



IT Security Risk Control Management

An Audit Preparation Plan

—

Raymond Pompon

Apress®

IT Security Risk Control Management

An Audit Preparation Plan



Raymond Pompon

Apress®

IT Security Risk Control Management: An Audit Preparation Plan

Raymond Pompon
Seattle, Washington
USA

ISBN-13 (pbk): 978-1-4842-2139-6
DOI 10.1007/978-1-4842-2140-2

ISBN-13 (electronic): 978-1-4842-2140-2

Library of Congress Control Number: 2016952621

Copyright © 2016 by Raymond Pompon

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr

Acquisitions Editor: Susan McDermott

Developmental Editor: Laura Berendson

Technical Reviewer: Mike Simon, Dena Solt

Editorial Board: Steve Anglin, Pramila Balen, Laura Berendson, Aaron Black, Louise Corrigan,

Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Nikhil Karkal, James Markham,

Susan McDermott, Matthew Moodie, Natalie Pao, Gwenan Spearing

Coordinating Editor: Rita Fernando

Copy Editor: Kim Burton-Weisman

Compositor: SPi Global

Indexer: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springer.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales-eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

Printed on acid-free paper

To all the defenders out there working unnoticed to keep us safe.

Contents at a Glance

About the Author	xxiii
About the Technical Reviewer	xxv
Acknowledgments	xxvii
Introduction	xxix
■ Part I: Getting a Handle on Things	1
■ Chapter 1: Why Audit?	3
■ Chapter 2: Assume Breach	13
■ Chapter 3: Risk Analysis: Assets and Impacts	23
■ Chapter 4: Risk Analysis: Natural Threats	39
■ Chapter 5: Risk Analysis: Adversarial Risk	51
■ Part II: Wrangling the Organization	67
■ Chapter 6: Scope	69
■ Chapter 7: Governance	81
■ Chapter 8: Talking to the Suits	99
■ Chapter 9: Talking to the Techs	113
■ Chapter 10: Talking to the Users	123
■ Part III: Managing Risk with Controls	131
■ Chapter 11: Policy	133
■ Chapter 12: Control Design	145
■ Chapter 13: Administrative Controls	153

■ Chapter 14: Vulnerability Management	165
■ Chapter 15: People Controls	175
■ Chapter 16: Logical Access Control	187
■ Chapter 17: Network Security	197
■ Chapter 18: More Technical Controls	219
■ Chapter 19: Physical Security Controls	231
■ Chapter 20: Response Controls	239
■ Part IV: Being Audited	259
■ Chapter 21: Starting the Audit	261
■ Chapter 22: Internal Audit	275
■ Chapter 23: Third-Party Security	283
■ Chapter 24: Post Audit Improvement	293
Index	301

Contents

About the Author	xxiii
About the Technical Reviewer	xxv
Acknowledgments	xxvii
Introduction	xxix
■ Part I: Getting a Handle on Things	1
■ Chapter 1: Why Audit?	3
You Will Be Audited.....	3
What Is an Audit?.....	3
Regulated Industries That Require Audits.....	4
Regulated Industries Without Explicit Audits	4
Business Transactions Can Loop You into an Audit.....	5
A Lawsuit May Drag You into Something Worse Than an Audit	6
Business-to-Business Audits	6
Will/Should You Audit Your IT Security Controls?	6
Audit Misconceptions	7
The Burden of Audit Is on You.....	7
Aim Higher Than Compliance	7
Audits Are Useful	7
Audits Make You Look Good	8
The Audit as a Forcing Function	8
Audit Types	9
ISO 27001	9
The SSAE 16	9

PCI DSS.....	10
Auditors Auditing	10
What Is the Right Audit for You?.....	11
■ Chapter 2: Assume Breach	13
The Lesson of Fort Pulaski	13
The Invincible	13
Ownership Changes Hand	15
New Exploit Technology Is Introduced	15
The Complexity of IT Systems	16
A Tangled Web of Code	17
Complexity and Vulnerability	18
Technical Vulnerabilities	19
Attackers Are Motivated	19
The Assume Breach Mindset.....	20
Living in Assume Breach World	20
■ Chapter 3: Risk Analysis: Assets and Impacts	23
Why Risk.....	23
Risk Is Context Sensitive	24
Components of Risk	24
Calculating Likelihood	25
Calculating Impact	26
IT Asset Inventory	27
Asset Value Assessment	27
Assessing Impact	28
Indirect Impacts.....	29
Compliance Impacts	30
Qualitative vs. Quantitative	30
Qualitative Analysis	30
Clarifying Your Qualitative.....	30

Quantitative Analysis	34
Annualized Loss Expectancy	36
Formalizing Your Risk Process	36
■ Chapter 4: Risk Analysis: Natural Threats	39
Disaster Strikes	39
Risk Modeling.....	40
Modeling Natural Threats	41
Modeling Impact with Failure Mode Effects Analysis.....	43
Simple FMEA Example.....	44
Breaking down a System.....	45
Analyzing Functions.....	46
Determining Failure Effects.....	46
Business Impact Analysis.....	47
Documenting Assumptions.....	50
■ Chapter 5: Risk Analysis: Adversarial Risk	51
A Hospital under Attack.....	51
Adversarial Risk	52
Overview of Attacker Types	52
Understanding Attacker Capability	53
Technical Capability.....	53
Trickery Capability	54
Time.....	55
Techniques.....	55
Understanding Attacker Incentives	56
Monetary Incentives	57
Political Incentives.....	58
Personal Incentives	59

Common Attack Techniques	60
Kill Chain.....	60
Stealing Authentication.....	61
Exfiltration	62
Building the Adversarial Risk Model.....	62
Qualitative Example	62
Quantitative Example.....	64
■ Part II: Wrangling the Organization	67
■ Chapter 6: Scope	69
Developing Scope.....	69
Compliance Requirement Gathering	71
Zero in on PII.....	71
PCI DSS scoping	73
SSAE SOC 1 Scoping.....	73
Supporting Non-IT Departments.....	73
Double Check.....	73
Writing Scope Statements.....	74
Control Inventory	74
Control Effectiveness and Efficiency	75
Scoping Adjacent Systems.....	75
Scope Barriers.....	76
Technical Barriers.....	77
Physical Barriers.....	78
Process Barriers	78
Scoping Hints	79
Start Small and Expand	79
But Not Too Small	79
Simplification.....	79

■ Chapter 7: Governance	81
Governance Frameworks	82
The ISMS	82
Establish the ISMS	83
The ISMS Steering Committee.....	83
Duties of the ISMS Committee.....	85
Key Roles	86
ISMS Charter	88
Obtain Executive Sponsorship	90
Plan: Implement and Operate a Security Program	90
Decide upon and Publish the Goals	90
Do: Risk Treatment	91
Risk Treatment.....	93
Check: Monitor and Review Security Program	97
Act: Maintain and Improve Security Program.....	98
■ Chapter 8: Talking to the Suits	99
When Security Appears to be Anti-Business	99
Who Really Decides?	100
Understanding the Organization.....	100
How to Ask.....	101
Who Do You Ask	101
What to Ask.....	101
What to Do with This.....	103
Answering Questions	103
Do the Research	103
Don't Wander Outside Your Area of Expertise	104
How to Talk Their Talk.....	104
Explaining Risk.....	105
Proposing a Course of Action.....	107

- **Chapter 9: Talking to the Techs** **113**
 - IT Security vs. IT 114
 - Techie Traps..... 115
 - The Infinitely Long IT Work Queue 115
 - Perpetual Design 116
 - Dragging Projects 117
 - Other Tools..... 117
 - Working with Other Security Pros 118
 - IT Security Roles..... 118
 - Hiring for Security..... 119
- **Chapter 10: Talking to the Users** **123**
 - Specific Challenges for the Users 123
 - Complexity 124
 - Different Paradigm, Different Goals 124
 - Culture Clashes..... 125
 - Tools for Helping Users..... 125
 - Empathy..... 125
 - Let the Work Flow Smoothly 126
 - Work with the Users 127
 - Get Users on Your Side 128
 - Security Awareness Training 129
- **Part III: Managing Risk with Controls**..... **131**
 - **Chapter 11: Policy** **133**
 - What Is Policy? 133
 - What Isn't Policy 134
 - Writing Policy 134
 - Policy and the Law 135
 - Keep It Simple 135
 - Policies Don't Have to Be Perfect 135

Key Policy: Security Policy.....	136
Components of the Policy	136
Scope.....	136
Policy Goal	136
Governance.....	136
Risk Management.....	136
Expectations for User Behavior	137
Sample Security Policy	137
Key Policy: Acceptable Usage Policy	138
Goal.....	139
Scope.....	139
Privacy Disclaimers	139
Handling the Data	139
Handling the Machines	139
Define Misuse.....	140
Social Media	140
Security Responsibilities	140
Sanctions.....	140
Sample Acceptable Usage Policy.....	141
Policy Rollout.....	143
■ Chapter 12: Control Design.....	145
A Control Not Used Is a Control Wasted.....	145
What Is a Control?	146
What Is a Good Control?	146
Proportionate to Risk.....	146
Standardized and Measured.....	147
Documented	147

Control Lists	147
Controls in Combination	148
Key Controls	148
Compensating Controls	149
Control Functions and Failures	149
Control Cost.....	150
Reducing the Cost of Controls	151
■ Chapter 13: Administrative Controls	153
Control Maturity.....	153
Capability Maturity Model.....	154
The Power of Good Admin Controls	155
Differences in Documents	155
Critical Admin Control: Asset Management	156
Sample Asset Management Policy	156
Sample Asset Management Standard	156
Critical Admin Control: Change Control	157
Sample Change Control Policy.....	158
Change Control Standards.....	159
Change Control Tracking.....	159
Critical Admin Control: Application Security	160
Sample Application Security Policy	160
Application Security Standards	161
Software Acquisition.....	161
Critical Manual Control: Record and Media Management	162
Sample Record and Media Management Policy	162
■ Chapter 14: Vulnerability Management	165
Organizing Vulnerability Management.....	166
Sample Vulnerability Management Policy.....	166
Vulnerability Management Breakdown of Responsibilities.....	166

Hardening Standards.....	167
Sample Hardening and Vulnerability Management Standard	167
How to Fill in the Hardening Standards?	168
Vulnerability Discovery.....	169
Vulnerability Notification.....	169
Discovery Scanning	169
Vulnerability Scanning.....	171
Penetration Testing.....	172
Dynamic Application Testing.....	172
Prioritization and Risk Scoring	173
Higher Priority.....	173
Lower Priority	173
More Food for Thought	174
Patching	174
Scan Again.....	174
■ Chapter 15: People Controls	175
Policy for the People.....	175
Sample Human Resource Security Policy.....	175
Employee Role Changes.....	176
Background Screening	177
When to Check.....	178
Who to Check.....	178
What to Check	179
What to Do When There's a Problem	180
Employment Agreements	180
Security Training.....	181
Sanctions for Policy Violations	181
Managing the Insider Threat	182
Monitoring	182
Least Privilege	183

- Strong User Management..... 183
- Segregation of Duties 183
- Know Your User 184
- Filtering 184
- Processes, Not Individuals 184
- **Chapter 16: Logical Access Control..... 187**
- Defining Access Control 187
 - Sample Logical Access Control Policy 187
- Authentication 188
 - Something You Know 188
 - Something You Have..... 189
 - Something You Are..... 190
 - Multifactor Authentication 190
 - Authentication Standards 190
- Authorization 192
 - Role-based Access Control..... 192
 - System Authorization..... 194
 - Sample Authorization Standards 194
- Accountability..... 194
- Access Control Tools 195
- **Chapter 17: Network Security 197**
- Understand Networking Technology..... 197
- Network-based Attacks..... 198
 - Remote Exploits..... 199
 - Remote Password Guessing 200
 - Drive-by-Download Attacks 200
 - Network Denial of Service 201
 - Sniffing 202
 - Impersonation..... 204

Man-in-the-Middle	204
Exfiltration of Data	205
Network Controls.....	206
<i>Sample Network Security Policy</i>	206
Network Security Standards.....	208
Network Security Procedures.....	208
Firewalls	209
IDS/IPS.....	211
Transmission Encryption	212
■ Chapter 18: More Technical Controls.....	219
Internet Services Security	219
Web Services.....	219
E-mail Security	221
DNS Security.....	223
Encrypting Data at Rest.....	224
Why Is Encryption Hard to Do?	225
Storage Crypto Policy and Standards	226
Tokenization.....	226
Malware Controls	227
Anti-Malware Policy and Standards	227
Malware Defense in Depth	227
Building Custom Controls.....	228
■ Chapter 19: Physical Security Controls	231
Getting a Handle on Physical Security	231
Physical Risk Assessments	232
Physical Security Policy	232
Sample Physical Security Policy.....	233
Personnel Security	234
Visitor Security	234
Training.....	234

Security in the Offices	235
Clean Desk Policies	235
Network Access Controls.....	236
Secured Facilities Controls	236
Racks and Cages	236
Cameras	236
Alarms	236
Guards	237
Environmental Controls	237
Media and Portable Media Controls	237
Media Destruction	237
Laptop Controls	238
Convergence of IT and Physical Security Controls	238
■ Chapter 20: Response Controls	239
Logging	239
Sample Logging Policy	240
What You Must Log	240
Look at Your Logs	241
Protecting Your Logs.....	243
Backup and Failover	244
Keep Backups Offsite and Safe	244
What to Back Up	244
Backup Policy	245
Failover Systems	245
Business Continuity Planning	245
Sample Business Continuity Policy.....	246
Expectations for Recovery	246
Disaster Recovery Planning.....	247
Incident Response Planning	248
Incident Response Policy.....	248

Incident Response Plan	249
A Team Effort	249
Communication Strategies	251
Procedures for Common Scenarios	251
Gathering Data.....	252
Hunting and Fixing.....	253
Legal Reporting Requirements	253
Working with Law Enforcement.....	254
Human Side of Incident Response.....	254
After Action Analysis.....	255
Root Cause Analysis	255
Executive Summary.....	256
Practicing.....	256
■ Part IV: Being Audited.....	259
■ Chapter 21: Starting the Audit.....	261
Getting Ready for Audit	261
Picking an Auditor	263
We're All on the Same Side	264
What Happens During Audit	264
Scope Review	265
Control Review	265
Audit Evidence Gathering	266
Roles During an Audit.....	267
Specific Audits.....	268
SSAE 16 Audits	269
ISO 27001 Audits	271
PCI DSS Audit.....	272
Disagreeing with Auditors	273

- Chapter 22: Internal Audit 275**
 - The Role of Internal Audit..... 275
 - Internal Auditor Independence 275
 - Internal Auditor Competence 276
 - How Small Can the Role Go? 277
 - To Heal, Not to Punish 277
 - Check Before the Auditors Check 277
 - The Internal Audit Process 278
 - Measuring a Control 278
 - Publish to Management..... 281
 - Keep Records..... 281

- Chapter 23: Third-Party Security..... 283**
 - Which Third Parties Are Relevant? 283
 - Analysis of Third Parties..... 284
 - Risk Analysis..... 284
 - Control Gap Analysis Approach..... 285
 - Getting Answers 286
 - Reading Their Audit Reports 286
 - Analyzing It All 287
 - Controlling Third-Party Risk 287
 - Sample Policy for Third-Party Management 288
 - Software Procurement..... 288
 - Security Service Agreements 289
 - Technical Controls 291
 - Document Your Work 292

■ **Chapter 24: Post Audit Improvement 293**

Reviewing Everything..... 293

 Reviewing What Worked 293

 Reviewing What Didn't Work 295

Analyzing the Data 296

 Looking for Systematic Issues..... 297

 Look for Things that Aren't Broken yet, but Will Be 297

Making Changes..... 298

 Look Before You Leap 298

 Improving the Controls 298

 Bridge Letters 299

 Rolling out a Change Plan..... 299

We Can Never Stop Trying to Improve 300

Index..... 301