Account Monitoring/Atypical Usage</i>
		SI-4	Information System Monitoring
FAU_SAA.3	Security Audit Analysis Simple Attack Heuristics	SI-3(7)	Malicious Code Protection <i>Non Signature-Based Protection</i>
		SI-4	Information System Monitoring
FAU_SAA.4	Security Audit Analysis Complex Attack Heuristics	SI-3(7)	Malicious Code Protection <i>Non Signature-Based Protection</i>
		SI-4	Information System Monitoring
FAU_SAR.1	Security Audit Review Audit Review	AU-7	Audit Reduction and Report Generation
FAU_SAR.2	Security Audit Review Restricted Audit Review	AU-9(6)	Protection of Audit Information <i>Read Only Access</i>
FAU_SAR.3	Security Audit Review Selectable Audit Review	AU-7	Audit Reduction and Report Generation
		AU-7(1)	Audit Reduction and Report Generation <i>Automatic Processing</i>
		AU-7(2)	Audit Reduction and Report Generation <i>Automatic Sort and Search</i>
FAU_SEL.1	Security Audit Event Selection	AU-12	Audit Generation

Figure 7-5 ISO/IEC 15408 controls mapped to NIST controls (from NIST Special Publication 800-53)

in some way trace back to the three goals of security (confidentiality, integrity, and availability), as well as the supporting elements that include identification, authentication, and authorization. This is generally true regardless of which security control framework you examine.



NOTE You'll find that many control frameworks are derived from and map to the ISO/IEC standards. They are international standards and can be applied across most industries and market spaces.

SANS Critical Security Controls

As an international security professional, training, and research organization, SANS (which stands for SysAdmin, Audit, Networking, and Security but is referred to officially only as the SANS Institute) has developed and maintains the Top 20 Critical Security Controls (CSC). These controls were developed based upon recommendations from government and industry as high-priority measures organizations should take to protect

information systems and data. The Council on CyberSecurity (CCS) currently manages these controls, listed here:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defenses
- Application Software Security
- Wireless Access Control
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defense
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Account Monitoring and Control
- Data Protection
- Incident Response and Management
- Secure Network Engineering
- Penetration Tests and Red Team Exercises

Obviously, these 20 controls map to other control frameworks we've discussed but aren't intended to replace them. They are simply recommendations for organizations to implement as the controls that can be the most effective in protecting systems and data. You can find more information on the Critical Security Controls at www.sans.org/critical-security-controls/.



TIP The SANS CSC Critical Security Controls cover only the top 20 "critical" controls considered to be the most important in an information security and risk management program, as recommended by the industry. They do not go into as much depth as other control catalogs.

Australian Signals Directorate “Strategies to Mitigate Targeted Cyber Intrusions”

The Australian Signals Directorate have developed a set of “top 35” security controls (referred to as *mitigation strategies*). This document is called “Strategies to Mitigate Targeted Cyber Intrusions,” and it prioritizes controls such as application whitelisting, patching, restriction of administrative privileges, and so on. The document offers predicted levels of security effectiveness (in subjective terms of Essential, Excellent, Good, and Average), as well as predicted user resistance to these controls, up-front resource cost, and maintenance cost (all in subjective terms of High, Medium, and Low). The strategies also define what function the mitigation supports (for example, detecting intrusions, preventing code execution, stopping network propagation, and preventing data exfiltration). The entire set of mitigation strategies (controls) was updated in 2014 and can be viewed at www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm.

ISA

The International Society of Automation (ISA) has developed standards and controls that apply to automated systems, such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA). Since so many of these systems are now using traditional computers and networks to process and carry data, they are also subject to the same attacks, data modification, loss, and other risks as traditional information systems and data. Examples of the many uses of industrial control and SCADA systems include those found in nuclear power plants, electric power facilities, production factories, medical devices, and other critical infrastructures.

Obviously, then, these types of systems require at least the same level of risk management and protection through security controls as traditional systems. While some traditional security controls and frameworks have been applied to these types of systems (particularly NIST controls), there are also specific control sets developed by that industry that address vulnerabilities. There are particular standards and controls that ISA has developed that specifically can be applied to information security requirements. While ISA, in conjunction with the American National Standards Institute (ANSI), develops a wide variety of standards, some dealing with safety, electrical equipment, and so on, specific security-related ISA standards include the ISA 62443 series (for example, ISA 62443-2-1:2009 and ISA 62443-3-3:2013).



NOTE While the ISA controls specifically apply to ICS and SCADA systems, they are meant to be supplemented by other controls, such as those found in NIST.

Exercise 7-1: Choosing Control Standards to Use

Determine from your management and governance which control standards your organization uses. Are they any of the ones we’ve discussed? Should your organization be looking at multiple control sets, based upon different forms of governance? If your organization does not currently use any control standards, which ones would you suggest to management?

Cybersecurity Framework from NIST

Interestingly enough, NIST—through its February 2014 “Framework for Improving Critical Infrastructure Cybersecurity” publication (also known as the Cybersecurity Framework)—has done a great job of decomposing five key security-related functions into categories and subcategories. These five functions are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The framework also provides formally defined designators that can be used by an organization to ensure standardization. In Figure 7-6, there’s an example directly taken from the cybersecurity framework that shows how this decomposition of security functions occurs. Notice the similarities in functions and categories to the material we have been discussing throughout the book.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 7-6 NIST’s cybersecurity functions and categories (from the “Framework for Improving Critical Infrastructure Cybersecurity” publication, February 2014)

Function	Category	Subcategory	Informative References
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	<ul style="list-style-type: none"> • COBIT 5 BA101.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
		RS.CO-1: Personnel know their roles and order of operations when a response is needed	<ul style="list-style-type: none"> • ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.4 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-2: Events are reported consistent with established criteria	<ul style="list-style-type: none"> • ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A16.1.2 • NIST SP 800-53 Rev. 4 AU-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	<ul style="list-style-type: none"> • ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	<ul style="list-style-type: none"> • ISA 62443-2-1:2009 4.3.4.5.5 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 PM-15, SI-5

Figure 7-7 Mapping functions to subcategories and controls in the NIST Cybersecurity Framework (from the “Framework for Improving Critical Infrastructure Cybersecurity” publication, February 2014)

The framework, taking into account that different organizations use different control frameworks and control sets, also provides for a convenient mapping to various control libraries, some of which we have discussed. Figure 7-7 shows how the cybersecurity framework maps its critical security functions to a variety of control sets and frameworks, including NIST, COBIT 5, ISO/IEC, ISA, and others. The purpose of this mapping is to help provide standardization to organizations that use different control sets to map to defined security functions. This can help organizations convert to equivalent control sets when dealing with auditors or partners and provide a path forward when determining risk strategy and management. It also helps users who may be under different governance requirements to use multiple control sets to leverage their efforts to meet the requirements of more than one control set simultaneously.

Chapter Review

In this chapter, we went over the basic concepts of controls and examined different control frameworks. Controls are security measures implemented to ensure that processes are performed to a certain standard, degree, or depth; they offer detailed guidance relevant to a specific requirement. Controls directly address a known risk or vulnerability in a given system, environment, or program. Controls can be classified as administrative, technical, and physical controls. They can also be classified in terms of function, such as deterrent, preventative, or corrective controls. Controls are used to reduce likelihood and impact factors in risk and protect assets by reducing vulnerabilities.

We examined the NIST control framework from Special Publication 800-53, which is a comprehensive catalog of controls covering all aspects of information system and data security. We defined the different attributes of a NIST control, such as the baseline and priority aspects. We also looked at its counterpart, Special Publication 800-53A, which provides guidance on assessing those same controls.

We then looked at COBIT, a management and governance framework, developed and used extensively by ISACA in its various risk management and business process frameworks. COBIT controls cover various areas, including auditing, compliance, information assurance, IT operations, and security risk management, but at a higher-level perspective. COBIT version 5 also incorporates the Val IT governance and management framework. Val IT consists of three main domains: Value Governance (VG), Portfolio Management (PM), and Investment Management (IM); it is used to help obtain business value from IT infrastructure.

PCI-DSS is a set of security requirements levied on merchants that process credit card transactions, developed by major card providers. Although not a law in itself, it is considered mandatory for retailers and service providers that process credit card transactions and has actually been incorporated into several U.S. state laws. PCI-DSS controls are broken down into 6 control objectives and 12 requirements, which are further broken down into specific controls.

We also looked at a variety of other control frameworks, such as international standards promoted by ISO and IEC. These included ISO/IEC 27001 and ISO/IEC 15408; we demonstrated how these standards and other control sets have much in common and can often be mapped to each other, allowing for standardization and cross-utilization. The SANS Institute's Top 20 Critical Security Controls were developed based upon recommendations from government and industry as high-priority measures that organizations should take to protect information systems and data. They include controls that address areas such as device inventory, secure configuration, and application software security, to name just a few. In another example of a non-U.S. control standard, we briefly looked at the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions, a list of 35 mitigation strategies (security controls). This standard covers critical control areas such as application whitelisting, patching, and restriction of administrative privileges, among others. Then we took a brief look at standards and controls that apply to automated systems, such as industrial control systems and supervisory control and data acquisition. Specifically, examples of these specialized types of controls are those developed by the International Society of Automation.

Finally, we looked at NIST's Cybersecurity Framework, which defines five key security-related functions, divides them into categories and subcategories, and also maps them to various control libraries. These five functions are as follows: Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The functions can be mapped to almost any of the various control sets discussed throughout the book, grouping similar functions together and identifying the controls associated with those functions.

Review Questions

1. Security measures implemented to ensure that processes are performed to a certain standard, degree, or depth are called _____.
 - A. Risks
 - B. Objectives
 - C. Requirements
 - D. Controls
2. All of the following statements describe characteristics of controls except which one?
 - A. Controls are defined and implemented in terms of addressing a specific vulnerability or deficiency in asset protection.
 - B. They are used to specify what measures should be taken to ensure security and reduce risk.
 - C. Controls are designed to be effective in completely eliminating a particular risk.
 - D. Specific control sets may be required by legal governance.
3. Which of the following would be considered an administrative control?
 - A. Documented policy on firewall rules and exceptions
 - B. Physical or logical placement of the firewall within the IT infrastructure
 - C. Rule configuration on the firewall
 - D. Traffic exceptions listed in the firewall ruleset
4. Which of the following would be considered a preventative control?
 - A. Warning sign stating that unauthorized personnel may not enter a restricted area
 - B. A security fence
 - C. A server's audit logs
 - D. A full data backup used to restore a server after a disk failure
5. Which of the following elements of risk can controls be used to reduce? (Choose two answers.)
 - A. Likelihood
 - B. Impact
 - C. Threat
 - D. Threat agent

6. Which of the following is the catalog of controls published by the National Institute of Standards and Technology?
 - A. ISO/IEC 27001
 - B. ISO/IEC 15408
 - C. Special Publication 800-53
 - D. Special Publication 800-53A
7. Which control family is *not* included in NIST's 18 families of controls?
 - A. Privacy
 - B. Personnel Security
 - C. Media Protection
 - D. Incident Response
8. Which of the following management and governance frameworks incorporates both the Risk IT Framework and the Val IT framework?
 - A. ISO/IEC 27001
 - B. SANS Top 20 CSC
 - C. NIST SP 800-53
 - D. COBIT 5
9. All the following are domains of the Val IT framework except which one?
 - A. Value Governance
 - B. Security Management
 - C. Portfolio Management
 - D. Investment Management
10. Which control framework is not normally legally required but is mandated by the members of its industry and is imposed on merchants and retailers?
 - A. ISO/IEC 15408
 - B. NIST SP 800-53
 - C. PCI-DSS
 - D. Val IT
11. Which of the following control objectives is specific to PCI-DSS?
 - A. System and Services Acquisition
 - B. Build and Maintain a Secure Network and Systems
 - C. Manage Business Process Controls
 - D. Monitor, Evaluate, and Assess Performance and Conformance

12. Which of the following control sets are considered internationally developed and accepted standards? (Choose two answers.)
- A. NIST SP 800-53
 - B. COBIT 5
 - C. ISO/IEC 27001
 - D. ISO/IEC 15408
13. Which of the following control standards is commonly known as part of the Common Criteria?
- A. ISO/IEC 15408
 - B. ISO/IEC 27005
 - C. ISO/IEC 31010
 - D. ISO/IEC 27001
14. Which of the following control libraries was developed based upon recommendations from government and industry as high-priority measures that organizations should take to protect information systems and data?
- A. SANS Top 20 Critical Security Controls
 - B. NIST SP 800-53A
 - C. COBIT 5
 - D. ISO/IEC 27001
15. Which of the following sets of terms describes how the Australian Signals Directorate offers predicted levels of security effectiveness for its controls?
- A. High, Medium, and Low
 - B. Essential, Excellent, Good, and Average
 - C. Levels 1–10
 - D. Very Low, Low, Moderate, High, and Very High
16. Which control framework might be specifically applied to industrial control systems?
- A. COBIT 5
 - B. ISO/IEC 15408
 - C. ISA 62443-3-3:2013
 - D. Australian Signals Directorate’s “Strategies to Mitigate Targeted Cyber Intrusions”

17. Which the following is *not* one of the five key security-related functions defined in NIST's Cybersecurity Framework?
- A. Identify
 - B. Protect
 - C. Detect
 - D. Manage
18. Which of the following control libraries contains BAI04: Manage Availability and Capacity?
- A. COBIT 5
 - B. NIST SP 800-53
 - C. ISO/IEC 27001
 - D. ISA 62443-3-3:2013
19. Which of the following can be used to assess controls under NIST SP 800-53?
- A. NIST SP 800-37
 - B. NIST SP 800-30
 - C. NIST SP 800-53A
 - D. FIPS 199
20. Which of the following control sets would AC-7 belong to?
- A. NIST SP 800-53
 - B. COBIT
 - C. PCI-DSS
 - D. ISA 62443-2-1:2009

Answers

1. D. Controls are security measures implemented to ensure that processes are performed to a certain standard, degree, or depth.
2. C. Controls are designed to be effective, but they can never completely eliminate a particular risk; they can only reduce or mitigate it.
3. A. A documented policy on firewall rules and exceptions would be considered an administrative control.
4. B. A security fence would be considered a preventative control since it actually prevents unauthorized persons from entering an area. A sign, by itself, might deter a person but could not prevent that person from entering an area. Audit logs are detective controls. Backups used *after* a failure would be a recovery control.

5. **A, B.** Controls can be used to reduce likelihood of a threat exploiting a vulnerability or the impact on the asset if a threat does exploit the vulnerability. Controls cannot reduce threats or threat agents.
6. **C.** Special Publication 800-53 is the catalog of controls published by the National Institute of Standards and Technology.
7. **A.** Privacy controls are *not* included in NIST's 18 families of controls, although they are included in SP 800-53 as a separate appendix of 8 control families.
8. **D.** COBIT 5 is a management and governance framework, developed by ISACA, which incorporates both the Risk IT Framework and Val IT framework.
9. **B.** Security Management is not one of the domains of the Val IT framework.
10. **C.** The PCI-DSS control framework is not normally legally required but is mandated by the members of the card payment industry and is imposed on merchants and retailers.
11. **B.** Build and Maintain a Secure Network and Systems is a control objective specific to PCI-DSS.
12. **C, D.** Both ISO/IEC 27001 and ISO/IEC 15408 are considered internationally developed and accepted standards.
13. **A.** ISO/IEC 15408 is commonly known as part of the Common Criteria.
14. **A.** The SANS Top 20 Critical Security Controls were developed based upon recommendations from government and industry as high-priority measures that organizations should take to protect information systems and data.
15. **B.** The Australian Signals Directorate offers predicted levels of security effectiveness for its controls in terms of Essential, Excellent, Good, and Average.
16. **C.** ISA 62443-3-3:2013, developed by the International Society of Automation, specifically applies to industrial control systems.
17. **D.** The Manage function is *not* one of the five key security-related functions defined in NIST's Cybersecurity Framework, which consists of the following: Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC).
18. **A.** BAI04: Manage Availability and Capacity is part of the COBIT 5 library.
19. **C.** NIST SP 800-53A was specially developed to assess controls under NIST SP 800-53.
20. **A.** AC-7 is part of the NIST SP 800-53 control set, specifically under the Access Control family.

This page intentionally left blank

Designing and Implementing Controls

In this chapter, you will:

- Learn business perspectives of information controls
- Examine the information system security engineering process and its relationship to control design and implementation
- Review effective control design principles
- Learn about information categorization and how it affects control selection
- Learn about implementing information controls

In Chapter 7 we covered the basics of controls, and in previous chapters we've discussed how to assess controls as part of the overall risk assessment process, but we haven't yet covered the finer points of how controls are designed and implemented. In this chapter, we'll discuss controls from the design and implementation perspectives. We will look at business perspectives on information controls, as well as the value of business cases in justifying control implementation or modification. We'll also cover these controls and frameworks from the governance view, including the governmental, financial, and healthcare views. You'll learn about the information system security engineering (ISSE) process and how it affects the control life cycle, as well as how controls are selected to perform specific functions in protecting systems and data. We'll cover some of the principles of effective control design, as well as how to implement controls.

The CRISC exam objectives that we will continue to cover during this chapter include the following task statements:

- 2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
- 2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment
- 3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level

- 3.4 Ensure that control ownership is assigned to establish clear lines of accountability
- 3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution

Notice that we've also partially covered these objectives in previous chapters, but more in the context of discussing risk assessment than control design and implementation. We'll touch on some previously discussed topics, as well as introduce some new concepts to round out the discussion of these objectives. Like in the previous chapter, you'll find that this chapter covers more material than you might find on the exam; again, it's important that you understand foundational and conceptual knowledge about control design and implementation both for the exam and in the real world when dealing with information systems and their controls. And, to reiterate, this book is intended to be not only a study guide for the exam but also a comprehensive reference you will use even after you have passed the CRISC exam.

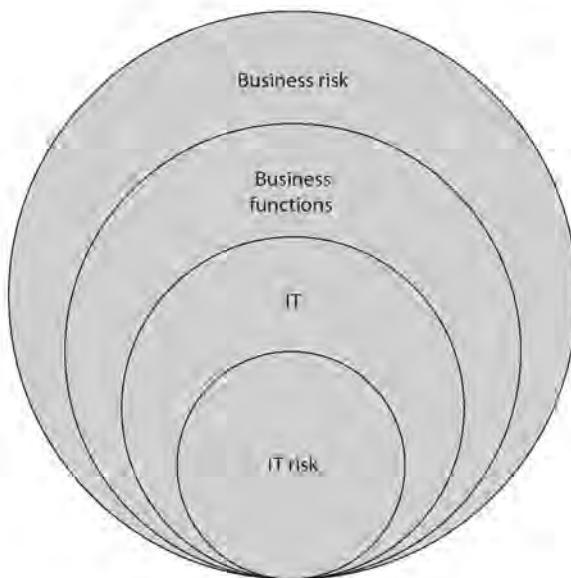
Business Perspectives of Controls

As has been emphasized throughout this entire book, IT risk is only a subset of the entire sum of the business risk the organization incurs. Likewise, IT controls serve to limit IT risk, so the overall business risk can be reduced. Therefore, from a business perspective, IT controls should contribute to the overall reduction of business risk in some fashion. The organization should consistently be able to trace an IT control to an IT asset, to an IT risk, and then on to a business risk to justify the existence or implementation of the IT control in the first place. Often, because of the expense involved or because higher-level executives don't always make the connection between IT risk and business risk, a business case must be made for controls, which I'll discuss next. Figure 8-1 shows a representation of the relationships between IT risk, IT, business functions, and business risk, all of which will be discussed throughout this chapter.

Business Cases for Controls

Although it may seem to be common sense to implement a control to offset an IT risk, often a concrete business case must be made for implementing controls, particularly when controls cost more than an asset is worth or are not as effective in reducing the risk as the organization would like. There may be other factors, however, that necessitate the implementation of the control that the business must evaluate on a case-by-case basis. Some of these factors include compliance with laws or other governance, compliance with partner agreements or contracts, industry requirements, or data sensitivity issues. That's why making business cases for IT controls may be necessary from time to time to highlight these requirements or justify the expense and effectiveness of the control. The next few sections will talk about making business cases for IT controls.

Figure 8-1
Relationship of IT
risk, IT, business
functions, and
business risk



Security Goals and Supporting Concepts

Controls aren't selected simply because they sound cool to implement. They are usually selected because of a need to mitigate a particular risk, support a particular security goal, or even support one of the basic tenets of security. Some controls might support confidentiality, integrity, and availability; others may support identification, authentication, authorization, nonrepudiation, or accountability. For example, to support confidentiality, encryption controls on data at rest and data in transit may be required. There's also corresponding risk that these encryption controls can mitigate, and that risk is of unauthorized access to data. Including the security goals that a control supports, as well as the risks that it mitigates, in a business case is essential to getting approval to implement a control. It's also critical to identify any impacts to the asset's organization if the control is not implemented. This ensures that senior managers and executives are aware of the consequences of not implementing the control.

Due Diligence, Due Care, and Liability

As soon as you start talking about due diligence, due care, and liability issues, then the question changes from "How can we afford to implement these controls?" to "How can we afford *not* to?" When making a business case to implement various controls, these three issues should be looked at carefully, in terms of how they will impact an organization from a legal perspective. Organizations could be charged with criminal neglect or find themselves victim to civil suits if they have not implemented the proper information security controls. Even if governance (discussed next) does not require an organization to implement a particular control or safeguard, that doesn't necessarily mean that this excuse will get them out of legal trouble. For example, even if an organization isn't

required to encrypt data at rest, in the event of a serious data breach, the organization may face legal ramifications by not following this industry-accepted practice.



TIP Don't neglect discussing liability issues in a business case. Often this could be the make-or-break decision for implementing a control since liabilities could subject the business to legal fees and fines that cost far more than the control itself.

Governance

Obviously, governance can be used to drive a business case as well. Since governance can't easily be ignored, even in the face of limited resources, it's worthwhile to include governance requirements for controls in any business case that supports implementing particular information system controls. Governance requirements can be used to justify the cost, as well as the need to implement security controls. The particular types of governance your organization is subject to will need to be carefully examined before inclusion in any business case to ensure that they are properly interpreted. We'll discuss particular types of governance later in this chapter.



NOTE Like the liability issues mentioned earlier, governance can also be a make-or-break decision for implementing a control since the organization may be legally required to implement certain data protection controls and failure to do so may be breaking the law. You definitely want to include any potential governance or legal compliance issues in business cases because senior management needs to be aware of any potential compliance issues involved with the decision.

Economy and Efficiency of Use

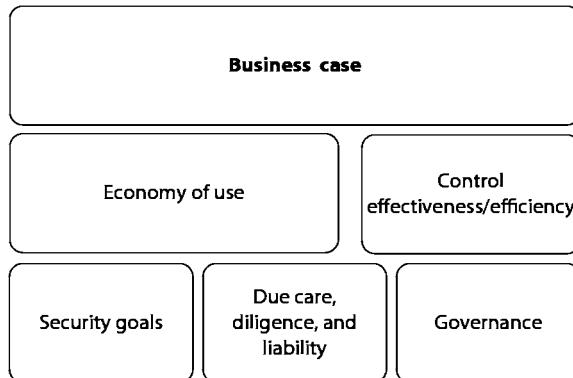
Although design principles of efficiency and economy of use are covered later in this chapter, they're worth mentioning here simply because they can be effective in presenting a good business case for implementing controls. The business case should discuss why a particular control is effective in mitigating a particular risk and, if possible, should discuss control efficiency when compared with other potential control choices that might be less costly. The business case should also try to examine controls that follow the principle of economy of use; that is, they can be used for more than one system or to mitigate more than one risk. We'll cover economy of use of controls a bit more later in the chapter. These two topics, in the context of a business case, relate more to a return-on-investment consideration of controls more so than anything else. Figure 8-2 sums up the factors we've discussed here that are used to support a business case.



EXAM TIP Keep in mind the different considerations you should include in a business case: support for security goals, governance, due care, diligence, liability; as well as control effectiveness, efficiency, and economy of use. The business case should also discuss the pros and cons of implementing a control versus not implementing the control, as well as the risk involved.

Figure 8-2

Factors used to support a business case



Regulatory Guidance and Controls

Control implementation is heavily influenced by governance. Often, different governance requirements mandate the use of specific control frameworks. Some, on the other hand, are concerned with meeting security requirements and leave the control framework decision to the organization, based upon their particular needs. This section will discuss the particulars of different regulatory requirements and the control frameworks they prescribe. Note that we are covering only a few of the major, common governance vehicles.

Payment Card Industry Data Security Standard

As mentioned in Chapter 7, the Payment Card Industry Data Security Standard (PCI-DSS) standards aren't necessarily mandatory legal or regulatory requirements that come from the government (although a few U.S. states have adopted them as mandatory) but are industry-developed standards that are imposed on merchants and retailers that process credit card payments. So, this governance is more of a self-regulation type of governance the credit card payment industry imposes on itself. This is a rare example of such self-regulation; so many other market segments and industries don't develop any mandatory governance for its members but may simply (at best) publish recommended guidelines that its members may or may not choose to adopt at their discretion. The PCI Security Standards Council develops the PCI-DSS standards, as well as standards for vendors that supply point-of-sale (POS) devices (PIN pad terminals, for example), as well as the Payment Application Data Security Standard (PA-DSS), which applies to the system applications that actually process the payment transactions. It's worth noting that the PCI Security Standards Council does not enforce the PCI-DSS standards or levy sanctions on merchants that don't comply with the standards. It is the specific card provider (for example, Visa, MasterCard, and so on) that enforces the standards and imposes penalties on individual noncompliant merchants.

Along with this self-imposed governance, the PCI-DSS standards are, in fact, also controls, as described in Chapter 7. The controls are divided into 6 control objectives, which are further divided into 12 major requirements, which are further decomposed into more than 200 subrequirements; these are considered the controls of the standard.

PCI-DSS controls are often used alongside other controls mandated by other governance since many merchants are governed by other requirements and take credit card payments incidental to their primary business (think of a doctor's office, covered by HIPAA governance, which processes credit card payments for medical services rendered, for instance).



EXAM TIP PCI-DSS standards are typically not legally mandatory, except in a few states. The standards are industry imposed; they are not actually laws or regulations unless they have been mandated for use by a particular law.

The Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) prescribes security requirements in the form of the HIPAA Security Rule. The Security Rule (45 CFR, Part 160 and Subparts A and C of Part 164) is broken up into subrequirements, called *HIPAA security standards*, which detail at a bit of a higher level the particular security requirements that hospitals, clinics, and other covered entities (the HIPAA term for any organization, usually one that deals with personal health information [PHI], that must comply with HIPAA requirements). The security standards really are not controls in themselves but are requirements for securing electronic personal health information (EPHI). HIPAA categorizes its requirements much like other security frameworks, such as NIST, ISO, and PCI-DSS, in terms of Administrative, Physical, Technical, Organizational, and Documentation requirements. All in all, there are 67 HIPAA security standards, covering the typical range of requirements, from appointing a senior security official to formulating access control policy, securing facilities that house EPHI systems, and encrypting EPHI during transmission, for instance. An example of a HIPAA security standard would be §164.308(a)(1)(i), “Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.”

Note that this seems a bit broad and ambiguous; the rule doesn't exactly say which policies and procedures you must develop and implement to comply with the standard. Other rules do go a bit further and amplify this requirement somewhat, but all the standards are typically broad and don't get into the details of implementation. That's where more detailed controls would come into play. HIPAA does not require any particular control set or framework but does highly recommend that the NIST control library, found in NIST SP 800-53, be used to support the implementation of the security standards. HIPAA guidance doesn't go into a great deal of depth on exactly how to implement the NIST controls to support compliance with the security standards, but NIST has published NIST Special Publication 800-66, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” which offers guidance on how to use the NIST controls (as well as the RMF) to support HIPAA compliance. The publication also loosely maps the HIPAA security standards to the SP 800-53 controls. Again, the use of NIST controls is not mandatory under HIPAA but is highly recommended.



EXAM TIP HIPAA does not mandate any particular control framework but recommends NIST controls.

The Gramm–Leach–Bliley Act

The Gramm–Leach–Bliley Act (GLBA) was passed with the primary goals of allowing certain types of corporate structure changes, such as mergers, and changing the conflict-of-interest requirements for company officers. It also includes clauses that provide for the safeguarding of client financial and personal information. This falls under the GLBA Safeguards Rule, which requires, among other things, a senior person formally appointed to manage information security, analyze and manage risk, and develop and maintain an information security program. Parts of the act also attempt to reduce the risk of social engineering by reducing pretexting, that is, by gaining protected personal or financial information under false pretenses through phishing and other social engineering techniques. The act requires that covered financial institutions create and maintain a formalized, written information security plan, which addresses, in particular, managing and training employees, securing information systems, and detecting and managing system failures.

GLBA describes in detail what requirements organizations must fulfill to comply with the act (see <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>) but does not specifically call out any particular control framework. In reviewing these requirements, you can see how a variety of controls might be implemented to meet the Safeguard Rule. Obviously, both the NIST and COBIT frameworks might be used to meet these requirements, as well as PCI-DSS, as needed.

The Sarbanes–Oxley Act of 2002

The Sarbanes–Oxley (SOX) Act of 2002 was enacted to answer the growing tide of corporate accounting and auditing scandals, such as the infamous Enron accounting scandal, and enforce new requirements of protection, disclosure, and auditing of financial information. It applies to publicly held companies, as well as other classifications of financial institutions. It also applies to accounting and auditing firms. SOX implements several key pieces of legislative requirements, again primarily focusing on auditor independence, data protection and preservation, and accounting practices. For information security professionals, this equates to ensuring protections for sensitive data and systems, particularly focusing on access control and data integrity protections, as well as auditing system and data access. It also means that information security personnel maintain accurate documentation of the same.

Information security requirements in general fall under section 404 of the act, which broadly covers auditing internal controls. Like GLBA, SOX does not require any specific control framework but is more concerned with open, transparent control audit practices and accountability, regardless of which control framework is used. COBIT is often used to support SOX compliance, as are the American Institute of Certified Public Accountants' Statements on Auditing Standards. Many of the SOX requirements also map to the controls of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, which, if you remember from Chapter 1, has been integrated into COBIT 5 control requirements. In addition to these governance and management frameworks, for detailed technical control requirements, organizations often also use NIST and PCI-DSS.



NOTE SOX compliance primarily involves auditing, particularly processes associated with financial accounting. However, information systems and data are also subject to auditing to ensure data integrity. SOX also primarily covers management and governance processes, instead of technical controls.

The Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) (44 U.S.C. §§ 3541-3549) was enacted in 2002 to require U.S. government agencies to implement comprehensive cybersecurity measures to protect U.S. government systems and data. FISMA tasks NIST with developing standards and guidelines for agencies to use in fulfilling the requirements of the act. As such, federal agencies are required to use the NIST control framework at a minimum, as well as other control frameworks as required by other regulations the agencies are subject to (for example, HIPAA, SOX, and so on). Until recently, the U.S. Department of Defense (DoD) implemented its own control framework under the Defense Information Assurance Certification and Accreditation Program (DIACAP). DIACAP used controls similar in many respects to NIST but were specifically geared toward DoD needs, such as specific types of national intelligence and weapons systems. Since March 2014, however, the DoD has been directed to transition to the NIST RMF, as well as its related control library. The application of NIST controls to specialized systems is achieved through the use of specially developed *overlays*, which are control baselines specific to systems of a military or intelligence nature.



NOTE All U.S. government federal agencies are subject to FISMA, which in turn requires adherence to NIST standards and use of the RMF.

Business Functions and Controls

Controls are implemented to protect assets, but from a business perspective, controls are also there to protect the integrity and continuity of business functions. Business functions, such as sales, human resources or accounting processes, or even processes that take place with third parties, are all also considerations when designing and implementing controls. Protecting assets is of course a priority, but assets don't exist simply for their own benefit. They exist to support business goals, processes, and functions. So, considering different business functions is also part of the process of determining how to design and implement security controls. This section will cover various functions and how controls serve to support those functions. You'll find that for the most part controls aren't always specific to a particular function or area; design principles that we'll discuss later in the chapter dictate that controls be designed in such a way to maximize their benefit across multiple functions, business areas, and assets.

Internal Functions

Internal functions are those that are specific to the internal workings of a business organization. This could include functions such as human resources, accounting, security,

production, marketing, and so on. Controls may be necessary to protect information systems within the organization, typically from an access control perspective. In other words, based upon the sensitivity of systems and information, different employees or personnel may not have access to all systems or data within an organization. It's not uncommon to find accounting servers and data, for example, encrypted and protected by internal firewalls to prevent access by other employees. It's also not uncommon to find different segmented secure areas where certain groups of employees are allowed to access those areas and others are not.

Control design and implementation should take internal functions into consideration simply because often internal functions are not always given the same level of protection as data and systems that cross organizational boundaries into the Internet or a third-party organization. Frequently businesses don't do as good a job of protecting internal assets from employees as they do protecting these same assets from external entities. Internal security is often overlooked. Controls should be considered that protect data on the internal infrastructure, using access controls, rights, permissions and privileges, encryption, and so on. Policies are also important controls that protect internal systems and information. These administrative controls direct the actions and behavior of organizational personnel, so they primarily serve to protect internal assets. When developing business cases for controls, don't neglect internal systems and data. Internal controls serve to protect data from threats such as malicious insiders, employee complacency and neglect, and accidental access, modification, or destruction.

External Functions

Most organizations put a higher priority on protecting external functions, such as external websites, and other potentially publicly accessible data. The typical example of a control that protects external functions is a firewall, of course, but that's not the only control available and certainly shouldn't be the only control an organization uses. Strong authentication, encryption, third-party agreements, and other access controls should be used to protect external functions and data since these functions are often on stand-alone servers in a DMZ configuration or on third-party servers and networks, which may not be as protected as internal assets, and could potentially be accessible from the public, including resourceful malicious hackers.

Cross-boundary Functions

Closely related to external functions are those functions that tend to cross the physical and logical boundaries of the organization between the internal and external networks. These can be the functions that are most difficult to secure simply because data must pass between the internal and external boundaries of the infrastructure to enable the business to carry out its day-to-day mission, so they can't be completely closed off from the outside world. This can widen the attack surface of the organization's protected network. Again, firewalls are the ubiquitous security control used to protect and separate internal and external boundaries; this definitely shouldn't be the only type of control used. For example, strong authentication should be used for any entity that needs to come from the external network into the internal network for any reason. Usually multifactor authentication is preferred in those cases. Also, data encryption is a must,

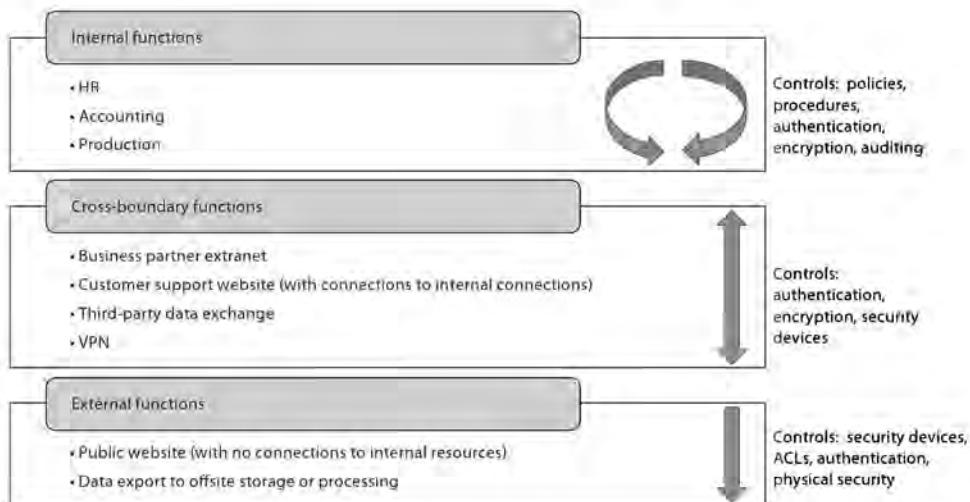


Figure 8-3 Examples of internal, external, and cross-boundary functions and controls

since data traversing in either direction should be protected from unauthorized access and interception. Even the architectural design of the boundaries between the internal network and the external world serves as a security control. For example, a DMZ configuration serves as a boundary layer between the Internet and the internal network, consisting of multiple firewalls, routers, and segmented networks. Examples of cross-boundary traffic might include VPN traffic, business extranets, and public access to an e-commerce website. Controls must be selected and implemented that protect and restrict any and all access that is actually allowed from the external to the internal network, and vice versa. Figure 8-3 illustrates the concepts of internal, external, and cross-boundary functions, with appropriate functions and control examples.



CAUTION Ensure that you consider data sensitivity and segmentation when designing controls for internal, external, and cross-boundary interfaces. This might mean implementing controls such as network segmentation and VLANs, different authentication credentials for systems with data of different sensitivity levels, and restrictive access rights and permissions. It also includes implementing perimeter security controls, such as a DMZ, internal and external firewalls, and separated extranets, as well as strong authentication and encryption mechanisms.

Information System Security Engineering

We discussed the systems development life cycle (SDLC) already in-depth in Chapter 2, but we'll briefly recap it here as a lead-in to the discussion on information systems security engineering. Remember that the SDLC drives the processes of system or software

development, acquisition, implementation, sustainment, and eventual replacement or disposal. The SDLC varies between organizations, and there are several different SDLC models. Some are sequential in nature, while some are iterative, depending upon how the organization develops or acquires systems and software. Also remember the basic generic steps of the different SDLC models. For the most part, all have some sort of requirements phase, design phase, development/acquisition phase, test phase, implementation phase, sustainment and maintenance, and finally, disposal or retirement. Keep in mind that these are just generic phases; most SDLC models use some variation of these particular phases, though, and may even combine or separate them differently. Figure 8-4 shows an example of an SDLC model, promulgated by NIST.

As mentioned, there are several different models with basic generic phases. We'll briefly recap those phases here. The requirements phase is probably the most important since that's when requirements for the systems or software to be built or acquired are determined. Functional and performance requirements are specified during this phase, and all stakeholders must agree on formally defined requirements. If requirements aren't adequately defined during this phase, then the product that will eventually be acquired or developed won't fulfill its intended function or performance levels. This may result in a system that performs the wrong functions, doesn't perform all the required functions, or performs them poorly or below standards.



Figure 8-4 A generic SDLC model

The design phase involves actually taking the requirements and turning them into a workable architecture and design. For systems, this might involve designing interfaces for different components, as well as higher-level assemblies decomposed into lower-level components. For systems that will be acquired, rather than developed by the organization, system specifications are generated during this phase. In the development or acquisition phase, the organization would then go out and find a source for the system it desires or, at the least, the components that will be used to build the system. If the system is to be developed internally by the organization, this process involves actually assembling the components or developing software. The test phase involves performing several different types of tests to ensure that the end product meets the performance and functionality specifications set forth in the requirements phase. Testing could include individual unit testing, systemwide testing, integration testing, and regression testing, to name a few types. Once a system is acquired or developed, it goes through a formal acceptance process. If accepted by the organization, it is usually implemented. Implementation involves actually putting the system into production for its intended use. Some models also distinguish a sustainment or maintenance phase separate from the implementation phase, where the system is maintained, updated, and upgraded occasionally and kept functional. Finally, after the system has reached the end of its useful life cycle, it is disposed of, replaced, or retired. These basic steps of the SDLC are fairly common, and most models, once again, follow them with some variation.

Unfortunately, most of these models, such as the waterfall, iterative, and agile models, were developed before security became a concern. As security became more and more important, it was included later in the life cycle, typically during the implementation or sustainment phase, and applied to a system that was already built. This didn't always work because adding security mechanisms to a system or software after it is already in production may have required refitting a system or integrating security technologies into a system that wasn't designed to accept them. This practice was known as "bolting on" security as an afterthought. For example, if the system was designed with no encryption mechanisms, applying encryption controls to it would be difficult at best and impossible at worst. That would mean that you would have a functional system that was not as secure as it needed to be and didn't protect data during storage, processing, or transmission. Because of issues such as these, it became apparent that a way was needed to "bake in" security from the beginning, from the requirements phase all the way to system disposal. That's where the information system security engineering discipline came into play.

ISSE approaches the SDLC from the perspective that security should be included throughout the entire system's life cycle. One approach is to include security elements in existing SDLC models, but this isn't always easy to do since many of these models are rigid and don't necessarily allow for considering security as a requirement when developing a system. Another approach is to construct development models that are specific to information security engineering and match them up with available SDLC models. Three (of the many) such examples of these models that we'll discuss are the Information Assurance Technical Framework, NIST's SP 800-160, and the ISO/IEC 21827:2008.



EXAM TIP You likely won't be asked about any specific ISSE model on the exam, but it's a good idea to be aware of some of the basic ones and how ISSE affects control design and implementation.

Information Assurance Technical Framework

The Information Assurance Technical Framework (IATF) was developed by the National Security Agency (NSA) in an effort to establish an official U.S. government approach to system security engineering. Its latest iteration dates back to September 2002, actually making it one of the earlier standards and attempts at a cohesive ISSE model. The IATF defines ISSE as "...the art and science of discovering users' information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected." This definition seems a bit lofty, but the goal of the IATF was to establish a concrete set of processes for ISSE, which could be adapted to most SDLC models and extensively covered integration of security considerations into all phases of the system life cycle.

The IATF, particularly in Chapter 3, calls for six phases in its ISSE model, as follows:

1. Discover Needs
2. Define System Requirements
3. Design System Architecture
4. Develop Detailed Design
5. Implement System
6. Assess Effectiveness

Each of these phases is broken down into specific activities particular to that phase. Although the model is sequential in nature, phase 6, Assess Effectiveness, is intended to be conducted simultaneously with all the other phases, allowing practitioners to check to ensure that the goal of the phase has been accomplished before moving on to the next phase. The IATF has not been updated since 2002, with the community generally waiting for and moving toward a new ISSE-related publication anticipated from NIST, discussed next.

NIST SP 800-160

NIST has also produced an informative guide on ISSE, in the form of its Special Publication 800-160, "Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems." Previously, NIST had published its SP 800-64, "Security Considerations in the System Development Life Cycle," in 2008. This older guidance simply looked at security engineering processes in the greater context of the SDLC, rather than as a separate, broader discipline. It made recommendations on security processes and activities that should be considered during the initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal (the particular version of the SDLC phases defined in this publication). The newer SP 800-160 looks

at systems security engineering as a discipline in its own right and defines technical and nontechnical processes for integrating security activities into the system life cycle. This guidance has a system security model highly reminiscent of the IATF model and includes the following phases from the technical processes:

- 1. Stakeholder Requirements Definition Process**
 - a. Elicit Stakeholder Security Requirements
 - b. Define Stakeholder Security Requirements
 - c. Analyze and Maintain Stakeholder Security Requirements
- 2. Requirements Analysis Process**
 - a. Define System Security Requirements
 - b. Analyze and Maintain System Security Requirements
- 3. Architectural Design Process**
 - a. Define the Security Architecture
 - b. Analyze and Evaluate the Security Architecture
 - c. Document and Maintain the Security Architecture
- 4. Implementation Process**
 - a. Plan the Security Implementation of System Elements
 - b. Perform Security Integration of System Elements
- 5. Integration Process**
 - a. Plan the Security Integration of System Elements
 - b. Perform Security Integration of System Elements
- 6. Verification Process**
 - a. Plan the Security Verification of the System
 - b. Perform Security Verification of the System
- 7. Transition Process**
 - a. Plan for the Secure Transition of the System
 - b. Perform the Secure Transition of the System
- 8. Validation Process**
 - a. Plan the Security Validation of the System
 - b. Perform Security Validation of the System
- 9. Operation Process**
 - a. Prepare for the Secure Operation of the System
 - b. Perform Security Operational Activation of the System
 - c. Use the System to Secure Operations

- d. Perform Operational Security Problem Resolution
- e. Support the Customer to Provide Continuous Protection of Assets

10. Maintenance Process

- a. Plan for the Secure Maintenance of the System
- b. Perform Secure Maintenance on the System

11. Disposal Process

- a. Plan for the Secure Disposal of the System
- b. Perform Secure Disposal of the System

SP 800-160 also maps its phases to processes found in a number of specific systems engineering processes defined in various ISO/IEC and IEEE standards, including 15288:2008, “Systems and software engineering – System life cycle processes.” Note that as of this writing, NIST SP 800-160 is still in its draft form, which was published in May 2014.

ISO/IEC 21827:2008

This standard offers a view of a system’s security engineering process model, known as the Systems Security Engineering Capability Maturity Model. It does not detail exact processes; rather, it covers industry best practices related to system security engineering. The model describes the security engineering life cycle and phases, as well as their supporting activities. It takes a holistic view of the organization’s management and engineering processes and their interactions, as well as the interactions between systems, software, compliance, development, and acquisition activities.

ISSE and Control Design

So, what does ISSE have to do with control design and implementation? The entire purpose of an ISSE model and processes is to ensure that security is considered during the entire life cycle of systems, software, and data. This means defining security needs and requirements early on, before the system is even built or bought and before any sensitive data is even generated. The security requirements developed early on in the ISSE process directly influence how sensitive data and systems are, what threats and threat actors exist, potential vulnerabilities, and the overall potential risk to an asset. So, ISSE heavily influences the risk management process. It can help determine what level of protection assets require and what controls should be considered for implementation to protect data and systems. ISSE follows the system from beginning to end, so it ensures that security controls are considered, applied, maintained, and verified during the entire product life cycle.



TIP Understand that the ISSE process is intended to ensure the security is included in all phases of the SDLC model so that security is “baked in” to a system and not “bolted on” after the fact. In this way, it helps reduce risk by considering security early on in the system life cycle.

Design Considerations

Now that we've discussed business requirements, governance, and information security engineering as contributing to the design and implementation process involved with selecting and using controls to protect systems and data, we'll cover some basic design principles to keep in mind when considering controls. Note that these principles aren't specific to a particular type or function of a control; they should be considered for all controls and control functions. These considerations normally are looked at after business and governance requirements are considered since those requirements are usually mandatory or not easily negotiated. These considerations, however, should be considered throughout the ISSE and SDLC processes.

Effectiveness

The *effectiveness* of a control is determined by how well it fulfills its intended security function and protects assets. If a control is ineffective, it is not performing the intended security function for which it was designed or implemented, or it's not performing it to the degree it needs to, leaving an asset vulnerable to threats and allowing an unacceptable level of risk to the asset or organization. In these cases, control gaps, already discussed previously in the book, exist and must be closed (or reduced) by supplementing the control, adding additional controls, or replacing the control. Control effectiveness may not necessarily be the fault of the system administrators or security professionals on the job; in fact, it may not even be a faulty control. Sometimes ineffective controls can be traced back to poorly defined requirements from the SDLC or ISSE process (if any were even considered at all). Measuring control effectiveness is closely related to the concepts of key risk indicators (KRIs) and key performance indicators (KPIs), as well as security metrics, discussed earlier in Chapter 6 and again later in Chapter 9.

Efficiency

Efficiency isn't the same thing as effectiveness; effectiveness relates to if the control fulfills its intended function and how well it does so. Efficiency, on the other hand, relates more to how well the control does in relation to other factors, such as cost, maintainability, interoperability, and so on. Even if a control is effective at what it's supposed to be doing, is it costing too much to maintain it? Does it use up too many resources (manpower, electricity, spare parts); or, in the case of a nontechnical control, does it require overly complicated processes? Is it interoperable with other systems or processes?

In looking at efficiency, the organization must consider controls that are not only effective but reasonable to operate and maintain in terms of the value they add and the level of protection they afford consistent with the asset's value. An older firewall already in place that does the job but is no longer supported by its manufacturer and is therefore hard to get maintenance work or spare parts for, is not necessarily an efficient control. If it requires specialized training that is hard to find or costly, it may be less efficient to use that particular firewall. Process efficiency should also be a consideration in control selection and use. A particular backup system, while effective, may require additional work processes or equipment to ensure its effectiveness or may add components and complexity to the infrastructure. These are definitely aspects to think about while selecting and implementing controls.



EXAM TIP Keep in mind that *control effectiveness* relates to how well it performs its assigned function in protecting an asset. *Control efficiency* relates to how the control interacts with its environment, in terms of cost, interoperability, complexity, staffing requirements, processes, and so forth.

Economy of Use

The term *economy of use*, in this context, refers to the smart design and employment of controls such that they can be used to protect multiple assets at once or provide multiple security functions. Controls that are used to protect only one single asset, or are single-function, tend to be not as useful because additional controls that provide other functions and protect other assets are required. Likewise, controls that are highly specialized in terms of function or level of protection tend to be more expensive, require more training, and may require more personnel or hours to manage and maintain. An example might be a traffic-filtering firewall that performs only that single function versus a multifunctional security appliance that can provide firewall, IDS, and proxy services. Another example might be the use of several security appliances deployed at different points in the network, which could be consolidated and deployed at a more central point in the physical and logical architecture, covering more than one subnet or segment. Yet another instance could be the use of VLANs implemented on a single powerful layer 3 switch, instead of having multiple subnets from many different physical switches. Suppose a system requires specialized hardware encryption devices, which can be expensive. If you have other systems that also require encryption, you could possibly expand the use of these devices to include those other systems, thus providing protection for multiple systems and getting more for the investment than you would if you protected only one system. This is yet another example of the principle of economy of use.

To achieve economy of use, you should examine different aspects of the architecture, data sensitivity and protection requirements, and common protection requirements of assets. Additionally, you can look at the different levels of functionality and features of security technologies and controls to see whether there are better solutions available than single-purpose controls. Of course, cost should be considered and balanced with looking at where a better investment can be made; if a control technology is better suited for economy of use but seems to cost more, in the long run it may represent a cost savings to the organization, as well as help to simplify the sustainment and maintenance of the control.



EXAM TIP *Economy of use* refers to the intelligent acquisition and deployment of security controls, considering them for use in protecting multiple systems, having multiple functions, or providing a greater depth of protection than single-use or system-specific controls.

Meets Defined Requirements

Controls are of little use if they do not meet the protection requirements the organization depends on them for. If a control is not sufficiently reducing a vulnerability for an asset, reducing the likelihood or impact of a threat exploitation, or providing sufficient

protection, the control is not effective. This could mean that the control itself is faulty or it has not been implemented and configured correctly. It also could mean, however, that the original requirements were flawed; that is, they either didn't completely cover what the organization actually needed to protect an asset or were out of scope with what protection levels the control provides.

In any event, if the control is not meeting the asset's protection requirements, either the control (or its implementation) or the requirements are at fault. This is why it's so vitally important for the organization to implement a solid SDLC and ISSE process, as well as to put careful consideration into the selection of controls, including their design and implementation.



TIP The preceding section emphasizes how important the security requirements phase can be since it can make the difference between faulty control design and implementation or effective and efficient controls. You should make every effort to make sure that the security requirements phase is thoroughly and completely accomplished.

Control Redundancy

On the surface, it may seem to be a violation of the design principles of economy of use, efficiency, and common sense, not to mention a waste of resources, to have redundant controls. But think of it like this: What if a control fails or is circumvented by a threat, enabling a vulnerability to be exploited and an asset damaged? If you've heard the term *defense in depth*, then you know that this principle actually encourages multiple, redundant controls, implemented at different levels of the infrastructure or at various points in the system or data-processing cycle to provide sustained protection in the event a single control fails. For example, if a centrally managed anti-malware solution is implemented on your company's e-mail and other infrastructure servers but not on client machines, there's still a possibility a virus could infect the network through other means. That's why you also have the redundant control of having anti-malware software installed on workstations and other client devices, just in case. That redundancy provides defense in depth, maintaining protection against threats. The same could be said for redundant physical controls (multiple security fences, secure doors, and so on). These are all in place in case one fails, still preventing an unauthorized person from entering a secure area.

Control redundancy should be looked at to provide effective protection for an asset but still should be balanced with good design principles. Redundant controls that cover many systems at once and several different types of data, or even serve different security functions simultaneously, should be looked at and implemented. A good example is a unified threat management (UTM) appliance, which provides several services at once, including firewall, intrusion detection and prevention, anti-malware, and content filtering functions. This would be more effective and efficient than having separate security appliances that perform an individual function and having to install multiple instances of each all over the network. Having multiple UTM appliances, placed at various strategic and critical points in the infrastructure, would ensure control redundancy and defense

in depth, while being more efficient than having multiple separate appliances scattered throughout the infrastructure. The same could apply to other security technologies and even processes.

Control Selection

We touched on control selection in Chapter 5, from a risk response perspective, but in this section we'll look once again at this process, more from an implementation and design perspective. Selecting the controls that will be used to protect a particular asset involves categorizing the information in terms of sensitivity across the areas of confidentiality, integrity, and availability, as well as selecting an appropriate baseline set of controls for the asset in question. It also involves the concepts of business function and needs, governance, and the SDLC and ISSE processes discussed earlier, which may influence data sensitivity and required protection levels. Additionally, control selection should involve an understanding of the existing threat landscape the organization resides in since controls must be able to protect against specified threats.

Information Categorization

Control selection has a great deal to do with information classification and data sensitivity. Controls are selected and put into place to protect data, so the right controls have to be implemented to provide the right amount of protection. So, it naturally follows that you must determine the data sensitivity and protection needs first (coincidentally, the first step in the IATF ISSE model discussed earlier). This is where a well-thought-out and well-written data sensitivity and classification policy comes into play. Then, you must look at each data type and determine its impact on the organization if it were to be lost, destroyed, or otherwise unavailable or compromised.

If you follow the NIST RMF process model, the first step in the model is security categorization. This means that data is identified and categorized with sensitivity levels that relate to impact in three areas: confidentiality, integrity, and availability. The level of impact to the organization is determined for each of these areas individually, in terms of high, moderate, and low (per FIPS 199). Then, the overall security categorization (SC) is formulated as follows:

$$\text{SC information system} = \{(\text{confidentiality}, \text{impact}), (\text{integrity}, \text{impact}), (\text{availability}, \text{impact})\}$$

When the values of high, moderate, or low are assigned for each security goal, the highest-valued impact generally becomes the overall security categorization. For example, suppose you had the following levels of impact determined:

$$\text{SC information system} = \{(\text{confidentiality}, \text{MODERATE}), (\text{integrity}, \text{HIGH}), (\text{availability}, \text{MODERATE})\}$$

In this case, the highest impact value is for integrity and has been determined to be high, so the overall security categorization would be assigned as high. This uses the high water mark concept to determine the overall SC of the asset. In short, a system considered

to have an SC of low impact is an information system in which all three of the security objectives are determined to be low. An information system determined to have an SC of moderate is one in which at least one of the security objectives is moderate and no other security objective is rated at a level higher than moderate. Of course, a high-impact system is an information system in which at *least* one security objective is rated as high.

Selecting the Control Baseline

Continuing the example from the NIST RMF, a security baseline is selected based upon the security categorization of the information under discussion. A baseline, as mentioned, is a selected set of controls that apply to a particular security categorization. NIST defines three security baselines: High, Moderate, and Low. Each baseline, starting with Low, offers a certain level of protection for the data type in question. With progressively higher baselines, more controls are added, or the depth of those controls is increased, providing more protection. Note that organizations aren't strictly tied to these security baselines; they are tailorable by the organization, based upon its unique security requirements. For example, even an organization that defines a data asset as a low SC can add additional controls or increase their rigor to account for different and unique circumstances, such as increased threats, asset value, vulnerabilities, and so on. FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," discusses the minimum control baseline requirements for systems, with regard to protecting the confidentiality, integrity, and availability of systems and data. However, these are only the minimum standards that should be considered; a well-developed security categorization may determine many other controls and a much higher security baseline for those assets.

Obviously, this is the NIST RMF methodology; there are other ways to determine asset protection requirements and categorize them, but it all goes back to the basics of data sensitivity levels, protection requirements, and the level of impact to the organization if the data were lost or otherwise unavailable. Controls are selected based upon these and the previous factors discussed and are applied accordingly. NIST SP 800-60 provides guidance on selecting the right control baseline, as well as modifying it based on an organization's unique needs. Figure 8-5, taken from NIST SP 800-53, shows how different controls align with the three basic security control baselines.



EXAM TIP You will not be required to know the specifics of security categorization for the exam, but you may encounter questions that assume you have already performed the security categorization of an asset, or at least know how to do so.

Implementing Controls

Now that you've seen how to categorize information and select the various controls you need for your control baseline, we'll discuss the actual implementation of controls. By and large, this simply means that once the controls have been approved and resourced by management (to include hardware/software purchases, creation of policies and procedures, and staffed with trained personnel), they are put in place. Often this means

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	—	—	—	—
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	Withdrawn	—	—	—	—
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)

Figure 8-5 Controls and their corresponding security control baselines (from NIST SP 800-53)

installing technical solutions (software, equipment, or new configurations), but it also may mean creating and implementing policies and other administrative controls. It also may mean installing physical controls or implementing new or modified processes. In any event, implementation isn't simply turning the switch on for a firewall or distributing a policy. It also means managing and maintaining the control, as well as assessing its effectiveness and adjusting it based upon new or updated risk analysis. The threat landscape changes frequently, and it's up to the organization to monitor these changes in risk to the organization and subsequently add or change controls as needed. In the following sections, we'll discuss the particulars of implementing and maintaining controls, as well as owning and managing the risk associated with them.

Evaluating Existing Control Effectiveness

In Chapter 4 we briefly discussed evaluating and analyzing controls. Remember that effectiveness is how well a control meets the security requirements defined for it. There are several ways to determine control effectiveness; performance monitoring and testing are the most common. Performance monitoring usually takes the form of examining metrics

or data produced while the control is performing its normal function. For instance, a security administrator could view IDS or firewall logs and examine the traffic flows for metrics on how much traffic was blocked by the firewall rules, including what type, its protocol, its origin and destination Internet Protocol (IP) addresses, and so on. From this information, you could gather how effectively the firewall ruleset is blocking or allowing certain types of traffic.

Similarly, for administrative controls, you could measure the effectiveness of policies and procedures by looking at the number of security events for a given time period, noting what the most common incidents were and if the policies and procedures adequately covered those types of incidents. This might also be an indicator of security training effectiveness, as people may inadvertently violate policies because of a lack of training, complacency, or outright maliciousness.

Testing is definitely a way to measure the effectiveness of security controls. In Chapter 6 we discussed different assessments, such as vulnerability assessments and penetration testing. Remember that vulnerability testing is a critical part of risk assessment since you must identify vulnerabilities to identify risk. Vulnerability testing can tell you whether system and data assets have weaknesses, particularly technical ones. Keep in mind that a vulnerability assessment simply tells you the potential for exploitation; only an in-depth penetration test can tell you whether a vulnerability is actually exploitable. The difference between a vulnerability showing up as potentially exploitable and actually being able to exploit it is often the effectiveness of the control in place to mitigate the risk of exploitation. Therefore, a penetration test can give you a much better idea as to how effective your controls really are. Otherwise, you have only a list of vulnerabilities that could be exploited, without knowing how strong the controls protecting them really are.

Once you've performed performance monitoring and in-depth testing, you'll get a better feel for how effective your controls really are and be able to identify shortfalls between the job the control is performing and the real protection requirements it needs to fulfill. This shortfall is a control gap that must be considered for risk response.



EXAM TIP The two primary ways of determining the effectiveness of a control are monitoring the control's performance and testing (including vulnerability and penetration testing).

Adjusting Controls Based on Mitigation Requirements and Control Gaps

If you've identified any control gaps, you must decide how to address them. The gaps must be closed, or at least reduced to an acceptable level. The risk practitioner, in conjunction with management, will have to devise a strategy, based on risk appetite, tolerance, protection requirements, and resources, to close control gaps. Adjusting controls to make up for gaps may require several different actions. You'll need to decide whether to simply reconfigure the control, supplement the control, or add new controls entirely. It's also possible that you may have to replace the existing control with a totally new one.

In any case, whichever action you take, after you've adjusted the control, you should retest it to ensure that it meets the protection requirements for the asset in question.

Supplementing Existing Controls

Supplementing existing controls is an action you can take when the control already in place is doing somewhat of a good job, but maybe it's not quite enough. Perhaps there are new threats that weren't originally considered when the control was implemented, or perhaps the control has become somewhat obsolete. In any case, it may be more cost-effective simply to supplement an existing control by adding controls at other points in the infrastructure to offset the control gap or to temporarily add controls until a more permanent solution can be found. In any case, you'll need to test and make sure that any changes you make to a control meet the security requirements you need, in addition to being interoperable with the environment. For example, suppose you have a firewall that requires an additional module to be installed to counter a new threat. The existing firewall works fine for almost everything else, but this new threat presents significant risk to the infrastructure. Instead of completely replacing the firewall, you could simply add the new module that mitigates the threat. As another example, you could also upgrade your encryption strength to counter new cryptographic threats. However, other systems in the infrastructure may not be able to interoperate with the upgraded encryption mechanism. You would have to perform systemwide testing to determine any interoperability issues and how to approach the upgrade. You may have to choose to upgrade the encryption mechanisms on all the other systems, if they are capable of handling it, or not upgrade the encryption mechanism and come up with some other control to mitigate those threats.

Adding New Controls

Adding new controls could mean either implementing additional controls to mitigate the threats or completely replacing an older or ineffective control with a new one. For example, you could completely replace an older firewall that performs poorly or doesn't have the capability to counter modern threats. In that case, you may simply replace it with a new model. Another example would be an outdated policy that requires backups to older tapes and equipment that is no longer supported by its manufacturer. You could produce a new policy, replacing the old one, which modernizes your backup strategy and also requires you to upgrade to new equipment. The same applies to physical controls.

When adding new controls, you have to consider a few things. First, you must make sure that the new control meets the security requirements you really need. This is a good time to review the security requirements originally defined in your ISSE or SDLC requirements phase or to redefine new requirements. There's also the issue of interoperability to consider. New controls, whether they are technical, administrative, or physical in nature, have to be interoperable with existing infrastructure. New security devices have to be able to communicate with older equipment. The policies and procedures have to be compatible with existing ones and may require that existing processes be slightly modified to accommodate them. Physical controls can be expensive to replace and may even

require modifications to facilities to implement new controls. All of these things have to be considered when adding new controls. And, as with any new control or even an older control that has been supplemented or altered, you should test the control to ensure that it gives you the protection you require.



CAUTION Always test controls after they have been modified, supplemented, replaced, or added to. You want to test for both security and interoperability. Vulnerability testing, penetration testing, and integration testing are key test types that you will want to consider when modifying or changing controls.

Managing Control Ownership and Risk

As mentioned, control/risk ownership is an important part of an organization's enterprise risk management process. Ownership is important because the individuals who are able to make decisions and allocate resources must also be held accountable for control operation and risk management. Without a formal control or risk owner, there may be no one to ensure that controls are monitored for effectiveness and risk is adequately reduced. In all aspects of control design and implementation, control owners must be identified and included in this process since they will ultimately be responsible for their operation and maintenance, as well as monitoring them for effectiveness. While the control and risk owner may be a senior manager, it is also best to ensure that the appropriate technical personnel familiar with the control operations are consulted on best design and implementation practices.

Documenting Controls

Once controls have been implemented and determined to be efficient, be effective, and meet the original (or new) security requirements, you must also make sure that they are well-documented, for several reasons. First, documentation helps to maintain the control history, that is, the records of installing, updating, supplementing, adding, or changing controls necessary for change and configuration management processes. Second, documentation serves as objective evidence of compliance when being audited. Documentation also serves to help support the risk assessment process (remember in Chapter 4, when we discussed reviewing documentation as part of the assessment methodology?). Finally, documentation can help when you are troubleshooting issues with the controls or measuring control effectiveness.

Control owners are generally responsible for maintaining control documentation, but often they are assisted in preparing and maintaining this documentation by technical personnel and risk management practitioners. Control documentation includes configuration settings, architectural diagrams, control procedures, and, of course, policies relating to particular controls. This documentation not only provides compliance validation for controls but also assists in effective control execution. Documentation should be consistent, be standardized, and clearly state how the control protects an asset. It should also be mapped to a formally defined security requirement, for traceability purposes.

Control documentation is part of the greater risk documentation library, contributing to risk profiles, plans of action and milestones, and risk registers.

Chapter Review

In this chapter, you took a deeper look at controls, focusing on design and implementation concepts. First, you looked at the business perspectives of controls and learned how important the business case may be when justifying supplementing or adding to controls. Business cases are useful for justifying controls when there are cost versus effectiveness issues, and the requirement for a control must be matched to a business need. Some of the supporting reasons for a good business case include support for security goals, governance, due diligence, liability, efficiency, and cost effectiveness. You also looked at regulatory guidance and how the selection of controls is influenced by laws, regulations, and other external requirements imposed on businesses. Some examples we covered included the PCI-DSS standards, HIPAA, GLBA, SOC, and FISMA. We also discussed business functions and their relationships to controls, since controls are implemented to reduce IT risk and in turn reduce business risk. We explained internal, external, and cross-boundary functions that influence the design and implementation of security controls.

We then explained the role that the information system security engineering process plays in control development and implementation. We discussed how ISSE ensures that security is built into systems throughout the life cycle, all the way from concept through design and development, through acquisition and implementation, and finally to disposal or retirement. We discussed several different ISSE models, including those from the IATF, NIST, and ISO/IEC.

There are several design considerations that we covered as well, to ensure that the design process is well considered and takes into account control effectiveness, efficiency, economy of use, and redundancy. We also stressed that controls must meet the original security requirements they were designed to fulfill in asset protection.

Control selection is based upon several factors, including information categorization, which attempts to assign a level of impact to the organization if the asset is lost. After information is categorized, a baseline set of controls is assigned to it, based upon those factors. We then looked at actual control implementation and included several processes that occur when controls are implemented, as well as maintained. These processes include evaluating the effectiveness of existing controls, through performance monitoring and testing, as well as adjusting existing controls to reduce any identified control gaps. We also covered the value of supplementing existing controls versus adding or replacing controls. Finally, we looked at managing control and risk ownership to ensure that individuals are held accountable for sound decisions and allocating resources involved with designing, implementing, maintaining, operating, and documenting controls, as well as the risk they are intended to mitigate.

Review Questions

1. Which of the following is the ultimate goal of IT controls?
 - A. Reduce IT risk
 - B. Reduce business risk
 - C. Eliminate risk
 - D. Eliminate threats
2. Which of the following best describes the reason to create a business case for IT control implementation?
 - A. To determine the cost to the organization if a control is implemented
 - B. To help create the organization's risk profile
 - C. To justify the resources expended in implementing the IT control
 - D. To inform control owners about the potential risk of a control
3. All of the following are valid supporting factors in building a business case to justify implementing an IT control, except which one?
 - A. Profitability
 - B. Security goals
 - C. Liability
 - D. Governance
4. Which of the following two factors relating to how well a control can be used for multiple purposes, and how it compares to other controls in terms of cost and interoperability, are used in business cases? (Choose two.)
 - A. Economy of use
 - B. Support for security goals
 - C. Efficiency
 - D. Threat reduction
5. Which of the following governance sources explicitly requires the use of NIST controls as the preferred control framework to support it?
 - A. SOX
 - B. GLBA
 - C. HIPAA
 - D. FISMA

6. Which of the following is not necessarily a mandatory legal standard for governance but is imposed by its industry?
 - A. HIPAA
 - B. PCI-DSS
 - C. FISMA
 - D. SOX
7. Which of the following control frameworks does HIPAA governance recommend but is not mandatory?
 - A. NIST
 - B. ISO/IEC 27001
 - C. COBIT
 - D. PCI-DSS
8. Which of the following was enacted into law to ensure the safeguarding of client financial and personal information by specified financial institutions?
 - A. PCI-DSS
 - B. SOX
 - C. GLBA
 - D. HIPAA
9. Which of the following laws uses COBIT and COSO, among other control frameworks, to enforce auditing and information governance requirements?
 - A. HIPAA
 - B. PCI-DSS
 - C. SOX
 - D. FISMA
10. Which type of business functions are concerned with data flows and system interfaces between internal and external networks and organizations?
 - A. Cross-boundary functions
 - B. External functions
 - C. Internal functions
 - D. E-commerce functions
11. How can ISSE processes assist the control design and implementation process?
 - A. By ensuring security is considered throughout the entire SDLC process
 - B. By minimizing threats to assets and threat actors
 - C. By ensuring that vulnerabilities are not exposed to threats
 - D. By eliminating risk for a particular asset as it is designed, developed, and implemented

12. Which design principle relates to how well a control performs its intended function in protecting an asset?
- A. Efficiency
 - B. Effectiveness
 - C. Economy of use
 - D. Control redundancy
13. Which of the following design principles is concerned with how well a control operates within its environment, in terms of cost, interoperability, ease of use, and so on?
- A. Effectiveness
 - B. Economy of use
 - C. Efficiency
 - D. Meeting requirements
14. Which of the following concepts supports the principle of control redundancy?
- A. Defense in depth
 - B. Effectiveness
 - C. ISSE
 - D. Economy of use
15. Per FIPS 199, when formulating a security categorization, all of the following are considered in the levels of impact to an organization if an asset is lost or damaged, or in terms of criticality to the organization, except which one?
- A. Confidentiality
 - B. Integrity
 - C. Availability
 - D. Accountability
16. Which of the following best describes how security categorization for data is calculated?
- A. SC information system = {(vulnerability, impact), (threat, impact), (asset, impact)}
 - B. SC information system = {(confidentiality, impact), (integrity, impact), (authorization, impact)}
 - C. SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}
 - D. SC information system = {(confidentiality, risk), (integrity, risk), (availability, risk)}

17. Which the following are ways to evaluate control effectiveness? (Choose two.)
- A. Monitoring control performance
 - B. Calculating reduced likelihood
 - C. Calculating reduced impact to the asset
 - D. Testing
18. Which of the following scenarios best describes a control gap?
- A. Permissions on a sensitive network share that allow all users to read the contents
 - B. A firewall that successfully blocks all traffic except for that specifically allowed
 - C. Encryption settings that encrypt both sensitive and nonsensitive data
 - D. Whitelisting only specific applications that are allowed on a workstation
19. Which of the following options should be considered to close control gaps? (Choose two.)
- A. Reducing threats
 - B. Supplementing existing controls
 - C. Adding new controls
 - D. Upgrading the system
20. When considering control and risk ownership, which of the following is the main concern?
- A. How much a control costs to maintain
 - B. Accountability
 - C. Organizational structuring
 - D. Ensuring that risk and control owners are separate to ensure that there is no conflict of interest

Answers

1. **B.** While IT security controls do reduce IT risk, the ultimate goal is to reduce the overall risk to the business.
2. **C.** A business case is used to justify the resources expended to implement a control, balancing cost with the risk incurred if the control is not implemented.
3. **A.** Profitability is not a valid supporting factor in building a business case to support implementing an IT control.
4. **A, C.** Economy of use (relating to multipurpose controls) and efficiency (relating to cost and interoperability) are two design principles often used in business cases to justify the implementation of controls.

5. **D.** FISMA explicitly requires the use of NIST controls as the preferred control framework to support it.
6. **B.** PCI-DSS standards are not necessarily a mandatory legal governance but are imposed by the card payment industry.
7. **A.** HIPAA governance recommends, but does not require, the use of the NIST control framework.
8. **C.** GLBA was enacted into law to ensure, among other things, the safeguarding of certain client financial and personal information by banks and other financial institutions.
9. **C.** SOX uses COBIT and COSO, along with other control frameworks, to enforce auditing and information governance requirements.
10. **A.** Cross-boundary functions are those concerned with data flows and system interfaces between internal and external networks and organizations.
11. **A.** ISSE contributes to the control design and implementation process by ensuring that security is considered throughout the entire SDLC process.
12. **B.** Control *effectiveness* refers to how well a control performs its intended function in protecting an asset.
13. **C.** The design principle of *efficiency* is concerned with how well a control operates within its environment, in terms of cost, interoperability, and complexity, among other factors.
14. **A.** The concept of *defense in depth* supports the principle of control redundancy because it allows for multiple controls to be in place in case a single control fails.
15. **D.** Accountability is not considered in the levels of impact to an organization if an asset is lost or damaged or in terms of criticality during a security categorization.
16. **C.** Security categorization for an information system is calculated as follows:
$$\text{SC information system} = \{(\text{confidentiality}, \text{impact}), (\text{integrity}, \text{impact}), (\text{availability}, \text{impact})\}$$
17. **A, D.** Monitoring control performance and testing are two ways to evaluate control effectiveness.
18. **A.** Permissions on a sensitive network share that allow all users to read the contents would be considered ineffective in protecting sensitive information, thus showing a control gap; all the other examples are of effective controls or, even in some cases, controls that may be configured too securely.
19. **B, C.** Both supplementing existing controls and adding new controls should be considered to close control gaps.
20. **B.** Accountability is the main concern when considering control and risk ownership.

Measuring Risk and Control Effectiveness

In this chapter, you will:

- Learn about how to measure various aspects of risk and control related to business processes and effectiveness within different organizational contexts.

This chapter reviews real-world examples of metrics designed to measure the risk and control effectiveness. The following are the CRISC exam objectives from Domain 4 that we'll review and apply within this chapter:

- 4.2 Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
- 4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.
- 4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.
- 4.5 Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.
- 4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

Applying Key Performance Indicators

In Chapter 6, you learned about KRIs and KPIs and what they're used for. This chapter will apply that knowledge toward helping you determine what a useful metric might be for your organization.



NOTE More information on the controls measured within KRIs and KPIs is available in Chapters 7 and 8. It is critical that you understand what should be measured, and how it relates to improving the risk posture, before you develop either KPIs or KRIs.

Key Performance Indicator Review

As discussed, you use *key performance indicators* (KPIs) to understand and enable the measurement of control performance. Control performance can be anything from how often your firewall blocks malicious incoming traffic to how often you exercise your continuity of operations plan. The level of “performance” can be different for each organization; it’s important that you not borrow the KPIs from another organization as a whole but really focus on how your KPIs meet your organizational objectives and what your risk appetite is.



NOTE A hospital might have a KPI or KRI related to systems having proper redundancy to support medical operations during a crisis situation. That level of performance would not be appropriate to a university’s local area network. Understand the context in which you’re working to build the best measures of success.

KPIs should be S.M.A.R.T. to be most effective. This stands for the following:

- Specific
- Measurable
- Attainable
- Relevant
- Timely

When a KPI is S.M.A.R.T., it is tailored to the organization and the area being measured. As discussed earlier, the metric will differ greatly depending on whether you are wanting to measure availability in a stock trading environment versus, say, a college network. It’s incredibly important to think about what’s relevant to your organization when determining your KPIs.

Key Performance Indicator Development

It’s critical that, as you develop your KPIs, you use a standard format. You could use a number of formats, but they generally include standard fields, such as unique name to track the metric by, the target for success, and how success will be measured. It’s important also to delineate what evidence will be used to show the level of success; do you intend to take someone’s word for it that they met the KPI goal? Probably not, so you need to find a way to show evidence, be it a signed document, logs, or other “authoritative” source. Also, remember that it’s always better to get this document yourself (or perhaps by one of your team members) directly from the source, rather than relying on someone who’s being assessed to supply it. This simply cuts down on the likelihood that your implementation evidence has been tampered with.

Table 9-1 shows the template we’ll be utilizing within this chapter to discuss some solid KPIs, adapted from NIST Special Publication 800-55. This template has a few

Field	Data
Measure ID	Here you state the unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	This is a statement of strategic goal or an information security goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	This is a statement of measurement. Use a numeric statement that begins with the word <i>percentage, number, frequency, average</i> , or a similar term.
Type	This is a statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	This is a calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	This is a threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. A target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select a final and interim target to enable tracking of progress toward the stated goal.
Implementation Evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure.
Frequency	This field indicates how often the data is collected and analyzed and how often the data is reported. Select the frequency of data collection based on a rate of change in a particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Here you indicate the following key stakeholders: <ul style="list-style-type: none"> • <i>Information owner:</i> Identify the organizational component and individual who owns required pieces of information. • <i>Information collector:</i> Identify the organizational component and individual responsible for collecting the data. (Note that if possible, the information collector should be a different individual or even a representative of a different organizational unit than the information owner to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.) • <i>Information customer:</i> Identify the organizational component and individual who will receive the data.
Data Source	This is the location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	This field indicates how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Table 9-1 NIST Special Publication 800-55 Measures Template and Instructions

attributes that make it an appealing choice. For instance, it's free for use, it's quite comprehensive, and it already has some great security metrics that are associated with it. Remember that NIST has a number of risk-related documents and frameworks (we've discussed some of them previously), and the organization has done a good job building this template to take those ideas in and create a usable metric. We'll build on NIST's work and use this template later in the chapter to incorporate other measurable risk concepts, such as usability and budget concerns. Also, for our purposes, when you see the term *metric* used by NIST, it is interchangeable with KPI, as discussed within Chapter 6.

Also, don't forget the questions discussed in Chapter 6 that were developed by Oak Ridge Institute for Science and Education to determine the quality of metrics; you should consider these within each KPI you develop.

- Is the metric objectively measurable?
- Does the metric include a clear statement of the end results expected?
- Does the metric support customer requirements, including compliance issues where appropriate?
- Does the metric focus on effectiveness or efficiency of the system being measured?
- Does the metric allow for meaningful trend or statistical analysis?
- Have appropriate industry or other external standards been applied?
- Does the metric include milestones or indicators to express qualitative criteria?
- Are the metrics challenging but at the same time attainable?
- Are assumptions and definitions specified for what constitutes satisfactory performance?
- Have those who are responsible for the performance being measured been fully involved in the development of this metric?
- Has the metric been mutually agreed upon by you and your customers?

Types of Key Performance Indicators

There are any number of KPIs that you could choose to measure the user adoption, network health, or any other attribute of your organization's risk posture. However, we will focus on a subset of KPIs that can help identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls. In the following sections, we will discuss KPIs associated with the following: availability; configuration management; system and services acquisition; contingency planning; access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; system and communications protection; and system and information integrity.

Availability One way to measure availability is through the use of *uptime*, or the percentage of time that a system, collection of systems, or even a website is available. High availability is measured in terms of what systems personnel refer to as *the nines*. For example, you might see 99.99 percent availability, or even 99.999 percent availability (referred to as *5 nines* of availability). The more decimal places, the higher availability required. Uptime is usually measured as 99.9 percent, 99.99 percent, or 99.999 percent. At 99 percent, the asset could be down for about three days in a year, while at 99.999 percent availability, the measured asset is unavailable for only about five minutes a year. Think of how damaging a three-day downtime would be for a retail website, say, around Black Friday. It's important to understand the required service time and put it in your service provider's agreement. Table 9-2 provides a sample availability measure that could be used to measure against the nines.

Field	Data
Measure ID	Availability measure.
Goal	<i>Strategic goal:</i> To provide consistent service to both external and internal users through website availability.
Measure	The measure is the percentage (%) of time that the website is available for use.
Type	Effectiveness/Efficiency.
Formula	The formula is the agreed-upon service time (downtime/agreed-upon service time).
Target	This should be a high percentage defined by the organization (as stated previously, this could be 99.9 percent, 99.99 percent, or 99.999 percent, depending on the desired level of availability).
Implementation Evidence	1 Does the organization use an automated "uptime" measure, such as the <i>uptime</i> command in UNIX? <input type="checkbox"/> Yes <input type="checkbox"/> No 2. What is the agreed-upon service time? _____ 3. What is the actual service time (measured through the <i>uptime</i> command or another agreed-upon tool)? _____
Frequency	<i>Collection frequency:</i> This is defined by the organization (for example, minutes). <i>Reporting frequency:</i> This is defined by the organization (for example, minutes).
Responsible Parties	<ul style="list-style-type: none"> • <i>Information owner:</i> This is defined by the organization (for example, the chief information officer [CIO]). • <i>Information collector:</i> This is defined by the organization (for example, system administrators). • <i>Information customer:</i> This could be the chief information officer (CIO) or chief executive officer (CEO).
Data Source	This is an uptime tool that conducts "pings" of the website at regular intervals.
Reporting Format	This is a pie chart comparing the percentage of time the system or site is available versus the percentage it is unavailable.

Table 9-2 Availability Measure

Configuration Management Applications and systems should have a defined, documented configuration baseline that consists of the basic functional operational settings needed for proper system and application use. This baseline should include all the hardware, software, firmware, and associated documentation across the life cycle of the application or system. The baseline may change with updates and patches and should be tested to ensure that the changes are not problematic before full adoption. Changes are presented and enforced through the use of boards that allow or deny the requested changes and automated tools designed to alert on unauthorized changes. Table 9-3 details a measure that could be used to track the use of an automated configuration tool being implemented within an organization.

System and Services Acquisition In Chapter 5, we discussed the concept of a system development life cycle (SDLC), particularly NIST Special Publication 800-64, “Security Considerations in the System Development Life Cycle.” To recap, the NIST SDLC life cycle has five phases: initiation, acquisition/development, implementation/assessment, operations/maintenance, and sunset (otherwise known as disposition). It’s critical that controls are developed and implemented within each phase of this life cycle; NIST states that “an integrated security component (composed of milestones, deliverables, control gates, and interdependencies) that specifically addresses risk management...enables security to be planned, acquired, built-in, and employed as an integral part of a project or system.” To effectively achieve these goals, organizations must allocate sufficient resources, follow appropriate processes, and assure that these activities are undertaken also by any third parties that have access to information, applications, or services. Table 9-4 provides a KPI that can be used to track the percentage of system and service acquisition contracts that include those third-party security requirements.

Contingency Planning To maintain business continuity, proper planning must be conducted to ensure your organization not only survives but can function after a disaster or incident. This planning should include identifying critical processes, prioritizing systems and equipment, and determining the impact to the business if any of these processes, systems, or equipment are unavailable to the organization for extended periods of time. Additionally, appropriate planning includes determining strategies to bring those identified assets back online so the business can assume some level of operations. These plans should be tested regularly to be sure that they are effective and efficient and that all required personnel are ready to execute them in the heat of the moment. Table 9-5 presents a KPI for understanding the percentage of systems that have conducted their required contingency plan testing.

Access Control Proper access control requires an organization to restrict access to systems and data only to authorized users; often there are different data sensitivity levels and different access requirements for each. Any policy should address and support the principle of least privilege and mandate that only the minimum rights, permissions, and privileges necessary to accomplish a job or task be given to individuals. For example, it may state that for proprietary financial data, an individual needs to work within the finance department of the company. It also may detail requirements for any security clearance (in the case of government contractors, for example) and need-to-know

Field	Data
Measure ID	Configuration Changes measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To accelerate the development and use of an electronic information infrastructure. <i>Information Security goal:</i> To establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
Measure	The measure is the percentage (%) of approved and implemented configuration changes identified in the latest automated baseline configuration.
Type	Implementation.
Formula	The formula is as follows: (Number of approved and implemented configuration changes identified in the latest automated baseline configuration/total number of configuration changes identified through automated scans)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> 1. Does the organization manage configuration changes to information systems using an organizationally approved process? <input type="checkbox"/> Yes <input type="checkbox"/> No 2. Does the organization use automated scanning to identify configuration changes that were implemented on its systems and networks? <input type="checkbox"/> Yes <input type="checkbox"/> No 3. If yes, how many configuration changes were identified through automated scanning over the last reporting period? _____ 4. How many change control requests were approved and implemented over the last reporting period? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example the configuration manager). <i>Information collector:</i> This is defined by the organization (for example, the information system security officer [ISSO], system owner, and system administrator). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO]), authorizing official (AO), or configuration control board.
Data Source	The data source includes system security plans, configuration management database, and security tool logs.
Reporting Format	This is a pie chart comparing the percentage of approved and implemented changes documented in the latest baseline configuration versus the percentage of changes not documented in the latest baseline configuration.

Table 9-3 Configuration Changes Measure (Adapted from NIST Special Publication 800-55)

Field	Data
Measure ID	Service Acquisition Contract measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To accelerate the development and use of an electronic information infrastructure. <i>Information Security goal:</i> To ensure third-party providers employ adequate security measures to protect information, applications, or services outsourced from the organization.
Measure	The measure is the percentage (%) of system and service acquisition contracts that include security requirements or specifications.
Type	Implementation.
Formula	The formula is as follows: (Number of system and service acquisition contracts that include security requirements and specifications/total number of system and service acquisition contracts)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> How many active service acquisition contracts does the organization have? _____ How many active service acquisition contracts include security requirements and specifications? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the contracting officer). <i>Information collector:</i> This is defined by the organization (for example, the contracting officer's technical representative or the system owner). <i>Information customer:</i> This could be the contracting officer's technical representative, system owner, procurement officer, chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes service acquisition contracts.
Reporting Format	This is a pie chart comparing the percentage of system and service acquisition contracts that include security requirements or specifications versus the percentage of system and service acquisition contracts that do not include security requirements or specifications.

Table 9-4 Service Acquisition Contract Measure (Adapted from NIST Special Publication 800-55)

between departments. One common access control consideration is remote access, often used to allow users to telecommute or work from home. Table 9-6 provides a sample KPI that shows the percentage of legitimate remote access points used to gain authorized access to an organization.

Field	Data
Measure ID	Contingency Plan Testing measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Measure	The measure is the percentage (%) of information systems that have conducted annual contingency plan testing.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of information systems that have conducted annual contingency plans testing/number of information systems in the system inventory)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> How many information systems are in the system inventory? _____ How many information systems have an approved contingency plan? _____ How many contingency plans were successfully tested within the past year? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, annually). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the contingency plan manager). <i>Information collector:</i> This is defined by the organization (for example, the system owner or system administrator). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	The data source includes contingency plan testing results.
Reporting Format	This is a pie chart comparing the percentage of systems that conducted annual contingency plan testing versus the percentage of systems that have not conducted annual contingency plan testing.

Table 9-5 Contingency Plan Testing Measure (Adapted from NIST Special Publication 800-55)

Awareness and Training It's important that organizations have proper training and awareness programs that teach employees about current threats, laws, regulations, policies, and the implications of poor behaviors. These programs help improve user behavior through awareness of the risks associated with negative activities and ensuring that they are trained appropriately to carry out their duties safely. This is even more

Field	Data
Measure ID	Remote Access Control measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To restrict information, system, and component access to individuals or machines that are identifiable, known, credible, and authorized.
Measure	The measure is the percentage (%) of remote access points used to gain unauthorized access.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of remote access points used to gain unauthorized access/total number of remote access points)*100.
Target	This should be a low percentage defined by the organization.
Implementation Evidence	<p>1. Does the organization use automated tools to maintain an up-to-date network diagram that identifies all remote access points?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>2. How many remote access points exist in the organization's network? _____</p> <p>3. Does the organization employ an intrusion detection system (IDS) to monitor traffic traversing remote access points?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>4. Does the organization collect and review audit logs associated with all remote access points?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>5. Does the organization maintain a security incident database that identifies standardized incident categories for each incident?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>6. Based on reviews of the incident database, IDS logs and alerts, and appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period? _____</p>
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, monthly). <i>Reporting frequency:</i> This is defined by the organization (for example, quarterly).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This could be the computer security incident response team (CSIRT). <i>Information collector:</i> This could be the system administrator or information system security officer (ISSO). <i>Information customer:</i> This could be the chief information officer (CIO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the following: incident database, audit logs, network diagrams, and IDS logs and alerts.
Reporting Format	This is a stacked bar chart, by month, that illustrates the percentage of remote access points used for unauthorized access versus the total number of remote access points.

Table 9-6 Remote Access Control Measure (Adapted from NIST Special Publication 800-55)

critical for personnel assigned to perform information security or risk-focused duties. Table 9-7 provides a KPI for measuring the percentage of personnel assigned to information security-focused roles that have received their required security training.

Field	Data
Measure ID	Security Training measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure a high-quality workforce supported by modern and secure infrastructure and operational capabilities. <i>Information Security goal:</i> To ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
Measure	The measure is the percentage (%) of information system security personnel that have received security training.
Type	Implementation.
Formula	The formula is as follows: (Number of information system security personnel that have completed security training within the past year/total number of information system security personnel)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> Are significant security responsibilities defined with qualifications criteria and documented in policy? <input type="checkbox"/> Yes <input type="checkbox"/> No Are records kept of which employees have significant security responsibilities? <input type="checkbox"/> Yes <input type="checkbox"/> No How many employees in your agency (or agency component, as applicable) have significant security responsibilities? _____ Are training records maintained? (Training records indicate the training that specific employees have received.) <input type="checkbox"/> Yes <input type="checkbox"/> No How many of those with significant security responsibilities have received the required training? _____ If all personnel have not received training, state all the reasons that apply: <input type="checkbox"/> Insufficient funding <input type="checkbox"/> Insufficient time <input type="checkbox"/> Courses unavailable <input type="checkbox"/> Employee has not registered <input type="checkbox"/> Other (specify) _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the training manager). <i>Information collector:</i> This is defined by the organization (for example, the information system security officer [ISSO] or training manager). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes training and awareness tracking records.
Reporting Format	This is a pie chart illustrating the percentage of security personnel who have received training versus those who have not received training. If performance is below the target, a pie chart illustrates the causes of performance falling short of the targets.

Table 9-7 Security Training Measure (Adapted from NIST Special Publication 800-55)

Audit and Accountability Auditing is implemented by recording the actions of users or other systems or processes when interacting with your organizational systems or data. Auditing is a way of preventing data loss or modification, as well as detecting when it has occurred. Accountability, on the other hand, is the process of holding users accountable for their actions. Accountability serves two important functions. First, it can deter otherwise honest users from committing security policy violations, if they know that their actions are being audited and monitored. It is also used to punish or sanction users who do attempt to or successfully violate security policies. Auditing and accountability often go hand-in-hand because it is difficult to maintain accountability for actions in the system without auditing mechanisms in place. Table 9-8 provides a KPI that measures the average frequency that audit logs and other records are reviewed; you want this to be a high frequency.

Field	Data
Measure ID	Audit Record Review measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity.
Measure	The measure is the average frequency of audit records review and analysis for inappropriate activity.
Type	Effectiveness/Efficiency.
Formula	This is the average frequency during the reporting period.
Target	This should be a high frequency defined by the organization.
Implementation	For each system:
Evidence	<ol style="list-style-type: none"> Is logging activated on the system? <input type="checkbox"/> Yes <input type="checkbox"/> No Does the organization have clearly defined criteria for what constitutes evidence of "inappropriate" activity within system audit logs? <input type="checkbox"/> Yes <input type="checkbox"/> No For the reporting period, how many system audit logs have been reviewed within the following time frames for inappropriate activity (choose the nearest time period for each system)? Within the past day _____ Within the past week _____ 2 weeks to 1 month _____ 1 month to 6 months _____ More than 6 months _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, daily). <i>Reporting frequency:</i> This is defined by the organization (for example, quarterly).

Table 9-8 Audit Record Review Measure (Adapted from NIST Special Publication 800-55) (continued)

Field	Data
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the system owner). <i>Information collector:</i> This is defined by the organization (for example, system administrator). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes audit log reports.
Reporting Format	This is a bar chart showing the number of systems with average audit log reviews in each of the five categories within the Implementation Evidence field.

Table 9-8 Audit Record Review Measure (Adapted from NIST Special Publication 800-55)

Certification, Accreditation, and Security Assessments The term *certification and accreditation* (C&A) has moved out of vogue in favor of risk management and the concept of continuous monitoring. However, many organizations (particularly those within government contexts) are still required to periodically assess their controls and develop plans of action and milestones (POA&Ms) for any deficiencies. At the end of the process, an authorizing official gives permission for the system to be used for a certain period of time, until the process begins again. While this was previously quite documentation-driven, more conscientious organizations are now using automated tools that provide a “common operational picture” or real-time health of the critical systems across the organization. Table 9-9 discusses a KPI that can be used to measure the percentage of new systems that have completed their required C&A before being added to the network.

Identification and Authentication When a person, system, or process wants to access a system, the first thing they must do is identify themselves to the system. Most of us are used to presenting user credentials, such as a username and password combination to the system, and then logging into it. Presenting your credentials is known as *identification*. Authentication is the next step in the process of gaining access to a system or facility. Once you’ve identified yourself by presenting valid credentials, these credentials must be validated. *Authentication* is the validation of those credentials. Authentication is often performed by looking up credentials in a database or an access control list. Organizations should require authentication as a prerequisite to allowing access to their systems. Table 9-10 shows a KPI that can be used to measure the percentage of users with access to shared accounts or accounts that can be used by more than one user. These inherently challenge the concept of identification because it’s difficult (if not impossible) to trace the activity back to a single person, if other methods are not used.

Field	Data
Measure ID	C&A Completion measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To ensure all information systems have been certified and accredited as required.
Measure	The measure is the percentage (%) of new systems that have completed certification and accreditation (C&A) prior to their implementation.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of new systems with complete C&A packages with authorizing official [AO] approval prior to implementation)/(total number of new systems) *100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> Does your agency (or agency component, if applicable) maintain a complete and up-to-date system inventory? <input type="checkbox"/> Yes <input type="checkbox"/> No Is there a formal C&A process within your agency? <input type="checkbox"/> Yes <input type="checkbox"/> No If the answer to the previous question is yes, are system development projects required to complete C&A prior to implementation? <input type="checkbox"/> Yes <input type="checkbox"/> No How many new systems have been implemented during the reporting period? _____ How many systems indicated in the previous question have received an authority to operate prior to implementation? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, authorizing official [AO]). <i>Information collector:</i> This is defined by the organization (for example, system owners). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the system inventory and system C&A documentation.
Reporting Format	This is a pie chart comparing the percentage of new systems with AO-approved C&A packages versus new systems without AO-approved C&A packages.

Table 9-9 C&A Completion Measure (Adapted from NIST Special Publication 800-55)

Field	Data
Measure ID	User Accounts measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> All system users are identified and authenticated in accordance with information security policy.
Measure	The measure is the percentage (%) of users with access to shared accounts.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of users with access to shared accounts/total number of users)*100.
Target	This should be a low percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> How many users have access to the system? _____ How many users have access to shared accounts? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, monthly). <i>Reporting frequency:</i> This is defined by the organization (for example, monthly).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the system owner or system administrator). <i>Information collector:</i> This is defined by the organization (for example, the system administrator). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the configuration management database, access control list, and system-produced user ID lists.
Reporting Format	This is a pie chart comparing the percentage of users with access to shared accounts versus the percentage of users without access to shared accounts.

Table 9-10 User Accounts Measure (Adapted from NIST Special Publication 800-55)

Incident Response An incident can be defined as a negative event that adversely affects the organization, its data and systems, its people, and its overall ability to perform its mission or business functions. An incident could be an external hacking attempt or an insider threat, where an employee steals proprietary data and sells it to a competitor. Incidents can also be natural disasters such as a fire or flood. Organizations should establish a quick-response group for handling incidents that includes activities for preparation, detection, analysis, containment, recovery, and user response. The group should also track, document, and report incidents to required officials and authorities. Table 9-11 provides a KPI that allows you to track the percentage of incidents reported within a set time frame.

Field	Data
Measure ID	Incident Response measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To make accurate, timely information on the organization's programs and services readily available. <i>Information Security goal:</i> To track, document, and report incidents to appropriate organizational officials or authorities.
Measure	The measure is the percentage (%) of incidents reported within required time frame per applicable incident category (the measure will be computed for each incident category described in Implementation Evidence).
Type	Effectiveness/Efficiency.
Formula	For each incident category, the formula is as follows: (Number of incidents reported on time/total number of reported incidents)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<p>1. How many incidents were reported during the period?</p> <p>Category 1: Unauthorized Access _____</p> <p>Category 2: Denial of Service _____</p> <p>Category 3: Malicious Code _____</p> <p>Category 4: Improper Usage _____</p> <p>Category 5: Scans/Probes/Attempted Access _____</p> <p>Category 6: Investigation _____</p> <p>2. How many incidents involving personally identifiable information (PII) were reported during the period? _____</p> <p>3. Of the incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by US-CERT?</p> <p>Category 1: Unauthorized Access _____</p> <p>Category 2: Denial of Service _____</p> <p>Category 3: Malicious Code _____</p> <p>Category 4: Improper Usage _____</p> <p>Category 5: Scans/Probes/Attempted Access _____</p> <p>Category 6: Investigation _____</p> <p>4. Of the PII incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by US-CERT or OMB memorandum(s)? _____</p>
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, monthly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the computer security incident response team [CSIRT]). <i>Information collector:</i> This is defined by the organization (for example, the system owner, information system security officer [ISSO], CSIRT). <i>Information customer:</i> This could include the chief information officer (CIO) or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the following: incident logs and incident tracking database (if available).
Reporting Format	For a one-time snapshot, the format is a stacked bar chart illustrating the proportion of reported incidents per category that were reported on time. For trends, the format is a line chart where each line represents an individual category plus a line representing 100 percent.

Table 9-11 Incident Response Measure (Adapted from NIST Special Publication 800-55)

Maintenance It's important that every organization perform timely maintenance on all their systems in accordance with a set schedule. In many cases, this means that machines are brought offline, or made unavailable, to have operating system patches, software upgrades, or other scheduled activities that are required to keep the systems running in their best form. Table 9-12 lists a KPI measuring the percentage of systems and their components that have undergone maintenance based on the set maintenance schedules.

Field	Data
Measure ID	Maintenance measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To accelerate the development and use of an electronic information infrastructure. <i>Information Security goal:</i> To perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Measure	The measure is the percentage (%) of system components that have undergone maintenance in accordance with set maintenance schedules.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of system components that undergo maintenance according to formal maintenance schedules/total number of system components)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> 1. Does the system have a formal maintenance schedule? <input type="checkbox"/> Yes <input type="checkbox"/> No 2. How many components are contained within the system? _____ 3. How many components underwent maintenance in accordance with the formal maintenance schedule? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the system owner). <i>Information collector:</i> This is defined by the organization (for example, the system administrator). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the maintenance schedule and maintenance logs.
Reporting Format	This is a pie chart comparing the percentage of system components receiving maintenance in accordance with the formal maintenance schedule versus the percentage of system components not receiving maintenance in accordance with the formal maintenance schedule over the specified period.

Table 9-12 Maintenance Measure (Adapted from NIST Special Publication 800-55)

Media Protection Organizations should protect both paper and digital media, limit access to authorized users (as discussed in the “Access Control” section of this chapter), and sanitize or destroy that media before they are disposed or released for reuse. This is especially important for high-security environments where classified or other sensitive material is processed or printed. Table 9-13 depicts a KPI that measures the percentage of media passing the sanitization procedures testing, compared to all the media that have been tested.

Field	Data
Measure ID	Media Sanitization measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To sanitize or destroy information system media before disposal or release for reuse.
Measure	The measure is the percentage (%) of media that passes sanitization procedures testing.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of media that passes sanitization procedures testing/total number of media tested)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> Is there a policy for sanitizing media before it is discarded or reused? <input type="checkbox"/> Yes <input type="checkbox"/> No Does the organization test media sanitization procedures for high-impact systems? <input type="checkbox"/> Yes <input type="checkbox"/> No Number of media that successfully passed sanitization testing for high-impact systems? _____ Total number of media tested for FIPS high-impact systems? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the facility security officer). <i>Information collector:</i> This is defined by the organization (for example, system owner, information system security officer [ISSO]). <i>Information customer:</i> This could be the chief information officer (CIO) or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the sanitization testing results.
Reporting Format	This is a pie chart comparing the percentage of media passing sanitization procedures testing versus the percentage of media not passing sanitization procedures testing over the specified period.

Table 9-13 Media Sanitization Measure (Adapted from NIST Special Publication 800-55)

Physical and Environmental Protection As a risk professional, you need to be aware of how perimeter and physical controls are used to protect your systems and people. Physical controls are used to complement administrative and technical controls by controlling physical access to information systems and areas and to protect the people who work in the facility housing the systems in those areas. Organizations should limit access to their systems, equipment, and the environments housing them. Organizations should also protect systems against environmental hazards through the use of environmental controls. Table 9-14 presents a KPI measuring the percentage of physical security incidents allowing unauthorized entry into facilities containing information systems.

Field	Data
Measure ID	Physical Security Incidents measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's information resources.
Measure	The measure is the percentage (%) of physical security incidents allowing unauthorized entry into facilities containing information systems
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of physical security incidents allowing unauthorized entry into facilities containing information systems/total number of physical security incidents)*100.
Target	This should be a low percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> How many physical security incidents occurred during the specified period? _____ How many of the physical security incidents allowed unauthorized entry into facilities containing information systems? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, quarterly).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the physical security officer). <i>Information collector:</i> This is defined by the organization (for example, the computer security incident response team [CSIRT]). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the physical security incident reports and physical access control logs.
Reporting Format	This is a pie chart comparing the physical security incidents allowing unauthorized entry into facilities containing information systems versus the total number of physical security incidents.

Table 9-14 Physical Security Incidents Measure (Adapted from NIST Special Publication 800-55)

Planning NIST Special Publication 800-55 states that “[organizations] must develop, document, periodically update, and implement system security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.” An example of this type of policy, the acceptable use policy (AUP), is designed to list the things that are not allowed on company devices or traffic that is not allowed to traverse the company infrastructure. This generally includes things such as pornography, gaming, and stock trading. Table 9-15 presents a KPI measuring the percentage of employees who are authorized access to information systems only after they sign an acknowledgment that they have read and understood rules of behavior, such as an AUP.

Field	Data
Measure ID	Planning measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for information systems and the rules of behavior for individuals accessing these systems.
Measure	This is the percentage (%) of employees who are authorized access to information systems only after they sign an acknowledgment that they have read and understood rules of behavior.
Type	Implementation.
Formula	The formula is as follows: (Number of users who are granted system access after signing rules of behavior/total number of users with system access)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> How many users access the system? _____ How many users signed rules of behavior acknowledgments? _____ How many users have been granted access to the information system only after signing rules of behavior acknowledgments? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information Owner:</i> This is defined by the organization (for example, the system owner and information system security officer [ISSO]). <i>Information Collector:</i> This is defined by the organization (for example, the system administrator and system owner). <i>Information Customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the repositories containing rules of behavior records.
Reporting Format	This is a pie chart comparing the percentage of users who have signed an AUP prior to being granted access to the system, versus users who have accessed the system without signed AUPs.

Table 9-15 Planning Measure (Adapted from NIST Special Publication 800-55)

Personnel Security Personnel security addresses the requirements for how personnel interact with systems and data. For example, company personnel security policy may require background checks and security clearances for employees who require access to highly sensitive data, including third-party service providers. These background checks often include criminal checks, credit reporting agency checks, and so on. Another example of a personnel security policy might include those that describe separation of duties, job rotation, mandatory vacations, termination procedures, and sanctions in the event of violation. These policies might be included to prevent fraud, misuse of assets, and collusion. Table 9-16 provides a KPI that details the percentage of personnel who have received screening before receiving access to organizational information systems.

Field	Data
Measure ID	Personnel Security Screening measure.
Goal	<ul style="list-style-type: none"> • <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • <i>Information Security goal:</i> To ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.
Measure	The measure is the percentage (%) of individuals screened before being granted access to organizational information and information systems.
Type	Implementation.
Formula	The formula is as follows: (Number of individuals screened/total number of individuals with access)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> 1. How many individuals have been granted access to organizational information and information systems? _____ 2. What is the number of individuals who have completed personnel screening? _____
Frequency	<ul style="list-style-type: none"> • <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). • <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> • <i>Information owner:</i> This is defined by the organization (for example, human resources). • <i>Information collector:</i> This is defined by the organization (for example, system administrators, system owners, or information system security officer [ISSO]). • <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes clearance records and access control lists.
Reporting Format	This is a pie chart comparing the percentage of individuals screened versus the total number of individuals.

Table 9-16 Personnel Security Screening Measure (Adapted from NIST Special Publication 800-55)

Risk Assessment Remember that risk is a combination of several elements: assets, vulnerabilities, threats, threat agents, likelihood, and impact, and that a risk assessment is essentially the activities focusing on collection of information (threats, assets, vulnerabilities, and impacts) and analyzing that information to determine the degree of damage and impact to a system or business from threats. Organizations should consider the risk to their missions, their assets, and their reputation (which is much harder to quantify). Table 9-17 is a KPI to measure the percentage of high vulnerabilities mitigated within organizationally defined time periods after their discovery.

Field	Data
Measure ID	Risk Assessment Vulnerability measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security goal:</i> To ensure all vulnerabilities are identified and mitigated.
Measure	The measure is the percentage (%) of high vulnerabilities mitigated within organizationally defined time periods after discovery.
Type	Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of high vulnerabilities identified and mitigated within targeted time frame during the time period/number of high vulnerabilities identified within the time period)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> Number of high vulnerabilities identified across the enterprise during the time period? _____ Number of high vulnerabilities mitigated across the enterprise during the time period? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, quarterly).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This could be the chief information officer (CIO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO]), or system owner. <i>Information collector:</i> This could be the system administrator or information system security officer (ISSO). <i>Information customer:</i> This could be the chief information officer (CIO) or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the following: vulnerability scanning software, audit logs, vulnerability management systems, patch management systems, change management records.
Reporting Format	This is a stacked bar chart illustrating the percentage of high vulnerabilities closed within targeted time frames after discovery over several reporting periods.

Table 9-17 Risk Assessment Vulnerability Measure (Adapted from NIST Special Publication 800-55)

System and Communications Protection Organizations should protect their communications at internal and external boundaries and employ principles to ensure the protection of those communications. Cryptography is a common way to protect communications because it is, in the most basic sense, the practice of hiding information. Cryptography is used to keep information confidential so only people who are authorized to view it and interact with it can do so. Table 9-18 provides a KPI that measures

Field	Data
Measure ID	System and Communication Protection measure.
Goal	<ul style="list-style-type: none"> <i>Strategic goal:</i> To accelerate the development and use of an electronic information infrastructure. <i>Information Security goal:</i> To allocate sufficient resources to adequately protect electronic information infrastructure.
Measure	The measure is the percentage (%) of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.
Type	Implementation.
Formula	The formula is as follows: (Number of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation/total number of mobile computers and devices) *100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> How many mobile computers and devices are used in the organization? _____ How many mobile computers and devices employ cryptography? _____ <ol style="list-style-type: none"> How many mobile computers and devices employ FIPS 140-2 validated encryption modules? _____ How many of those mobile computers and devices perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation? _____ How many mobile computers and devices have cryptography implementation waivers? _____
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, quarterly). <i>Reporting frequency:</i> This is defined by the organization (for example, annually).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, system owners or the information system security officer [ISSO]). <i>Information collector:</i> This is defined by the organization (for example, system administrators, system owners, or information system security officer [ISSO]). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes the system security plans.
Reporting Format	This is a pie chart illustrating the number of mobile computers and devices that perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation as a percentage of the total number of mobile computers and devices.

Table 9-18 System and Communication Protection Measure (Adapted from NIST Special Publication 800-55)

the percentage of systems that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation. FIPS 140-2 is a U.S. government standard for accrediting cryptographic modules.

System and Information Integrity Integrity is a goal for ensuring that data and systems are maintained in a pristine, unaltered state, unless the alteration is intended because of normal processing. In other words, you want no unauthorized modification, alteration, creation, or deletion of data, and any changes to data must be only as part of authorized transformations in normal use and processing. Integrity can be maintained by the use of a variety of checks and mechanisms, including data checksums, comparison with known or computed data values, and cryptographic means. To ensure integrity, organizations should understand their system baseline and track any changes to it. They also should track vulnerabilities to the systems and apply patches when applicable. Table 9-19 presents a percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated.

Field	Data
Measure ID	System and Information Integrity measure.
Goal	<ul style="list-style-type: none"> • <i>Strategic goal:</i> To accelerate the development and use of an electronic information infrastructure. • <i>Information Security goal:</i> To provide protection from malicious code at appropriate locations within organizational information systems, monitor information systems security alerts and advisories, and take appropriate actions in response.
Measure	The measure is the percentage (%) of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated.
Type	Implementation and Effectiveness/Efficiency.
Formula	The formula is as follows: (Number of vulnerabilities addressed in distributed alerts and advisories for which patches have been implemented, determined as nonapplicable, or granted a waiver/total number of applicable vulnerabilities identified through alerts and advisories and through vulnerability scans)*100.
Target	This should be a high percentage defined by the organization.
Implementation Evidence	<ol style="list-style-type: none"> 1. Does the organization distribute alerts and advisories? <input type="checkbox"/> Yes <input type="checkbox"/> No 2. How many vulnerabilities were identified by analyzing distributed alerts and advisories? _____ 3. How many vulnerabilities were identified through vulnerability scans? _____ 4. How many patches or workarounds were implemented to address identified vulnerabilities? _____ 5. How many vulnerabilities were determined to be nonapplicable? _____ 6. How many waivers have been granted for weaknesses that could not be remediated by implementing patches or workarounds? _____

Table 9-19 System and Information Integrity Measure (Adapted from NIST Special Publication 800-55) (*continued*)

Field	Data
Frequency	<ul style="list-style-type: none"> <i>Collection frequency:</i> This is defined by the organization (for example, weekly). <i>Reporting frequency:</i> This is defined by the organization (for example, monthly).
Responsible Parties	<ul style="list-style-type: none"> <i>Information owner:</i> This is defined by the organization (for example, the computer security incident response team [CSIRT]). <i>Information collector:</i> This is defined by the organization (for example, information system security officer [ISSO] or system owners). <i>Information customer:</i> This could be the chief information officer (CIO), information system security officer (ISSO), or senior agency information security officer (SAISO) (for example, chief information security officer [CISO]).
Data Source	This includes vulnerability scans, POA&Ms, repositories of alerts and advisories, and risk assessments.
Reporting Format	This is a stacked bar chart with the total number of applicable vulnerabilities composed of percentages of number of vulnerabilities addressed in distributed alerts and advisories for which patches have been determined as nonapplicable, have been implemented, have had a waiver granted, or other.

Table 9-19 System and Information Integrity Measure (Adapted from NIST Special Publication 800-55)

Chapter Review

In this chapter, we discussed how you can assess and monitor the efficiency and effectiveness of controls and risk through the use of key performance indicators. KPIs are used to understand and enable the measurement of control performance. KPIs should be specific, measurable, attainable, relevant, and timely. We discussed the template for KPIs adapted from NIST Special Publication 800-55 and presented KPIs associated with availability; configuration management; system and services acquisition; contingency planning; access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; system and communications protection; and system and information integrity.

Review Questions

- When a KPI is S.M.A.R.T., it is which of the following? (Choose all that apply.)
 - Short
 - Measurable
 - Right
 - Timely

2. It's critical when developing a KPI that you use which of the following? (Choose all that apply.)
 - A. A standard format
 - B. An industry best practice
 - C. NIST frameworks
 - D. Evidence
3. The KPI category of _____ deals with maintaining baselines of systems and applications.
 - A. Awareness and training
 - B. Audit and accountability
 - C. Access control
 - D. Configuration management
4. The KPI should include a statement of whether it measures which of the following? (Choose all that apply.)
 - A. Effectiveness
 - B. Accountability
 - C. Efficiency
 - D. Impact
5. The KPI measure should be a _____ statement.
 - A. Strong
 - B. Numeric
 - C. Simple
 - D. Qualitative
6. The CISO wants to understand how the organization's KPI implementation metrics are trending weekly because there is a concern that the schedule is slipping. What is the KPI consideration that will make sure the data is collected on a timely basis?
 - A. Frequency
 - B. Evidence
 - C. Target
 - D. Data source
7. Who will receive the data from a KPI?
 - A. Information owner
 - B. Information collector
 - C. Information customer
 - D. Information analyst

Answers

1. **B, D.** KPIs should be S.M.A.R.T. to be most effective. This stands for specific, measurable, attainable, relevant, and timely.
2. **A, D.** When developing a KPI, you should use a standard format that includes fields, such as a name to track the KPI by and the target for success. You should also include evidence that supports the KPI findings, such as logs. Industry best practices and the NIST frameworks are certainly great options to incorporate but are not critical to KPI development.
3. **D.** The principles of configuration management state that organizations must establish and maintain baseline configurations and inventories of organizational information systems. All others are KPIs measuring other principles.
4. **A, C, D.** When developing a KPI, you should include a statement of whether the measure is implementation, effectiveness/efficiency, or impact. Accountability is a goal but is not a measure.
5. **B.** The KPI should be measured with a numeric statement. All other considerations are incorrect or secondary considerations for the metric choice.
6. **A.** The frequency of the data indicates how often the data is collected and analyzed and how often the data is reported. In this situation, you would choose a frequency, such as weekly, based on the CISO requirements. No other option meets the CISO needs.
7. **C.** The individual who will receive the data from a KPI is the information customer. This is perhaps the person responsible for reporting the KPI status. The individual who owns required pieces of information is the information owner. The information collector is responsible for collecting the data. Information analysts can detect trends and provide situational awareness but are not the primary information customer.

This page intentionally left blank

The NIST Risk Management Framework

We've discussed the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) throughout this book, albeit in specific pieces relevant to the context of each chapter. Here, in Appendix A, we've gathered this information all in one place, for easier reference and understanding. The NIST RMF is not testable on the exam; however, you'll find that more and more risk management professionals are being exposed to it and having to learn and apply it to their own organization's risk management strategy and programs. If you work in the U.S. government, compliance with the RMF is becoming mandatory by almost all government agencies and, by extension, to their contractors and anyone else they exchange official information with. If you work in a medical facility, such as a doctor's office, clinic, or hospital, you may have to apply the NIST RMF to your organization's risk management program because HIPAA recommends the RMF and NIST controls in its implementation guidance. In the private/commercial world, the RMF also has value in that it is comprehensive and tailorabile and it provides solid, in-depth guidance for managing information risk throughout its life cycle for organizations of almost any size. Additionally, it's free. That can't be said for some of the other risk management frameworks discussed throughout the book because their standards can cost a great deal and because finding people specially trained in those standards to help administer them in a risk management program can also be difficult and more costly. Yet another good reason for using the NIST RMF is its generality and interoperability with almost any other risk management framework you can find. All in all, the NIST RMF is the risk management framework of choice for many organizations. That's not to say it fits every situation or organization; as we've stated in the book, other frameworks may be more appropriate to use, either in place of or in conjunction with NIST, because of unique industry, market, and operating environment factors or governance standards.

NIST's Risk Management Framework is the product of many years of research and refinement by the U.S. government and NIST, based upon research, standardization throughout the industry, best practices, and recommendations from security professionals just like you. NIST employs a staff of experienced security professionals who come from all different aspects of the information security world, whose full-time job it is to develop and continually improve the standards that make up the Risk Management Framework. In this appendix, we'll discuss the RMF, including its applicability, publications, and detailed steps.

Overview

The Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, also known as FISMA) is Title III of the E-Government Act of 2002. This act requires that federal agencies develop, document, and implement agencywide programs to ensure information security for the systems and data under their control. FISMA tasked NIST to develop the standards that federal organizations must use to secure their information systems and data. The result was the Risk Management Framework, which was initially developed in 2005 and has been through several iterations. The framework provides all supporting publications, controls, and assessment methods for its implementation, although all agencies typically implement it a bit differently, according to their own needs and regulations. For example, the Department of Defense implements the RMF differently than the Department of the Treasury would, because it applies RMF to military weapons systems versus financial and record-keeping systems.

Tiered Approach

You'll notice in Figure A-1 that the NIST RMF looks at risk at three separate levels, or *tiers*. The first tier, the organizational level, looks at risk from a management and governance perspective (that is, from the top down) at the strategic level. At this level, risk isn't looked at from a technical perspective; it is viewed in terms of risk governance, the organization's risk appetite and tolerance levels, its risk management processes, and its overall risk strategy. Policies, procedures, and standards are also examined at this level (and may be examined at lower levels as well) to determine how they articulate with higher-level governance and to ensure they support the overall risk strategy of the organization.

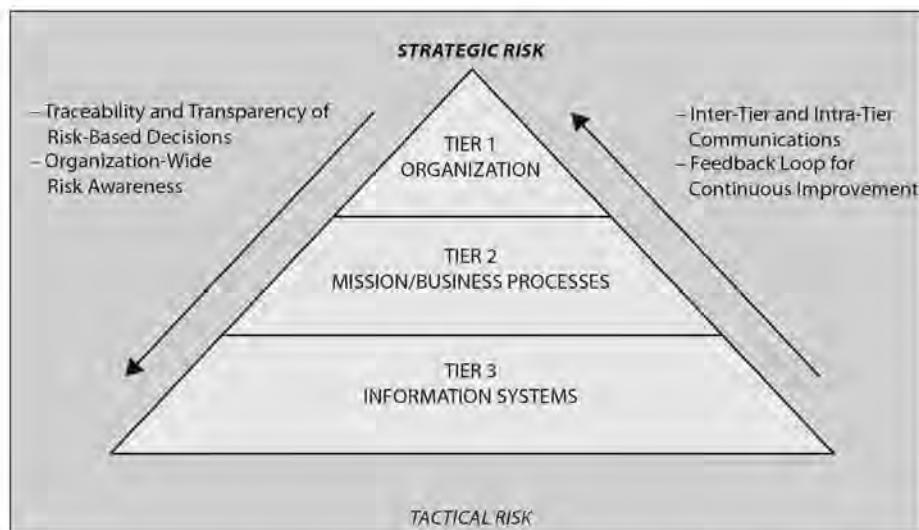


Figure A-1 The Risk Management Framework tiered approach (from NIST SP 800-53, revision 4)

At the second tier, encompassing mission and business processes, business functions are examined. These functions are the core of the business or organization, and they cover major business areas and their related processes, as well as the processes that interact with and between different business areas. An example of this process may be particular policies and procedures that relate to privacy or data sensitivity, for example. Technical risk is also not examined at this level; it's more at an operational level that risk is managed. Policies, procedures, and processes that could affect multiple systems, business areas, and technical areas are the focus at this level.

The last tier concerns itself with the actual information systems in the organization and the risk they represent. This is the tactical level of risk. At this level, technical risk is definitely considered, but there's still an examination of policies, procedures, and processes, albeit from a specific information systems viewpoint. While viewing all three tiers at once gives a holistic view of risk throughout the organization, the RMF also allows practitioners to focus on risk at each of these three levels separately as well, depending on the needs of the organization in a specific set of circumstances. As Figure A-1 illustrates, however, communication and risk awareness travel throughout all three levels, in both directions.

Applicability

As mentioned, the RMF is required for use by most U.S. government organizations. Even the Department of Defense, which previously had its own unique security management framework, called the Defense Information Assurance Certification and Accreditation Program (DIACAP), has begun the process of converting to the risk management framework. Even nongovernmental agencies that do business with the federal government, such as contractors, for example, may be subject to the RMF as part of their contractual agreements with the government. Also, private organizations, while not required to use the RMF, may certainly find it useful since it is a matured, developed process that can be applied and scaled to any information system or organizational infrastructure. An organization's governance may recommend or require the RMF as an adopted and enforced standard.

As far as scaling goes, the RMF can be applied to both small and large organizations. The RMF is both tailorabile and scalable, allowing organizations to follow the steps, use the controls, and assess risk on one system or a thousand. The RMF can be applied to a wide variety of industries and market segments, including healthcare organizations, industrial control systems, administrative and general service systems, and even special-purpose systems.

Publications

The core document of the RMF is Special Publication 800-37, but the entire NIST library of special publications could be considered part of the RMF because steps in the process often require performance to a relevant standard published by NIST. For example, cryptographic controls in SP 800-53 must meet the requirements set forth in Federal Information Processing Standards (FIPS) 140-1 and 140-2, although these publications aren't necessarily part of the RMF. You can see that you could conceivably go down a great many "rabbit holes" while navigating the RMF and going through each

step, as well as implementing the NIST controls. Table A-1 lists the most commonly used publications related to the RMF, in order by publication number. The table also lists the applicable RMF steps and describes the publication. Note that although the RMF prescribes particular publications for each step, in practice you'll find that you may use more publications than those specifically assigned to a step, and in some cases you may actually use some of these publications, as well as others, throughout all six steps.

RMF Steps

Although there are six steps listed in the RMF process, each step has many subprocesses to it. While NIST does not necessarily prescribe a rigid set of processes for each step, each organization to use the RMF must develop its own internal processes to support RMF steps. Although these were presented earlier in the book, we'll discuss the steps again here to bring all of this into context with other discussions of the RMF. Figure A-2 shows the high-level view of the RMF life cycle, depicted in six steps.

Although this life cycle seems to be sequential and ending with step 6, keep in mind that this is a continual process, and often previous steps must be revisited. For example, assessing security controls must be done on a frequent basis, to make sure those controls are still effective and mitigate the risk for which they were intended. Keep in mind that the typical risk management activities involving threat and vulnerability assessment also occur throughout all six steps, and the security posture of information systems, including adjustments to controls, are maintained accordingly based upon those assessments.

Step 1: Categorize Information Systems

This step involves identifying information and information systems belonging to the organization and assigning categories to that information based upon the level of impact if the security goals of confidentiality, integrity, and availability were affected or compromised for that particular information or system. This step uses subjective values of high, moderate, and low to assign values to each of the three goals for a particular type of information. Types of information processed on the system may include business-sensitive information, financial information, protected health information, and so on. FIPS 199 (as well as NIST Special Publication 800-60) provides detailed guidance on categorizing information systems. While FIPS 199 provides detailed information on security impact ranges (high, moderate, and low) and how they affect the security goals of confidentiality, integrity, and availability, 800-60 helps the organization decide which types of information map to which security impact levels. For example, SP 800-60 could assist the organization in finding the right type of security impact level for company-sensitive or proprietary information, in line with what FIPS 199 describes. Chapter 8 goes into detail on the security categorization process.

Step 2: Select Security Controls

Once information and systems have been categorized, the organization has to select the appropriate security controls assigned to each information system. This step provides baselines of security controls based upon the high, moderate, and low values assigned

Publication	Applicable RMF Step	Brief Description
FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems	Step 1: Categorize Information Systems	Establishes security categories for both data and information systems; assists in determining impact to the confidentiality, integrity, and availability aspects of systems
FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems	Step 2: Select Security Controls	Specifies minimum security requirements for federal information and information systems in 17 security-related areas
SP 800-30, "Guide for Conducting Risk Assessments"	Step 4: Assess Security Controls	Provides guidance for identifying and assessing risk
SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"	Step 5: Authorize Information Systems	Establishes and details the Risk Management Framework and its related processes
SP-800-39, "Managing Information Security Risk: Organization, Mission, and Information System View"	All	Explains how organizations frame, assess, respond to, and monitor risk; defines three tiers of risk management (organizational level, mission and business processes, and information systems)
SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"	Step 2: Select Security Controls	Catalogs the defined security controls
SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans"	Step 4: Assess Security Controls	Provides assessment guidance for each of the controls listed in SP 800-53
SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"	Step 1: Categorize Information Systems	Assists in mapping various types of information (financial, health, privacy, proprietary, and so on) to security impact levels
SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations"	Step 6: Monitor Security Controls	Provides guidance on how to continuously monitor the security posture of an organization's assets, ensuring that risk response strategies maintain effectiveness and monitoring for changes in risk factors for the operating environment of the organization and its assets
SP 800-160, "Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems" (still in draft form as of this writing)	Step 3: Implement Security Controls	Provides the systems security engineering approach to designing and building secure systems throughout their life cycle

Table A-1 NIST Publications Applicable to the Risk Management Framework

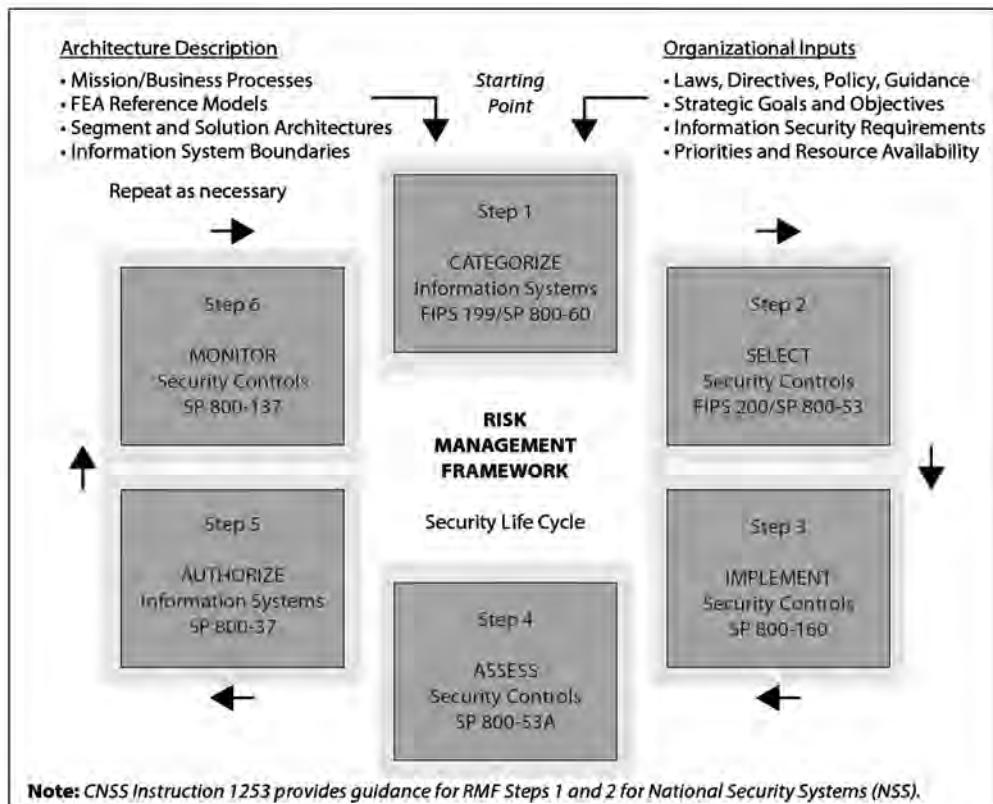


Figure A-2 The NIST Risk Management Framework (From NIST SP 800-53, revision 4)

during step 1. It uses high water marks for information to determine security baselines. So, if the aggregate value of information or a system has been rated as *high*, for example, then the high baseline of security controls is employed for that system. Once the security control baseline has been established, the organization has the latitude and flexibility to add or subtract security controls from the baseline as it sees fit based upon different factors including the applicability of some controls, the environment the system operates within, specific organizational governance, or even other risk factors. Controls are typically selected from SP 800-53 and combined with any other control frameworks the organization is required to use.

Step 3: Implement Security Controls

Once security controls have been selected, they are implemented on information systems and infrastructures that house and manage them. Some controls might be applicable to several different systems or types of data or to two different areas within the facility. These are usually considered *common controls*. Controls that are specific to a particular

system or a type of data are also applied, although using the principles of economy of use and effectiveness, limited-use controls should be kept to a minimum. Controls should be applied as much as possible that can cover several types of data and information systems and must also be consistent with other infrastructure components for interoperability purposes. Refer to Chapters 7 and 8 for more information on controls in different control frameworks. In this step, the organization is essentially securing the information system against any validated threats and reducing identified vulnerabilities. The RMF identifies SP 800-60 as a guiding publication for this since it covers the entire SDLC, but you'll also find that this publication should be consulted early on in the system's life cycle, before the system is even built or acquired. Additionally, special attention should be paid to the control details and implementation guidance as laid out in SP 800-53.

Step 4: Assess Security Controls

Chapter 4 detailed how security controls are assessed. During this step, the controls that the organization selects for the information system are formally verified that they have been implemented correctly and validated that they perform as they were designed. Controls are assessed based upon their effectiveness in protecting against the threats they were implemented to protect against. During this step, the system is assessed in its current state, with all existing controls and mitigations in place. Based upon the assessment, there may be recommendations for further controls and mitigations, as well as alterations to existing controls. In this step, the level of risk to the system and its data is normally analyzed and determined. NIST SP 800-53A provides detailed guidance on assessing security controls, and SP 800-30 provides excellent guidance on the assessment process in general. Both should be consulted during this step of the RMF.

Step 5: Authorize Information Systems

FISMA (and by extension, NIST) calls for a designated official who is legally responsible for determining risk and allowing a system to go into operation. In NIST terminology, this designated person is called the *authorizing official* (AO) and is normally a senior person in the organization, such as the CIO. In step 5, the authorizing official formally makes the decision to authorize a system (or not) to be implemented and put into operation. The authorizing official bases this decision upon various factors, including the level of risk assessed during step 4, the risk appetite the organization has settled on, and the tolerance for risk that the organization is willing to accept. The decision to authorize a system for use may also come with caveats, including conditional authorization based upon the plan going forward for the continued mitigation and reduction of risk, usually agreed to and implemented by the system or data owner. The authorization is the formal authority for the system to operate, made by someone with the legal authority to make that decision. It is typically in writing and valid for only a specified period of time, after which the system must be reassessed for risk and control compliance, although the theory of continuous monitoring (detailed next) suggests that the security posture of a system should be constantly reassessed based upon different factors and changes in the operating environment. NIST SP 800-37, which details the RMF, provides further information on the authorization process.

Step 6: Monitor Security Controls

Continuous monitoring of security controls defines step 6 in the RMF; just because an authorization decision is rendered doesn't mean that the system will now be operated forever without continually monitoring its security posture for new or increased risks. Existing controls will be monitored for continued compliance and effectiveness against identified threats, new risks will be occasionally discovered for the system as new threats and vulnerabilities are identified, and the system will have to be reauthorized after a certain period of time. Note that the RMF is a cyclical process; all these steps will be re-accomplished for each system at various times over the system's life cycle. As mentioned, even after an authorization decision has been rendered by an authorizing official, continuous monitoring indicates that a system will be checked and validated on a continual basis, not merely in the lead-in to its next authorization decision. NIST SP 800-137 details the continuous monitoring process.

ISACA's Risk IT Framework

We've discussed the ISACA's Risk IT Framework, as well as the NIST RMF, throughout this book, albeit in specific pieces relevant to the context of each chapter. Here, in Appendix B, we've gathered this information all in one place, for easier reference and understanding. The Risk IT Framework is not testable on the exam; however, you'll find that many unique ISACA concepts and terms on the exam come from the framework, so it's a good idea to be familiar with it. In this appendix, we'll discuss some particulars about the framework, including its relationship to COBIT 5 and the Val IT framework. We'll also break down some of the processes the framework describes.

ISACA published the Risk IT Framework in 2009, and it was a joint effort from many different industry partners and professionals. The framework is not simply a product of the United States, like the NIST framework is, but was developed and influenced by professionals and organizations from all over the world. Because ISACA is an independent professional organization and not tied to any particular governmental organization, the framework is suitable for deployment and use not only in the United States but everywhere in the world. This makes it especially attractive to non-U.S. entities that prefer not to use the NIST framework or to entities for which the NIST framework doesn't satisfy their needs. ISACA's framework is a subset of COBIT 5, which covers management and governance principles, processes, and requirements. The Risk IT Framework approaches risk from business perspective, while integrating IT risk into the overall risk management process for the organization.

Overview

The framework is based on COBIT 5 and, as such, articulates well with COBIT, as well as Val IT, since COBIT version 5 has absorbed that framework as well. The terminology, organization, processes, and concepts all articulate with each other, making it much easier to integrate all three in a comprehensive risk management strategy. The framework is broken down into several sections, which explain its purpose, its intended audience, and the benefits and outcomes of using the framework. It also describes basic risk IT principles before going into the meat of the framework. The three basic concepts of the Risk IT Framework include Risk Governance, Risk Evaluation, and Risk Response. There are major sections devoted to each of these three key areas. The framework emphasizes that IT risk is,

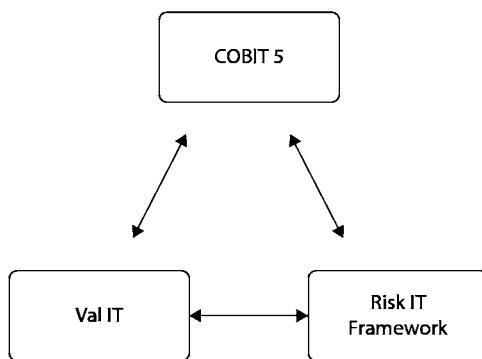
in fact, business risk; either it is an entity that benefits and adds value to the organization by providing opportunities for growth or it can create negative situations by increasing risk, via not protecting and preserving assets, which could result in business failure or, at minimum, missed opportunities as well as liabilities. The framework embraces enterprise risk management (ERM) principles, such as those found in the COSO framework and other frameworks, but does not necessarily require their implementation in order to be used. However, the use of ERM may be a necessary foundation for the successful implementation of the Risk IT Framework. The framework also discusses the integration of the COBIT, Val IT, and Risk IT frameworks. Essentially, COBIT covers IT management and governance practices from a top-down view. The Risk IT Framework focuses specifically on risk management, and, of course, Val IT is concerned with gaining value from an organization's IT portfolio. Although included in Chapter 7, for reference sake, the COBIT 5 and Val IT framework controls are included here in Tables B-1 and B-2, respectively.

Figure B-1 illustrates the relationship between these three frameworks.

The relationships between these controls are complementary; that is, they are not subsets of each other, nor are they interchangeable with each other. They can be mapped to each other, however, and since we are discussing the Risk IT Framework primarily here, it's worth noting that the appropriate and applicable COBIT and Val IT controls are mapped to the various processes that make up the Risk IT Framework. As they all cover different context areas, they are used in unison to cover management and governance, IT portfolio value, and risk management areas of an organization.

Finally, the framework's glossary and its higher-level mapping to other frameworks and standards round it out as a practical standard to reference in establishing and maintaining a solid risk management strategy. The framework is freely available from ISACA as a downloadable document; however, there are other documents that are necessary to implement the framework that require you become a member of ISACA to access. We'll discuss a few of those later in this appendix.

Figure B-1
The relationships
between the
COBIT, Val IT,
and Risk IT
Frameworks



Domain	Control
Governance Processes: Evaluate, Direct, and Monitor (EDM)	<ul style="list-style-type: none"> • EDM01: Ensure Governance Framework Setting and Maintenance • EDM02: Ensure Benefits Delivery • EDM03: Ensure Risk Optimization • EDM04: Ensure Resource Optimization • EDM05: Ensure Stakeholder Transparency
Management Domain: Align, Plan, and Organize (APO)	<ul style="list-style-type: none"> • APO01: Manage the IT Management Framework • APO02: Manage Strategy • APO03: Manage Enterprise Architecture • APO04: Manage Information • APO05: Manage Portfolio • APO06: Manage Budget and Costs • APO07: Manage Human Resources • APO08: Manage Relationships • APO09: Manage Service Agreements • APO10: Manage Suppliers • APO11: Manage Quality • APO12: Manage Risk • APO13: Manage Security
Management Domain: Build, Acquire, and Implement (BAI)	<ul style="list-style-type: none"> • BAI01: Manage Programs and Projects • BAI02: Manage Requirements Definition • BAI03: Manage Solutions Identification and Build • BAI04: Manage Availability and Capacity • BAI05: Manage Organizational Change Enablement • BAI06: Manage Changes • BAI07: Manage Change Acceptance and Transitioning • BAI08: Manage Knowledge • BAI09: Manage Assets • BAI10: Manage Configuration
Management Domain: Deliver, Service, and Support (DSS)	<ul style="list-style-type: none"> • DSS01: Manage Operations • DSS02: Manage Service Requests and Incidents • DSS03: Manage Problems • DSS04: Manage Continuity • DSS05: Manage Security Services • DSS06: Manage Business Process Controls
Management Domain: Monitor, Evaluate, and Assess (MEA)	<ul style="list-style-type: none"> • MEA01: Monitor, Evaluate, and Assess Performance and Conformance • MEA02: Monitor, Evaluate, and Assess the System of Internal Control • MEA03: Monitor, Evaluate, and Assess Compliance with External Requirements

Table B-1 COBIT 5 Domains and Controls

Applicability

The Risk IT Framework can be applied to almost any organization but typically works better in organizations that have a solid infrastructure and are more mature with regard to attitudes toward risk and risk appetite and tolerance and have the people and resources to implement it. As mentioned, since its development was influenced by international

Domain	Control
Value Governance (VG)	<ul style="list-style-type: none"> • VG1: Establish informed and committed leadership • VG2: Define and implement processes • VG3: Define portfolio characteristics • VG4: Align and integrate value management with enterprise financial planning • VG5: Establish effective governance monitoring • VG6: Continuously improve value management practices
Portfolio Management (PM)	<ul style="list-style-type: none"> • PM1: Establish strategic direction and target investment mix • PM2: Determine the availability and sources of funds • PM3: Manage the availability of human resources • PM4: Evaluate and select programs to fund • PM5: Monitor and report on investment portfolio performance • PM6: Optimize investment portfolio performance
Investment Management (IM)	<ul style="list-style-type: none"> • IM1: Develop and evaluate the initial program concept business case • IM2: Understand the candidate program and implementation options • IM3: Develop the program plan • IM4: Develop full life-cycle costs and benefits • IM5: Develop the detailed candidate program business case • IM6: Launch and manage the program • IM7: Update operational IT portfolios • IM8: Update the business case • IM9: Monitor and report on the program • IM10: Retire the program

Table B-2 Val IT Domains and Controls

professionals and organizations, it can be implemented all over the world. Since it uses higher-level processes, it can also be used in conjunction with other frameworks, such as NIST, PCI-DSS, and ISO/IEC standards, although the standards would typically be used to support the higher-level risk IT framework processes as lower-level controls. The Risk IT Framework also may be better suited for medium to large organizations that have the resources to adequately embrace it.

Publications

In addition to the basic Risk IT Framework document, you will probably need additional documents to gain a better understanding of the framework, as well as put it into practice. One particular publication is the *Risk IT Practitioner Guide*, which is a comprehensive document detailing practical approaches to the process model the Risk IT Framework promulgates. This document can be purchased only from ISACA or obtained for free by joining the organization. Other documents, some freely available and some available only to ISACA members, include those that focus on both COBIT and Val IT. An organization serious about implementing the Risk IT framework should not only

invest in professional membership in ISACA because this provides a wide variety of useful resources but also download and integrate all the necessary documentation required to implement the framework.

Framework Focus Areas

As mentioned, the framework focuses on three domains: Risk Governance, Risk Evaluation, and Risk Response. As discussed previously, different frameworks use many different terms for the same things, as well as combine or separate certain processes. The Risk IT Framework is no different in this regard; its domains and processes use particular terms and specific processes that you should understand for the exam, as well as be able to translate them to equivalent terms and processes in other frameworks. Each of these domains is decomposed into processes, as listed here:

1. Risk Governance (RG)
 - A. RG1: Establish and maintain a common risk view
 - B. RG2: Integrate with ERM
 - C. RG3: Make risk-aware business decisions
2. Risk Evaluation (RE)
 - A. RE1: Collect data
 - B. RE2: Analyze risk
 - C. RE3: Maintain risk profile
3. Risk Response (RR)
 - A. RR1: Articulate risk
 - B. RR2: Manage risk
 - C. RR3: React to events

We'll provide a detailed look at each of these domains and processes in the remainder of this appendix; however, you should also take the time to download the Risk IT Framework for yourself and read through it prior to the CRISC examination. This appendix merely summarizes the framework.

Risk Governance

Risk Governance covers areas that relate to developing the organization's risk appetite, its risk tolerance, and its entire culture and attitude with regard to risk. In this process, roles and responsibilities are defined, and relevant governance is examined for requirements that must be fulfilled in managing risk. Additionally, risk programs are established, particularly those that affect risk awareness and training. Communication guidelines between risk practitioners and managers, between managers and the general organizational populace,

and between other internal, as well as external communication lines, are defined. The Risk Governance domain covers three process areas, discussed in the next sections.

RG1: Establish and Maintain a Common Risk View

This process is broken down into several areas and involves performing an initial risk assessment to establish the organization's baseline. It also concurrently involves establishing and getting executive management approval for the organization's risk appetite and tolerance levels. These are written into a risk policy and strategy, which is also developed at this stage. Finally, a risk awareness and training program is set up, and formal risk communication methods and rules are established and included in the policy.

RG2: Integrate with ERM

In this process, the organization's enterprise risk management (ERM) system is formally established, if it doesn't already exist, and further definition of roles and responsibilities are refined and assigned. Risk ownership is a consideration during this stage because accountability for risk owners, as well as other key risk-related positions, is defined. Also in this part of the process, the overall IT strategy is examined and made to align with business strategy, if this has not already been accomplished. This includes a consideration of the relationship of IT risk to business risk, as well as how IT infrastructure supports the mission and functions of the organization.

IT risk management processes and practices are mapped to business risk management processes during this part of the framework and modified or supplemented as necessary to align with the organizational risk management strategy. IT risk management programs are also established, with emphasis given to adequately resourcing and staffing those programs with budgets, equipment, and trained personnel. Management processes and controls, including policies and other checks and balances, are used to ensure that risk management processes are being implemented and followed.

RG3: Make Risk-Aware Business Decisions

This process focuses on integrating risk management with sound decision making. Risk-based decisions are critical for the survivability in today's environment and market spaces. To get to this point of maturity in the organization's risk management capabilities, management must accept and support IT risk management processes and ensure that the entire organization conforms to security requirements. Management must also receive and approve accurate IT risk analysis reports, which assist them in making sound business decisions. They must carefully consider IT risk in all business decisions, understanding how IT risk affects business risk, and vice versa. In addition to accepting IT risk and making it part of the decision-making process, they must also carefully consider and prioritize IT risk responses.

Risk Evaluation

The Risk Evaluation processes in the ISACA framework cover risk identification and assessment. In RE processes, business impact is framed and described, and risk scenarios are also developed. Risks are assessed and analyzed, as well as presented to the organization's

management. The RE processes are further broken down into three process areas, which we will describe here in more detail.

RE1: Collect Data

The data collection process aligns with some of the risk identification processes previously described. During this process, risk management personnel develop a model for data collection, which provides for standardized data formats, measurements, and common data definitions. Data is collected on the various aspects of the organization and risk scenarios, including the business's operating environment, risk factors, threat sources and events, vulnerability data, and asset data. Data is also collected on the effectiveness of existing controls in the organization.

RE2: Analyze Risk

In this part of the Risk IT Framework, the organization begins to look at assessing and analyzing risk. First, it defines the risk analysis scope. The scope determines how broad and deep the risk analysis efforts will be, what areas the risk analysis will cover, and which assets will be examined for risk. To complete this part of the process, you'll need to consider all the documentation assembled up to this point: risk scenarios, asset inventories, breakdowns of business processes, prioritization of assets, and so on. This will help frame the risk analysis as well as determine scope.

During this step, IT risk is also estimated. This involves determining likelihood and impact values associated with the developed risk scenarios. You will also take into account existing controls and how effective they are as they are currently installed and functioning. Likelihood and impact values are also reevaluated after existing controls are considered.

Additionally, during this step of the ISACA process, you also identify and consider possible risk response options. The person assessing the risk may recommend several different response options, based upon the identified risk. What risk options an organization will actually make use of is determined later in the process and typically with the input and approval of senior management. Risk response options should be recommended that reduce risk to an acceptable level directly based upon the risk appetite and tolerance of the organization. Finally, risk analyses should be reviewed by knowledgeable peers to verify that the analysis process is sound and to validate the results.

RE3: Maintain Risk Profile

A *risk profile* is a collection of detailed data on identified IT risks. Risk profiles can certainly cover a single system or asset but are also often seen as describing risks on an organizational-wide basis. During this step of risk evaluation, a comprehensive document of identified risks and their characteristics, such as details regarding impact, likelihood, and contributing factors, is developed and maintained throughout the asset's or system's life cycle. Keep in mind that system or asset risk profiles are usually rolled up into a more comprehensive risk document that covers systems, assets, and business processes across the entire organization.

IT assets are also mapped to the business and organizational processes they support during this step; this helps translate IT risk to corresponding business risk and allows management to see how the organization would be affected if IT risk were realized on specific assets. This also allows the organization to develop criticality estimates of IT resources, from a business perspective. It's worth noting that this is similar to the same process followed during a business impact assessment (BIA). The key to understanding how IT risk affects business operations at this point is in understanding how the capabilities of IT are provided to the business processes in question and how critical IT is to a particular business process or operation. Maintaining a risk profile also means monitoring risk and updating risk scenarios and risk analysis as conditions and risk factors change. This involves keeping the risk register up to date as well. Finally, the organization should develop key risk indicators (KRIs) during this step, specifically focusing on IT resources. They allow the organization to monitor changes in risk for given scenarios, enabling the organization to modify its risk profiles as these indicators change.

Risk Response

Risk Response options are considered by management to reduce or offset risk, using the standard risk treatment options of risk avoidance, reduction or mitigation, sharing or transfer, and risk acceptance. In this process, the organization determines and communicates risks to all stakeholders actively managing the risk and reacting to risk events. We'll describe these processes next.

RR1: Articulate Risk

Articulating risk is done through several means, both formally and informally. Formal methods include analysis reports, the risk register, and other management products. Informally communicating risk involves the day-to-day interactions with risk professionals, risk and control owners, and others who actively work at both the technical and managerial levels to monitor and control risk on a daily basis.

During this process, the results of IT risk analysis are communicated to management and other stakeholders as necessary, using both formal and informal means. Communication has to be free-flowing and multidirectional, crossing internal organizational boundaries easily in order to ensure the risk management process is effective. Beyond analysis results, the operational and strategic-level risk management activities must be constantly communicated as needed. Compliance and risk level status must also be communicated as a priority to all stakeholders. In addition to internal risk management analysis and management activities, independent analysis and audit results must be briefed to all stakeholders to ensure that the organization's activities are validated and that they are on track with its program. Often these external findings must be analyzed, interpreted, and translated by risk practitioners into terms that management can understand, as well as to business functions and business risk. Additionally, during this step in the process, opportunities to expand or improve the IT infrastructure and its support for business processes can be identified.

RR2: Manage Risk

Managing risk is an ongoing, never-ending process. This part of the process occurs after a solid risk management plan and strategy have been established and risk owners, control owners, and risk practitioners (including all assigned organizational roles having assigned risk-related responsibilities) have been trained and are actively engaged in their procedures and processes. Controls are constantly inventoried and maintained, as well as monitored, to ensure they continue to meet security requirements. Business functions and ventures are also monitored to ensure that they operate within the established organizational levels of risk tolerance. This involves closely monitoring KPIs and KRIs. Based on careful and consistent risk monitoring, the organization responds to discovered risk, ideally before negative events occur, to prevent or reduce the impact of the event.

RR3: React to Events

In this process, the organization actively maintains incident response plans and continuously monitors IT risk and plans for risk events. When an event occurs, the organization executes its incident response plans, containing the incident, reducing damage, and performing analysis on the event. The organization should also be learning from the event, taking steps to change processes and add or supplement controls, adjusting risk management and incident response plans, and generally becoming more attuned to the changing threat landscape. Lessons learned are communicated to all stakeholders for action or heightened risk awareness.

This page intentionally left blank

About the Download

This e-book comes complete with Total Tester customizable practice exam software.

System Requirements

The Total Tester software requires Windows XP or higher and 30MB of hard disk space for full installation, in addition to a current or prior major release of Chrome, Firefox, Internet Explorer, or Safari. To run, the screen resolution must be set to 1024 × 768 or higher.

Downloading Total Tester Premium Practice Exam Software

To download the Total Tester software, simply click the link below and follow the directions for free online registration.

<http://www.totalsem.com/0071847146dl>

Total Tester Premium Practice Exam Software

Total Tester provides you with a simulation of the actual exam. You can also create custom exams from selected certification domains or chapters. You can further customize the number of questions and time allowed.

The exams can be taken in either Practice Mode or Exam Mode. Practice Mode provides an assistance window with hints, references to the book, explanations of the correct and incorrect answers, and the option to check your answers as you take the test. Exam Mode provides a simulation of the actual exam. The number of questions, the types of questions, and the time allowed are intended to be an accurate representation of the exam environment. Both Practice Mode and Exam Mode provide an overall grade and a grade broken down by certification domain.

To take a test, launch Total Tester and select the exam suite from the Installed Question Packs list. You can then select Practice Mode, Exam Mode, or Custom Mode. After making your selection, click Start Exam to begin.

Installing and Running Total Tester

Once you've downloaded the Total Tester software, double-click the Launch.exe icon. From the main screen you may install Total Tester by clicking the Install Total Tester Practice Exams link. This will begin the installation process and place an icon on your desktop and in your Start menu. To run Total Tester, navigate to Start | (All) Programs | Total Seminars, or double-click the icon on your desktop.

To uninstall the Total Tester software, go to Start | Settings | Control Panel | Add/Remove Programs (XP) or Programs And Features (Vista/7/8), and then select the Total Tester program. Select Remove, and Windows will completely uninstall the software.

Technical Support

Technical Support information is provided in the following sections by feature.

Total Seminars Technical Support

For questions regarding the Total Tester software, visit www.totalsem.com or e-mail support@totalsem.com.

McGraw-Hill Education Content Support

For questions regarding book content, e-mail customer.service@mheducation.com. For customers outside the United States, e-mail international_cs@mheducation.com.

acceptable use policy (AUP) Organizational policy that describes both acceptable and unacceptable actions when using organizational computing resources, as well as the consequences of violating the policy.

access control The processes and technologies involved in protecting information, systems, and data against unauthorized disclosure, modification, or loss through the control of access to those resources physically and/or logically.

accountability The ability to trace an action or event to a definitive user and to hold that user responsible for their actions.

active tools Tools that interact actively with a system and can often give you a more realistic perspective of vulnerabilities and the overall control effectiveness; can also cause performance issues.

assessment The process of determining whether a program or a project is meeting specified objectives and of determining whether the controls selected to protect the system are performing their desired function to the level required.

asset Anything of value to an organization; assets can include tangible items such as information, data, equipment, supplies, facilities, and systems, or intangible items such as customer loyalty and reputation.

auditing The process of reviewing different data sources, including log files and access control records, to determine compliance with security policy or detect deviations or anomalies.

authentication The process of validating credentials that a user has supplied to verify that they are the actual authorized user and that the credentials belong to that user.

authorization The process of giving authenticated users the proper accesses to systems, data, and facilities.

availability The goal of having information and systems available to authorized users whenever and however they need them.

business case Must be made if the response can't be quickly or easily implemented without a significant cost or change to the organization or the system. A business case for a risk response justifies the expense and work required to make the response function properly.

business continuity The process, generally detailed in a supporting plan, that keeps the company operating and functioning in the event of a power outage, IT malfunction, or major disaster.

business impact assessment The process of analyzing the critical missions and business processes and the systems used to complete those tasks and of determining the impact to the mission of a loss or disruption in access to those systems.

capability The ability for the organization to implement a risk response.

COBIT Control Objectives for Information and Related Technology (but now typically referred to by its acronym). This management and governance framework was developed and is used extensively by ISACA in its various risk management and business process frameworks. It is currently in version 5.

common controls Controls spanning the entire organization and protecting multiple assets rather than only a specific system. Physical controls are good examples of common controls, and the responsible entity for these controls would be the common controls provider.

confidentiality The goal of protecting systems and information from unauthorized disclosure.

control A measure put in place to increase protection for an asset, to make up for a lack of protection for an asset, or to strengthen a weakness for an asset. Controls can be administrative, technical, or physical and operational. They can also be further divided by functionality, including deterrent, preventative, detective, and so on.

control baseline The initial set of controls selected, based on security categorization, that are to be applied to systems and data and maintained throughout their life cycle.

control gap analysis The process of determining the difference between the existing state of a control's effectiveness and its desired state.

cost The financial impacts of any decision, as well as the less-easily quantified aspects such as loss of goodwill, loss of brand status, and other hard-to-define attributes. Cost also includes the maintenance of the responsive mitigation over its required life span.

data sensitivity The level of protection information or data required based upon its impact to the organization if it were disclosed to unauthorized people, subject to unauthorized modification, or otherwise lost.

deferral When risk response options simply don't make good business sense, risk is assumed temporarily, perhaps until the costs are reduced, alternate measures are adopted, or risk is ultimately accepted.

disaster recovery (DR) The process of reacting to an incident or disaster and recovering an organization, its personnel, and systems to a functioning state.

economy of use The design principle that states that you should attempt to design and implement controls that can be applied to more than one system or set of data or that provide more than one function in effectively mitigating risk. The goal is to minimize single-use controls (controls that apply only to a specific system or set of data) because they can be more expensive and specialized to implement.

effectiveness The extent to which the response reduces the likelihood or the impact of the risk event to the organization; also the degree and depth that a control fulfills its security requirements.

efficiency The interaction of a control with its environment, affecting factors such as cost, reliability, supportability, and interoperability.

exception management The documentation and tracking of accepted exceptions to policy.

false negative When a vulnerability isn't detected but it does actually exist.

false positive When a vulnerability is reported that isn't actually legitimate.

Family Educational Rights and Privacy Act (FERPA) U.S. law designed to protect the privacy of students in educational institutions. FERPA covers access control over data, as well as the circumstances under which information may be disclosed about students from educational records. The law, in particular, prescribes access control requirements for students older than 18 with regard to parents' rights of access to data, including grades, financial, and other records.

framework An overall methodology prescribing higher-level processes.

governance The legal or corporate standards that prescribe how an organization will conduct itself with regard to its behavior in handling information and data.

Gramm-Leach-Bliley Act (GLBA) U.S. law that requires financial institutions (to include banks, loan companies, insurance, and investment companies) to protect sensitive financial data and make their information-sharing practices known to their customers. Of particular interest to security professionals is the Safeguards Rule incorporated into GLBA, which requires institutions under the jurisdiction of the Federal Trade Commission to have specific measures in place to protect customer information.

Health Insurance Portability and Accountability Act (HIPAA) Law passed in 1996 requiring the U.S. government's Health and Human Services Department to establish requirements for protecting the privacy and security of personal health information (PHI). The two important elements of HIPAA of interest to security professionals are the HIPAA Privacy Rule and the HIPAA Security Rule, which set forth specific standards on how to protect electronic PHI.

identification The process of initially presenting credentials to a system for the purposes of identifying an authorized user.

impact The level of potential harm or damage to an asset or the organization if a given threat were to exploit a given vulnerability.

Information System Security Engineering (ISSE) The processes and methods used to manage the security life cycle of information and systems. ISSE typically follows and is adapted to the organization's system development life-cycle model but embeds security processes into each phase of the life cycle so that security is considered early on in the development process, rather than as an afterthought when the system is implemented and data produced.

integrity The goal of preventing unauthorized modification to a system or data.

ISO/IEC standards The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which together are responsible for a majority of information technology standards that are used worldwide, including several that apply to information security and risk management.

key performance indicators (KPIs) Used to understand and enable the measurement of control performance.

key risk indicators (KRIs) Highly probable indicators designed to accurately predict important levels of risk based on defined thresholds.

least privilege A security principle that dictates that entities should be given only the minimum level of rights, permissions, and privileges necessary to perform their designated functions or jobs, and no more than that.

likelihood The level of certainty that an incident will occur; often expressed statistically as a probability of occurrence.

need-to-know A security concept that requires an individual have an actual requirement to access systems or data, based upon their job requirements.

NIST The U.S. Department of Commerce's National Institute of Standards and Technology.

NIST Risk Management Framework (RMF) The overall risk management methodology published and promulgated by the National Institute of Standards and Technology (NIST).

nonrepudiation The security concept that requires an individual to be accountable for their actions, such that they cannot deny that they took an action.

OCTAVE The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology developed by Carnegie Mellon University and the U.S. government to assist organizations in identifying and assessing information security risk.

passive tools Passive tools listen for network traffic or monitor the hosts they reside on, quietly and with little to no impact on the ongoing operations; used when there is a desire for no interference with daily activities.

PCI-DSS A set of security requirements levied on merchants that process credit card transactions by the major payment card industry providers, including Discover, Visa, MasterCard, and American Express. PCI-DSS was developed in an effort to impose security requirements and controls on retailers (merchants and service providers) in order to reduce credit card fraud and identity theft.

penetration testing Designed to exploit weaknesses on a system based on their having been exploited, not just the probability.

platform A hardware or software infrastructure upon which to base computing operating systems, applications, and networks. It may involve different operating systems, network protocols, or particular types of hardware.

port scanner Allows a tester to determine which ports on the system are listening for requests.

portfolio A grouping of programs, managed as a whole. Portfolio management is the oversight and management of several different programs by a senior person in the organization.

practice A proven, standardized methodology or way of performing particular tasks or processes.

program A grouping of similar projects; programs are usually ongoing and longer-term in nature and may also encompass several individual projects, as well as other activities specific to processes that may have an indefinite duration.

project A limited-duration set of activities geared toward a particular goal; projects have definitive start and stop dates, resource allocations, scope, schedule, and costs.

project management A set of processes covering a defined project from start to finish, generally looking to cut costs such as time, scope, and overall project cost.

protocol analyzer Often known as a sniffer; dedicated hardware or software that collects network traffic for the purposes of examination, either for determining network issues or for capturing plain-text usernames, passwords, or other sensitive information being sent in the clear.

qualitative assessment An assessment technique that uses subjective values, such as low, moderate, and high, to describe various components of risk, such as likelihood and impact. Qualitative techniques rely on data that is often not easily described in numerical terms.

quantitative assessment An assessment technique that uses nonsubjective values, such as numerical or other quantitative data, to describe various components of risk, such as likelihood and impact. Quantitative techniques rely on data that is numerically derived and not easily subject to individual opinion.

quick wins Risk responses that are high reward and low cost, which are both effective and efficient.

recovery point objective (RPO) The maximum tolerable time period in which data can be lost by the organization because of an incident or disaster.

recovery time objective (RTO) The maximum amount of time that can be allowed to pass between an incident and recovering the business to an operational state.

resilience The ability of the business to survive negative events and continue with its mission and function.

risk The possibility of harm that can come to an asset or an organization.

risk acceptance When an active decision is made to assume risk (either inherent or residual) and take no further action to reduce it.

risk appetite The organization's overall acceptable level of risk for a given business venture.

risk assessment The process of identifying and assessing various factors, including threats, threat actors, vulnerabilities, assets, and likelihood, to determine their impact on the organization.

risk avoidance An option taken when, after controls have been considered, the level of risk is still not acceptable, and the project isn't started or is canceled.

risk culture The overall attitude toward risk, promulgated and supported by the organization's leadership.

risk factor Any factor that may contribute to an increase or decrease in risk; risk factors could be external or internal, and they could affect either likelihood or impact should a risk event actually occur.

Risk IT Framework ISACA's own risk management methodology; it is strongly tied to and integrated with COBIT 5. The Risk IT Framework merges traditional IT models with a more risk-focused mind-set.

risk management The overall process of managing risk within an organization at all levels, according to the organization's risk appetite, tolerance, and strategy.

risk mitigation Involves the application of controls that lower the overall level of risk through the reduction of the vulnerability, the likelihood of the threat exploit, or the reduction of the impact to the asset, if the risk were to be realized.

risk ownership The assignment of a particular aspect of risk to a responsible (and accountable) individual, usually a risk practitioner or manager who has the ability to affect risk response through their ownership of assets, controls, or status in the organization.

risk profile A collection of detailed data on identified IT risks; typically applied to a specific system or groups of systems.

risk register The master product or document that reflects the different risk scenarios and factors for the organization; it could be broken down by asset or system and reflects the different risk factors including threats, vulnerabilities, assets, likelihood, and impact to assets.

risk response action plan Lists the risk responses that have been chosen and charts their progress and associated timeline, with an appropriate action owner.

risk scenario An identified risk event possibility, which consists of a threat actor, threat, vulnerability, and asset.

risk sharing Often referred to as risk transference, entails the use of a third party to offset part of the risk. It can involve the outsourcing of some activities to a third party to reduce the financial impacts of a risk event.

risk tolerance The organization's level of acceptable variation from the risk appetite.

root-cause analysis (RCA) Looks to establish a causal relationship between the root cause (or causes) and the problem as it manifested itself.

Sarbanes-Oxley Act of 2002 (SOX) U.S. law passed in 2002 establishing requirements for public companies in the United States, as well as auditors and accounting firms, to improve the accuracy and reliability of corporate disclosures with regard to securities laws. The law is enforced by the U.S. Securities and Exchange Commission (SEC) and provides governance for the integrity and accuracy of data produced by an organization. For security professionals, this has the effect of imposing specific integrity and protection controls on information systems and processes.

security categorization The process of determining the impact to the organization, with regard to confidentiality, integrity, and availability, for information and systems. The security categorization uses qualitative benchmarks of low, moderate, and high. FIPS 199 and NIST SP 800-60 offer a defined process for the security categorization of information.

security information and event management (SIEM) Refers to the technologies and products used to integrate security information management and security event management information into a centralized interface, providing real-time event correlation and analysis.

service-level agreement (SLA) A contractual agreement, signed by an organization and a third-party provider, which details the level of security, data availability, and other protections afforded the organization's data held by the third party.

Software as a Service (SaaS) A third-party cloud-based service that offers outsourced use of software by an organization; this allows an organization to use licensed software at a lower cost than buying, installing, and maintaining software.

stakeholder Any business-related individual, department, or entity directly affected by risk to the organization.

standard A prescribed set of detailed processes, which may include specific levels of performance or function, used to complete and measure a given task or function.

systems development life cycle (SDLC) A framework describing the entire useful life of a system or software, which usually includes phases relating to requirements definition, design, development, acquisition, implementation, sustainability, and disposal.

threat An event or occurrence that has the potential to cause harm or damage to people, places, or things, or to adversely affect operations.

threat actor See *threat agent*.

threat agent An entity that has the intent to initiate a threat event. This doesn't have to be a person; it could also be nature, in the case of a natural disaster.

threat assessment An assessment that attempts to determine all potential threat actors and threats that may affect a given asset or its vulnerabilities.

threat modeling A threat assessment that attempts to determine all possible vectors of attack and includes risk factors that may affect the ability of a threat actor to initiate or complete a threat event.

Val IT A governance and management framework developed by the IT Governance Institute; it has been absorbed as part of COBIT 5. It consists of three main domains: Value Governance (VG), Portfolio Management (PM), and Investment Management (IM).

vulnerability A weakness in a system or asset, such as a flaw in software code; it can also be considered to be a lack of protection for an asset, such as an unlocked server room door.

vulnerability assessment An assessment that attempts to discover all potential weaknesses for an asset. Often designed for a third party to come into an organization, take stock of the assets that will be covered within the scope of the assessment, conduct scans and other tests against those assets, and provide a report of the vulnerabilities that have been found.

vulnerability scanner A piece of software designed to scan a system to determine what services the system is running and whether any unnecessary open ports, operating systems and applications, or back doors can be exploited because of a lack of patching or other flaw.

work breakdown structure (WBS) A detailed decomposition of the work to be performed during the project, including specific step-by-step tasks, as well as required resources.

INDEX

A

AC-5 control (NIST SP 800-53), 113, 114

AC-6 control (NIST SP 800-53), 190

AC-7 control (NIST SP 800-53), 188–189

access controls

defined, 4

KPI for, 244, 246, 248

supporting security goals, 7

accountability

defined, 5

KPI for audit and, 250–251

nonrepudiation and, 6–7

acquisition phase (SDLC), 51, 147

action plans for risk response, 137

administrative controls, 184

Agile program management framework, 150–151

analyzing risk scenarios, 80

ANSI (American National Standards Institute), 199

APO (Align, Plan, and Organize)

management domain (COBIT), 191, 277

applicability of Risk IT Framework, 277–278

applications, risks introduced by, 23–24

assessments. *See* threat assessments; risk

assessment and analysis

assets

data as, 4

exam tip, 72

factoring into risk scenarios, 71, 73, 74

identifying and categorizing, 101

ownership of, 116

profiling with OCTAVE Allegro, 94

threats and vulnerabilities inherent to, 102

auditing

accountability vs., 6

audit and accountability KPI, 250–251

Australian Signals Directorate, 199

authentication

about, 5

differences in identification, authorization, and, 6

authorization

about, 6

differences in identification, authorization, and, 6

implementing risk management systems after, 14–15

authorizing official (AO), 273

availability

access controls supporting, 4, 7

data risks and vulnerabilities for, 57–58

KPI for, 243

as security goal, 3

awareness and training KPI, 247, 249

B

BAI (Build, Acquire, and Implement)

management domain (COBIT), 191, 277

black-box testing, 162

blind tests, 162

bottom-up approach to risk scenarios, 76–77

bow-tie analysis, 109–110

Build, Acquire, and Implement (BAI)

management domain (COBIT), 191, 277

business cases

designing and implementing controls for, 210–212

factors supporting, 213

risk response for, 135–136

business continuity planning, 58–62

about, 58–59

exam tips, 62

NIST SP 800-34 resources on, 60

business continuity planning (*Cont.*)
recovery strategies in, 59
resilience and, 60
risk factors in, 60–61
threats and vulnerabilities for, 61–62
business processes, 42–62. *See also* business cases; business continuity planning; organizations
about, 42
business functions, 216–218
business information as data, 20–21
environmental risk factors for, 42–44
exam tips for, 62
mitigating operational risks in, 132
in risk scenarios, 78–79

C

capabilities of risk response, 134
Capability Maturity Model Integration (CMMI) framework, 149–150
CCS (Council on CyberSecurity), 198
certification and accreditation KPI, 251, 252
Certified in Risk and Information Systems Control exam. *See* CRISC exam objectives
CIA triad. *See also* availability; confidentiality; integrity
about, 2–3
equation for control of, 140
illustrated, 3
classifying
controls, 184–185
data, 5
risk factors, 70–71
CMMI (Capability Maturity Model Integration) framework, 149–150
COBIT 5 (Control Objectives for Information and Related Technology)
domains and processes within, 130–131, 277
framework of, 16–18
function of, 18
governance and management control domains for, 190–192
guidance on controls in, 182, 183

illustrated, 17
relationship between Risk IT, Val IT, and, 276
Val IT incorporated into, 190, 192
Committee of Sponsoring Organizations (COSO) framework, 16, 215
common controls, 116, 140–141, 272–273
communications
communicating risk results, 117
penetration test result reports, 164
reporting control monitoring results, 173–174
compatibility with emerging technology, 54
compensating controls, 138, 185
confidentiality
access controls supporting, 4
data risks and vulnerabilities for, 57–58
as security goal, 2
configuration management KPI, 244, 245
content and context of controls, 146
contingency planning KPI, 244, 247
continuity management, 58–60
control analysis, 111–115
control gaps, 113–114
evaluating effectiveness of existing controls, 111–113, 229–230
exam tip for, 113
ownership of risk and controls, 116
recommending controls, 114–115
control catalogs
about, 182
mapping controls to other, 184
NIST, 186–187
control enhancements, 189
control families
COBIT, 192
NIST, 186–187
control gaps, 113–114, 230–231
control libraries, 182, 183
control monitoring, 159–180. *See also* KPIs
about, 174
against metrics, 144
assessment tools for, 164–165
collecting and analyzing data, 172–173
exam objectives for, 159

- KPIs for, 166–171
KRIs for, 166, 171–172
making threat assessments, 160–161
measuring effectiveness, 230
reporting results of, 173–174
review questions and answers, 175–180
security controls, 15–16, 159, 274
testing and assessing controls, 160, 162–164
using root-cause analysis, 172
vulnerability assessments for, 161–162
- Control Objectives for Information and Related Technology.** *See* COBIT 5
- control redundancy, 226–227
control selection, 14, 15, 227–228, 229
- controls, 181–207. *See also* control analysis; control monitoring; designing and implementing controls
assessing risks for, 102
assessment techniques for, 142, 143
business functions and, 216–218
categories of, 138, 200, 201
choosing standards for, 199
classification of, 184–185
COBIT governance and management domains, 190–192
common, 116, 140–141, 272–273
defined, 4, 182
designing effective, 140–141, 224, 225, 229–230
developing for risk response, 138
effectiveness of existing, 111–113, 229–230
employee training for content/context of, 146
evaluating risk likelihood/impact for, 103
exam objectives for, 181
exam tips, 189, 193, 194
implementing and adjusting, 141
industrial control systems, 199
information security concepts for, 182–186
interoperability of, 184
ISO 27002 on, 139–140
mapping ISO/IEC to NIST controls, 195–197
monitoring, 15–16
NIST 800-53 on, 139, 140
- NIST RMF, 13–16, 186–190
objective and requirements for PCI-DSS, 193–194
other frameworks for, 195
overview, 201–202
recommending, 114–115
reduction of likelihood or impact with, 186
review questions and answers, 203–207
selecting and implementing, 14, 15, 185–186, 227–228, 229
testing and assessing risk response, 141–143
Val IT framework, 190, 192–193
- Cornell University KPIs, 167–168
- Corporate Governance of Information Technology* (ISO/IEC), 16
- corrective controls, 138, 184–185
- COSO (Committee of Sponsoring Organizations), 16, 215
- costs
risk and threat factors for, 45, 46
risk response, 134
- Council on CyberSecurity (CCS), 198
- credit card industry standards, 29, 30, 183, 193–194
- CRISC exam objectives
about exam, xviii–xix, 2
controls, 181
designing and implementing controls, 209–210
enterprise threats and vulnerabilities, 37
- KPIs and KRIs, 239
- managing risk scenarios, 69
- mitigation, 125–126
- monitoring controls, 159
- practice area map, xix–xxii
- risk assessment and analysis, 91–92
- risk concepts, 1
- risk response, 125–126
- threats and vulnerabilities, 37
- Critical Security Controls (CSC), 197–198
- criticality analysis, 72
- cross-boundary business functions, 217–218
- cryptography, 261–262, 269
- CSC (Critical Security Controls), 197–198
- cybersecurity controls, 200–201, 202

D

- data. *See also* CIA triad
business information as, 20–21
collecting for risk assessment and analysis, 98–101
confidentiality of, 2
data segmentation, 218
integrity of, 2
inventorying for RMF, 14
KPI/KRI for collecting and analyzing, 172–173
managing risk factors for, 57
ownership of, 56
Risk IT collection process for, 96
risks introduced by databases, 24
sensitivity of, 4–5, 218
threats and vulnerabilities of, 56–58
using documentation in risk assessment, 99–100
defense in depth, 226
Defense Information Assurance Certification and Accreditation Program (DIACAP), 29, 216, 269
deferral, 135, 136

E

- E-Government Act of 2002, 268
economy of use, 212, 213, 225
EDM (Evaluate, Direct, and Monitor)
management domain (COBIT), 190, 277
effectiveness. *See also* measuring risk and control effectiveness
control design, 224, 225
evaluating existing control, 111–113, 229–230
monitoring and testing control, 230
risk response, 134
efficiency
control design, 212, 213, 224–225
risk response, 134
electronic protected health information (EPHI), 29
emerging technologies, 53–54
employees
environmental risks associated with, 43
project risks associated with, 45
training in control content and context, 146
enterprise risk management (ERM), 11, 276, 280
entries in risk register, 83
environmental risks for businesses, 42–44
EPHI (electronic protected health information), 29
ERM (enterprise risk management), 11, 276, 280
Evaluate, Direct, and Monitor (EDM)
management domain (COBIT), 190, 277
events
event-tree analysis, 108–109
reacting to, 283
exceptions in risk response, 144–145
exercises
assessing risk, 119
choosing control standards, 199
creating risk scenarios, 79
determining vulnerabilities, 41–42
developing risk awareness program, 28

- identifying legal, regulatory, and contractual requirements, 30
qualitative and quantitative risk assessments, 108
external risks
defined, 71
factoring into risk scenarios, 77, 78, 79

F

- false positives and negatives, 165
fault- and event-tree analysis, 108–109
Federal Information Processing Standards.
See FIPS
Federal Information Security Management Act (FISMA), 29, 216, 268
Financial Privacy Rule, 29
FIPS (Federal Information Processing Standards)
about, 13
FIPS 140-1 and 140-2, 269–270
FIPS 199, 14, 15, 270, 271
FIPS 200, 15, 271
FISMA (Federal Information Security Management Act), 29, 216, 268
5 nines, 243
“Framework for Improving Critical Infrastructure Cybersecurity” (NIST), 200, 201
frameworks. *See also* specific frameworks
COBIT 5, 16–18, 130–131, 190–192
defined, 12–13
NIST cybersecurity, 200
Risk IT, 18–19, 96–98
risk response, 148–151
steps in NIST Risk Management Framework, 13–16, 127–129
studying about, 19
Val IT, 192–193

G

- GLBA (Gramm-Leach-Bliley Act), 29, 183, 215
government and management domains for COBIT 5, 190–192
gray-box tests, 162

H

HIPAA (Health Insurance Portability and Accountability Act)
about, 28–29
controls required by, 182, 183
designing controls supporting, 214

I

IATF (Information Assurance Technical Framework), 221
identification
asset categorization and, 101
authentication and, 5
difference in authentication, authorization, and, 6
identifying risk factors, 70
KPI for identification and authentication, 251, 253
impact
analyzing assessments of likelihood and, 110–111
contributing to risks, 10–11
defined, 9–10
evaluating in risk assessments, 102–103
organizational factors affecting, 80–81, 82
qualitative assessment of, 107
relationship to other risk elements, 11
risk scenarios and, 72, 74, 80
technological factors affecting, 81–82
implementation phase (SDLC), 51, 147
implementing controls
about, 228–229
adding controls, 231–232
adjusting control gaps, 230–231
documenting controls, 232–233
evaluating existing control effectiveness, 111–113, 229–230
exam tips, 230
managing control ownership and risk, 232
supplementing existing controls, 231
incident response KPI, 253–254
industrial control systems (ICS), 199
Information Assurance Technical Framework (IATF), 221

information categorization, 14, 15, 227–228
information security

access controls supporting, 4
control concepts for, 182–186
elements supporting security goals, 3–7
goals of, 2–3

information systems. *See also* ISSE

architecture for, 22
categorizing, 14, 15, 227–228

Information Systems Audit and Control Association. *See* ISACA

information technology. *See* IT

Information Technology Infrastructure Library (ITIL), 16

inherent risks, 11

initiation phase (SDLC), 50, 51, 147

integrity

access controls supporting, 4
data risks and vulnerabilities for, 57–58
KPI for system and information, 262–263

as security goal, 2

internal risks

defined, 71

factoring into risk scenarios, 77–78, 79

International Electrotechnical Commission. *See* ISO/IEC standards

International Organization for Standardization. *See* ISO/IEC standards

interoperability risks of technology, 54
interviews for risk assessments, 99

Investment Management (IM) domain (Val IT), 193

ISA (International Society of Automation) standards, 199

ISACA (Information Systems Audit and Control Association). *See also* COBIT 5; Risk IT Framework

approaches to risk scenarios, 75–77
COBIT 5 framework, 16–18, 130–131, 190–192

exam tips, 98

publications for Risk IT, 278–279

Risk IT framework, 18–19, 96–98, 129–130, 275–283

studying frameworks of, 13

ISO/IEC standards

- ISO 27001 control requirements, 195
- ISO 27002, 139–140
- ISO/IEC 15288:2008, 223
- ISO/IEC 15408 controls, 195, 197
- ISO/IEC 21827:2008, 220, 223
- ISO/IEC 27001, 195–196
- ISO/IEC 27005:2011, 95
- ISO/IEC 31000:2009, 95–96, 108
- ISO/IEC 38500-2008, 16
- risk assessment and analysis using, 95–96, 98

ISSE (information system security engineering). *See also* SDLC

- approach to SDLC model, 218–221
- control design and, 223–228
- exam tips, 221
- IATF phases in model of, 221
- ISO/IEC 21827:2008, 220, 223
- NIST SP 800-160 on, 221–223

IT (information technology). *See also* information security; risks

- factoring infrastructure in risk scenarios, 78
- threats and vulnerabilities in management of, 54–56

ITIL (Information Technology Infrastructure Library), 16**K****KPIs (key performance indicators), 242–263**

- access control, 244, 246, 248
- applying, 239
- audit and accountability, 250–251
- availability, 243
- awareness and training, 247, 249
- certification and accreditation, 251, 252
- collecting and analyzing data for, 172–173
- configuration management, 244, 245
- contingency planning, 244, 247
- criteria for, 166–171, 240
- defined, 166
- developing, 240, 242
- exam objectives for, 239
- identification and authentication, 251, 253
- incident response, 253–254

maintenance, 255

- media protection, 256
- NIST, 168–171
- Oak Ridge Institute for Science and Education, 168
- personnel security, 259
- physical and environmental protection, 257
- planning, 258
- risk assessment, 260
- S.M.A.R.T. mnemonic for, 167, 240
- system and communications protection, 261–262
- system and information integrity, 262–263
- system and services acquisition, 244, 246
- template for NIST, 241

KRIs (key risk indicators)

- collecting and analyzing data for, 172–173
- defined, 130, 166
- developing, 171–172
- exam objectives for, 239
- Risk IT Framework, 171
- S.M.A.R.T. mnemonic for, 172

L**Lean mind-sets, 151****legal and governance standards. *See also* FIPS; frameworks; NIST; and specific standards**

- about, 28
- controls and regulatory guidance, 213
- defined, 13
- exercise choosing control, 199
- influence on control design and implementation, 212
- ISA and ANSI, 199
- laws, 28–29
- PCI-DSS, 29, 30, 183, 193–194, 213–214

liability, 211–212**life cycle. *See also* SDLC**

- PDCA, 126–127
- RMF in security, 15, 128
- system development, 49–53

likelihood

- analyzing assessments of impact and, 110–111
- contributing to risks, 10–11

likelihood (*Cont.*)
 defined, 10
 evaluating in risk assessments, 102–103
 factoring into risk scenario, 72, 74
 organizational factors affecting, 80–81, 82
 probability vs., 80
 qualitative assessment of, 107
 relationship to other risk elements, 11
 risk scenarios and, 80
 technological factors affecting, 81–82

M

maintenance KPI, 255
 management of IT operations, 54–56, 131
 mapping
 controls to other control catalogs, 184
 functions to NIST subcategories and controls, 201
 ISO/IEC to NIST controls, 195–197
 MEA (Monitor, Evaluate, and Assess)
 management domain (COBIT), 192, 277
 measuring risk and control effectiveness, 239–265. *See also* KPIs; metrics
 access control KPI, 244, 246, 248
 applying KPI, 239
 audit and accountability, 250–251
 availability KPI, 243
 awareness and training KPI, 247, 249
 certification and accreditation KPI, 251, 252
 configuration management KPI, 244, 245
 contingency planning KPI, 244, 247
 criteria for KPI, 166–171, 240
 developing KPI, 240, 242
 exam objectives, 239
 identification and authentication, 251, 253
 incident response KPI, 253–254
 maintenance KPI, 255
 media protection KPI, 256
 overview, 263
 personnel security KPI, 259
 physical and environmental protection, 257
 planning KPI, 258
 review questions and answers, 263–265

risk assessment KPI, 260
 system and communications protection KPI, 261–262
 system and information integrity KPI, 262–263
 system and services acquisition KPI, 244, 246
 types of KPIs, 242
 media protection KPI, 256
 metrics. *See also* KPIs; KRIs
 KPIs as, 242
 monitoring against, 144
 quality of, 242
 mitigation, 137–152
 about, 152–153
 adjusting control gaps, 230–231
 evaluating as risk response, 131–132
 exam objectives for, 125–126
 implementing controls as, 211
 with OCTAVE Allegro, 95
 review questions and answers, 153–157
 strategies for, 199
 Monitor, Evaluate, and Assess (MEA)
 management domain (COBIT), 192, 277
 monitoring. *See* control monitoring

N

National Institute for Standards and Technology. *See* NIST
 National Security Agency (NSA), 221
 networks, risks introduced by, 23
 NIST (National Institute for Standards and Technology), 13. *See also* NIST Special Publications; RMF
 COBIT control families vs., 192
 control exam tips for, 189
 control library supporting HIPAA, 214
 control-related SDLC from, 146–148
 cybersecurity framework, 200
 implementing FISMA requirements, 216, 268
 ISO/IEC 15408 controls mapped to, 197
 mapping controls to ISO/IEC 27001, 195–196

- Risk Management Framework, 13–16, 92–93
supplementing ISA controls with those of, 199
template for KPIs, 241
- NIST Risk Management Framework. *See* RMF
- NIST Special Publications
about, 16
SP 800-30, 16, 40, 92–93, 98, 107, 271, 273
SP 800-34, 60
SP 800-37, 15, 16, 92, 127, 128, 268, 269, 271, 272, 273
SP 800-39, 129, 271
SP 800-53, 14, 15, 113, 114, 128, 139, 140, 183, 186–188, 195, 214, 228, 229, 268, 269, 271, 272
SP 800-53A, 15, 113, 128, 189–190, 271, 273
SP 800-55, 168–171, 240–242, 245, 246, 247, 248, 249, 250–251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262–263
SP 800-60, 14, 15, 128, 228, 270, 271, 272
SP 800-64, 244
SP 800-66, 214
SP 800-115, 142, 162–163
SP 800-137, 15, 128, 271, 272, 274
SP 800-160, 15, 128, 220, 221–223, 271, 272
nonrepudiation, 6–7
- O**
- Oak Ridge Institute for Science and Education, 68
- OCTAVE (Operationally Critical Threat, Assets, and Vulnerability Evaluation), 93–95
exam tip for, 95
OCTAVE Allegro, 94–95
OCTAVE and OCTAVE-S, 93, 95
review of, 98
- Open Group Architecture Forum, The (TOGAF), 16
- Open-Source Security Testing Methodology Manual (OSSTMM), 143
- operating system risks, 24
- Operationally Critical Threat, Assets, and Vulnerability Evaluation. *See* OCTAVE
- operations/maintenance phase (SDLC), 147
- organizations. *See also* business processes
authorizing RMFs, 14–15
business goals and objectives for risk, 19–20
business information criteria, 20–21
business perspectives of controls for, 210–212
business processes in risk scenarios, 78–79
communicating risk analysis, 117
considering IT risks to, 24
continuity and disaster recovery for, 58–62
external business functions of, 217, 218
identifying risks of opportunities, 136–137
information systems architecture for, 22
legal, regulatory, and contractual requirements of, 30
making risk-aware business decisions, 280
management as factor in risk scenarios, 78
mitigations options for, 131–132
protecting internal business functions, 216–217, 218
reporting control monitoring results, 173–174
reporting risk response activities to, 145
resilience of, 60
risk culture of, 12
risk ownership within, 25
securing cross-boundary business functions, 217–218
senior management and risk tolerance, 26
structures of, 21–22
threat assessments for controls, 160–161
training employees in control content and context, 146
transferred risks and responsibilities, 49
using ERM, 11
vulnerability assessments for controls, 161–162

OSSTMM (Open-Source Security Testing Methodology Manual), 143
 ownership
 asset, 116
 control, 116, 232
 data, 56
 risk, 24–30, 116, 232, 283
 risk response action plans and, 137

P

passive vs. active control testing tools, 164
 PCI-DSS (Payment Card Industry Data Security Standards)
 about, 29, 30, 183
 applying, 213–214
 control objective and requirements for, 193–194
 PDCA (Plan-Do-Check-Adjust) life cycle, 126–127
 penetration testing, 162–164
 personnel security KPI, 259
 physical and environmental protection KPI, 257
 physical controls, 184
 physical locations, 60
 Plan-Do-Check-Adjust (PDCA) life cycle, 126–127
 planning
 business continuity, 58–62
 KPIs for, 244, 247, 258
 risk response, 126–127
 risk response action plans, 137
 testing disaster recovery plans, 59
 platforms, 22–23
 PMBOK (Project Management Body of Knowledge), 16
 PMI-PMBOK (Project Management Institute Project Management Body of Knowledge), 16, 148, 149
 port scanners, 164–165
 portfolio management, 44
 Portfolio Management (PM) domain (Val IT), 193
 practices, 13
 preparedness, 132
 Pretexting Protection, 29

preventative controls, 138
 PRINCE2 (Projects in Controlled Environments 2), 16
 prioritizing risk responses, 134–136
 privacy, NIST control families for, 187
 probability, 80
 processes. *See* business processes; domains and processes
 Project Management Body of Knowledge (PMBOK), 16, 148, 149
 Project Management Institute Project Management Body of Knowledge (PMI-PMBOK), 16, 148, 149
 project/program management
 Agile framework for, 150–151
 CMMI, 149–150
 defined, 44
 illustrated, 47
 implementing as risk response, 148
 Lean mind-set, 151
 PMI-PMBOK framework, 16, 148, 149
 risk management and, 151–152
 risks, threats, and vulnerabilities, 44–47
 Projects in Controlled Environments 2 (PRINCE2), 16
 protocol analyzer, 164
 publications. *See also* NIST Special Publications
 Risk IT Framework, 278–279

Q

qualitative KPI, 166
 qualitative risk assessments
 combining with quantitative techniques, 107–108
 performing, 108
 using, 103, 106–107
 quantitative KPI, 166
 quantitative risk assessments, 103–106
 about, 103–104
 combining with qualitative techniques, 107–108
 exam tip for, 105
 scenario using, 104–106
 quick wins, 135

R

RCA (root-cause analysis), 172

recovery controls, 185

recovery point objective (RPO), 59

recovery time objective (RTO), 59

remote access control measure, 244,
246, 248

reporting results

control monitoring, 173–174

penetration testing, 164

risk assessment and analysis, 116

of risk response activities to
organizations, 145

requirements phase (SDLC), 50, 51

residual risks, 11, 117

resilience, 60

results documentation, 116–118

retirement phase (SDLC), 51

review questions and answers, 119–124

control monitoring, 175–180

controls, 203–207

designing and implementing controls,
234–238

measuring risk and control effectiveness,
263–265

risk assessment and analysis, 119–124

risk management concepts, 31–36

risk response, 153–157

risk scenarios, 84–89

threats and vulnerabilities, 62–67

risk acceptance, 133

risk appetite

defined, 12

factoring into business plan, 19, 20

senior management and, 26

risk assessment and analysis, 91–124. *See also*

risk scenarios

analyzing assessments, 110–111

analyzing controls, 102, 111–115

asset identification and categorization, 101

bow-tie analysis, 109–110

collecting data for, 98–101

communicating risk results, 117

determining risk from, 117

documenting results of, 118

exam objectives, 91–92

exam tips, 98, 103, 105, 110

exercise assessing risk, 119

fault- and event-tree analysis, 108–109

identifying asset threats and

vulnerabilities, 102

ISACA Risk IT Framework, 18–19, 96–98

ISO/IEC standards, 95–96, 98

likelihood determination and impact

analysis, 102–103

NIST RMF steps for, 92–93

OCTAVE methodology for, 93–95, 98

other methods of, 110

performing qualitative and quantitative
assessments, 108

processes in, 92, 103

qualitative techniques for, 103, 106–107

quantitative techniques for, 103–106

reporting results of, 116

review questions and answers, 119–124

system testing during, 100–101

risk assessment KPI, 260

risk avoidance, 133

risk awareness, 26–28

about, 26

developing program for, 27–28

exercise in developing program, 28

tools and techniques of, 26–27

risk culture, 12

Risk Evaluation (Risk IT), 129–130, 280–282

Risk Governance (Risk IT), 129–130, 279–280

Risk IT Framework, 275–283

applicability of, 277–278

exam tips for, 130

focus areas of, 279

guidance on use of controls in, 182

KRIs for, 171

managing risk response with, 129–130

overview, 275–277

publications for, 278–279

relationship between COBIT, Val IT,
and, 276

risk assessment and analysis using, 18–19,

96–98

- Risk IT Framework (*Cont.*)
- Risk Evaluation domain, 129–130, 280–282
 - Risk Governance domain, 129–130, 279–280
 - Risk Response domain, 129–130, 282–283
- Risk IT Practitioner Guide, The* (ISACA), 18
- risk management concepts, 1–36
 - business perspectives, 19–24
 - elements supporting security goals, 3–7
 - exam topics for, 1
 - information security goals, 2–7
 - information systems architecture, 22
 - legal and governance standards, 28–30
 - networks, 23
 - overview, 30–31
 - platforms, 22–23
 - review questions and answers, 31–36
 - risk awareness, 26–28
 - risk ownership, 24–30
 - terminology used, 8–19
- Risk Management Framework. *See* RMF
- risk profiles, 97–98, 281
 - risk register, 82–83, 118
 - risk response, 125–137
 - about, 152–153
 - creating plan for, 126–127, 137
 - developing controls, 138–140
 - documentation of options for, 143–144
 - evaluating options for, 131–137
 - exam objectives for, 125–126
 - exam tips, 132, 136
 - managing exceptions to, 144–145
 - methods of project management for, 148–152
 - mitigation as, 131–132
 - parameters of, 134
 - prioritizing, 134–136
 - reporting activities in, 145
 - review questions and answers, 153–157
 - risk acceptance as, 133
 - risk avoidance as, 133
 - Risk IT framework for, 129–130, 282–283
- risk sharing for, 132
 - RMF steps for, 127–129
 - standards and frameworks for, 127–131
 - training employees in control content and context, 146
- Risk Response (Risk IT), 129–130, 282–283
- risk scenarios, 60–90
 - about, 69–70
 - analyzing, 80
 - bottom-up approach, 76–77
 - business processes in, 78–79
 - classifying risks, 70–71
 - developing, 75, 79, 80
 - elements of, 71–74
 - exam objectives, 69
 - exam tips for, 71, 72, 75
 - factoring infrastructure in, 78
 - identifying risks, 70
 - identifying stakeholders, 79
 - internal and external risk factors, 77–78, 79
 - IT factors in, 78
 - likelihood and impact, 80
 - organizational factors in, 78, 80–81
 - pursuing low-cost responses to, 136
 - review questions and answers, 84–89
 - risk register, 82–83
 - sample, 74
 - time and location factors in, 72–74
 - top-down approach, 75–76, 77
 - using quantitative assessments, 104–106
- risk sharing, 132
- risk tolerance
- defined, 12
 - factoring into business plan, 19, 20
 - senior management and, 26
- risks. *See also* impact; likelihood
- acceptance of, 133
 - applications and, 23–24
 - business cases for controls and IT, 210–211
 - business continuity and disaster recovery, 60–61
 - classifying, 70–71

- communicating assessment of, 117
culture, appetite, and tolerance of, 12
elements of, 10–11
emerging technologies, 53
exercise assessing, 119
identifying, 70, 136–137
information technology management, 55
inherent and residual, 11
introduced by databases, 24
OCTAVE Allegro for measuring/
mitigating, 94
operating systems and, 24
organizational structures and approach
to, 21–22
ownership of, 24–30, 116, 232, 283
platforms and, 22–23
Risk IT analysis of, 97
SDLC, 52
third-party management, 48
threats and vulnerabilities contributing
to, 38
- RMF (Risk Management Framework). *See also* NIST Special Publications
about, 267
applicability of, 269
control families for, 186–187
DIACAP replaced with, 29
families of controls in, 182, 183
illustrated, 15, 128, 268
overview, 268–270
publications applicable to, 269–270,
271, 272
security categorization in, 227–228, 229
steps in, 13–16, 127–129, 270, 272–274
tiered approach of, 268–269
using in risk assessment and analysis,
92–93
- S**
- Safeguards Rule, 29
SANS (SysAdmin, Audit, Networking, and
Security) Critical Security Controls, 197–198
Sarbanes-Oxley Act (SOX), 183, 215–216
- SC (security categorization), 227–228
scale
developing for threat assessments, 39, 40
RMF applicability and, 269
scenarios. *See also* risk scenarios
identifying threat, 95
scheduling vulnerabilities
about, 46
scope creep and, 44
scope
developing for threat assessments, 39, 40
risk factors associated with, 45
scope creep, 44
threats and vulnerabilities from project, 46
SDLC (system development life cycle), 49–53
about, 49–50
ensuring security inherent in, 223
model and phases of, 50–51
NIST control-related, 146–148
risks, threats, and vulnerabilities of,
52–54
- security. *See also* security goals
HIPAA requirements for, 214
meeting defined requirements for controls,
225–226
NIST RMF control families for,
186–187
risk factors when using emerging
technologies, 53
RMF process throughout life cycle
of, 15, 128
- security categorization (SC), 227–228, 229
- security controls. *See* controls
- security goals
access controls supporting, 7
CIA, 2–3
controls mitigating risks for, 211
elements supporting, 3–7
illustrated, 7
security professionals, 14, 15
security training KPI, 247, 249
sensitivity, data classification and, 4–5
service level agreement (SLA), 48
SLA (service level agreement), 48

S.M.A.R.T. mnemonic, 167, 172, 240
sniffers, 164
software development life cycle. *See* SDLC
SOX (Sarbanes-Oxley Act), 183, 215–216
stakeholders, risk scenario, 79
standards. *See* legal and governance standards; *and specific standards*
“Strategies to Mitigate Targeted Cyber Intrusions” (Australian Signals Directorate), 199
sunset (disposition) phase (SDLC), 148
supervisory control and data acquisition (SCADA), 199
system and communications protection KPI, 261–262
system and information integrity KPI, 262–263
system and services acquisition KPI, 244, 246
system development life cycle. *See* SDLC
system documentation for risk assessment, 99–100

T

technical controls, 184
technology
assessing vulnerability of, 41, 44
mitigating risk for, 132
terminology, 8–19
testing
additional controls, 232
controls, 160, 162–164
disaster recovery plans, 59
effectiveness of controls, 230
penetration, 162–164
risk assessment using system, 100–101
risk response of controls, 141–143
tools for passive vs. active control, 164
the nines, 243
The Open Group Architecture Forum (TOGAF), 16
third-party management
about, 47–48
effect on continuity and disaster recovery, 60
risks, threats, and vulnerabilities, 48–49

threat actor, 38, 185–186
threat agents
characteristics of, 40
contributing to risks, 10–11
defined, 8–9, 38
exam tips, 72
factoring into risk scenarios, 71, 73, 74
relationship to other risk elements, 11
threat assessments
about, 38–40
characteristics of threat agents, 40
defined, 9
illustrated, 40
NIST SP 800-30 on, 16, 40, 92–93, 98, 107
reviewing controls with, 160–161
threat modeling. *See* threat assessments
threat scenarios, 95
threats and vulnerabilities, 37–67
assessments of, 39–41
business continuity and disaster recovery management, 58–62
contributing to risks, 10–11
data management, 56–58
defined, 8–9, 38
determining vulnerabilities, 41–42
effect of controls on, 185–186
emerging technologies, 53–54
evaluating for business processes, 42
exam objectives for, 37
exam tips, 38, 39, 62, 72
factoring into risk scenarios, 71, 73, 74
identifying, 38–39, 94
inherent to assets, 102
management of IT operations, 54–56
pairing of, 38, 39
project and program management, 44–47
relation to other elements, 11
review questions and answers, 62–67
system development life cycle, 49–53
third-party management, 47–49
threat agents and, 38
types of environmental risks, 43–44

time and location factors, 72–74

tools

- control monitoring assessment, 164–165

- risk awareness, 26–27

top-down approach to risk scenarios, 75–76, 77

tracking risk response exceptions, 144–145

training

- employees in control content and context, 146

- KPI for awareness and, 247, 249

- risk awareness, 26–27

U

uptime, 243

U.S. Department of Defense, 128, 216, 269

UTM (unified threat management), 226–227

V

Val IT

- domains and controls of, 192–193, 278

- incorporated into COBIT 5, 190, 192

- relationship between Risk IT, COBIT, and, 276

Value Governance (VG) domain (Val IT), 192

value stream map (VSM), 151

vulnerabilities. *See also* threats and

vulnerabilities

- assessing, 41–42, 161–162

- contributing to risks, 10–11

- defined, 8, 38

- relationship to other risk elements, 11

- technology, 41, 44

vulnerability scanner, 165

W

white-box tests, 162

work breakdown structure (WBS), 46

This page intentionally left blank

**Complete coverage
of today's top**

IT SECURITY

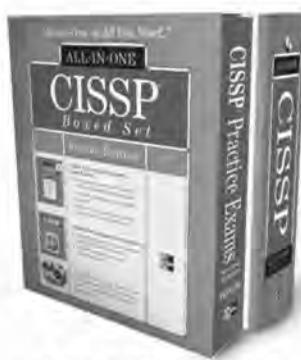
certification exams



0-07-176026-1 • \$60.00



0-07-178174-9 • \$80.00



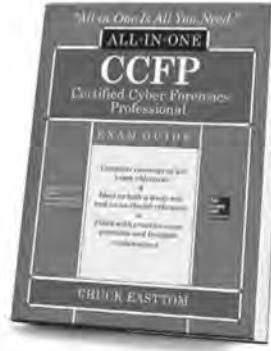
0-07-179308-9 • \$105.00



0-07-183557-1 • \$70.00



0-07-183156-8 • \$50.00



0-07-183976-3 • \$60.00



This page intentionally left blank

LICENSE AGREEMENT

THIS PRODUCT (THE "PRODUCT") CONTAINS PROPRIETARY SOFTWARE, DATA AND INFORMATION (INCLUDING DOCUMENTATION) OWNED BY McGRAW-HILL EDUCATION AND ITS LICENSORS. YOUR RIGHT TO USE THE PRODUCT IS GOVERNED BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.

LICENSE: Throughout this License Agreement, "you" shall mean either the individual or the entity whose agent opens this package. You are granted a non-exclusive and non-transferable license to use the Product subject to the following terms:

(i) If you have licensed a single user version of the Product, the Product may only be used on a single computer (i.e., a single CPU). If you licensed and paid the fee applicable to a local area network or wide area network version of the Product, you are subject to the terms of the following subparagraph (ii).

(ii) If you have licensed a local area network version, you may use the Product on unlimited workstations located in one single building selected by you that is served by such local area network. If you have licensed a wide area network version, you may use the Product on unlimited workstations located in multiple buildings on the same site selected by you that is served by such wide area network; provided, however, that any building will not be considered located in the same site if it is more than five (5) miles away from any building included in such site. In addition, you may only use a local area or wide area network version of the Product on one single server. If you wish to use the Product on more than one server, you must obtain written authorization from McGraw-Hill Education and pay additional fees.

(iii) You may make one copy of the Product for back-up purposes only and you must maintain an accurate record as to the location of the back-up at all times.

COPYRIGHT; RESTRICTIONS ON USE AND TRANSFER: All rights (including copyright) in and to the Product are owned by McGraw-Hill Education and its licensors. You are the owner of the enclosed disc on which the Product is recorded. You may not use, copy, decompile, disassemble, reverse engineer, modify, reproduce, create derivative works, transmit, distribute, sublicense, store in a database or retrieval system of any kind, rent or transfer the Product, or any portion thereof, in any form or by any means (including electronically or otherwise) except as expressly provided for in this License Agreement. You must reproduce the copyright notices, trademark notices, legends and logos of McGraw-Hill Education and its licensors that appear on the Product on the back-up copy of the Product which you are permitted to make hereunder. All rights in the Product not expressly granted herein are reserved by McGraw-Hill Education and its licensors.

TERM: This License Agreement is effective until terminated. It will terminate if you fail to comply with any term or condition of this License Agreement. Upon termination, you are obligated to return to McGraw-Hill Education the Product together with all copies thereof and to purge all copies of the Product included in any and all servers and computer facilities.

DISCLAIMER OF WARRANTY: THE PRODUCT AND THE BACK-UP COPY ARE LICENSED "AS IS." McGRAW-HILL EDUCATION, ITS LICENSORS AND THE AUTHORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE RESULTS TO BE OBTAINED BY ANY PERSON OR ENTITY FROM USE OF THE PRODUCT, ANY INFORMATION OR DATA INCLUDED THEREIN AND/OR ANY TECHNICAL SUPPORT SERVICES PROVIDED HEREUNDER, IF ANY ("TECHNICAL SUPPORT SERVICES"). McGRAW-HILL EDUCATION, ITS LICENSORS AND THE AUTHORS MAKE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT TO THE PRODUCT. McGRAW-HILL EDUCATION, ITS LICENSORS, AND THE AUTHORS MAKE NO GUARANTEE THAT YOU WILL PASS ANY CERTIFICATION EXAM WHATSOEVER BY USING THIS PRODUCT. NEITHER McGRAW-HILL EDUCATION, ANY OF ITS LICENSORS NOR THE AUTHORS WARRANT THAT THE FUNCTIONS CONTAINED IN THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PRODUCT WILL BE UNINTERRUPTED OR ERROR FREE. YOU ASSUME THE ENTIRE RISK WITH RESPECT TO THE QUALITY AND PERFORMANCE OF THE PRODUCT.

LIMITED WARRANTY FOR DISC: To the original licensee only, McGraw-Hill Education warrants that the enclosed disc on which the Product is recorded is free from defects in materials and workmanship under normal use and service for a period of ninety (90) days from the date of purchase. In the event of a defect in the disc covered by the foregoing warranty, McGraw-Hill Education will replace the disc.

LIMITATION OF LIABILITY: NEITHER McGRAW-HILL EDUCATION, ITS LICENSORS NOR THE AUTHORS SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, SUCH AS BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFITS OR BENEFITS, RESULTING FROM THE USE OR INABILITY TO USE THE PRODUCT EVEN IF ANY OF THEM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL APPLY TO ANY CLAIM OR CAUSE WHATSOEVER WHETHER SUCH CLAIM OR CAUSE ARISES IN CONTRACT, TORT, OR OTHERWISE. Some states do not allow the exclusion or limitation of indirect, special or consequential damages, so the above limitation may not apply to you.

U.S. GOVERNMENT RESTRICTED RIGHTS: Any software included in the Product is provided with restricted rights subject to subparagraphs (c), (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 C.F.R. 52.227-19. The terms of this Agreement applicable to the use of the data in the Product are those under which the data are generally made available to the general public by McGraw-Hill Education. Except as provided herein, no reproduction, use, or disclosure rights are granted with respect to the data included in the Product and no right to modify or create derivative works from any such data is hereby granted.

GENERAL: This License Agreement constitutes the entire agreement between the parties relating to the Product. The terms of any Purchase Order shall have no effect on the terms of this License Agreement. Failure of McGraw-Hill Education to insist at any time on strict compliance with this License Agreement shall not constitute a waiver of any rights under this License Agreement. This License Agreement shall be construed and governed in accordance with the laws of the State of New York. If any provision of this License Agreement is held to be contrary to law, that provision will be enforced to the maximum extent permissible and the remaining provisions will remain in full force and effect.