# Contents at a Glance

Chapter 1: Understanding Policy ......................................................... 2  
Chapter 2: Policy Elements and Style ............................................... 32  
Chapter 3: Information Security Framework ................................. 64  
Chapter 4: Governance and Risk Management .............................. 92  
Chapter 5: Asset Management ....................................................... 124  
Chapter 6: Human Resources Security ........................................... 156  
Chapter 7: Physical and Environmental Security ......................... 188  
Chapter 8: Communications and Operations Security .................. 218  
Chapter 9: Access Control Management ........................................ 264  
Chapter 10: Information Systems Acquisition, Development,  
and Maintenance ......................................................................... 300  
Chapter 11: Information Security Incident Management .............. 328  
Chapter 12: Business Continuity Management .............................. 370  
Chapter 13: Regulatory Compliance for Financial Institutions ........ 408  
Chapter 14: Regulatory Compliance for the Healthcare Sector ....... 442  
Chapter 15: PCI Compliance for Merchants .................................... 482  
Appendix A: Information Security Program Resources ................. 516  
Appendix B: Sample Information Security Policy ........................... 520  
Appendix C: Information Systems Acceptable Use  
Agreement and Policy ................................................................... 568  
Index ................................................................................................ 574
# Table of Contents

## Chapter 1: Understanding Policy

Looking at Policy Through the Ages ................................................................. 3
The Bible as Ancient Policy ............................................................................ 4
The United States Constitution as a Policy Revolution .................................. 5
Policy Today .................................................................................................... 5
Information Security Policy ............................................................................ 7
Successful Policy Characteristics ................................................................... 8
The Role of Government .................................................................................. 13
Information Security Policy Lifecycle ............................................................. 16
Policy Development ....................................................................................... 17
Policy Publication .......................................................................................... 18
Policy Adoption .............................................................................................. 19
Policy Review ................................................................................................ 20
References ..................................................................................................... 29
Regulations and Directives Cited ................................................................. 30
Other References ........................................................................................... 31

## Chapter 2: Policy Elements and Style

Policy Hierarchy ............................................................................................. 32
Standards ......................................................................................................... 33
Baselines ......................................................................................................... 34
Guidelines ....................................................................................................... 34
Procedures ...................................................................................................... 35
Plans and Programs ......................................................................................... 36
Policy Format .................................................................................................. 36
Policy Audience ............................................................................................. 36
Policy Format Types ....................................................................................... 37
Policy Components ......................................................................................... 38
<table>
<thead>
<tr>
<th>Writing Style and Technique</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Plain Language</td>
<td>48</td>
</tr>
<tr>
<td>The Plain Language Movement</td>
<td>49</td>
</tr>
<tr>
<td>Plain Language Techniques for Policy Writing</td>
<td>50</td>
</tr>
<tr>
<td>References</td>
<td>62</td>
</tr>
<tr>
<td>Regulations and Directives Cited</td>
<td>62</td>
</tr>
<tr>
<td>Other References</td>
<td>62</td>
</tr>
</tbody>
</table>

**Chapter 3: Information Security Framework**

<table>
<thead>
<tr>
<th>CIA</th>
<th>65</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is Confidentiality?</td>
<td>66</td>
</tr>
<tr>
<td>What Is Integrity?</td>
<td>68</td>
</tr>
<tr>
<td>What Is Availability?</td>
<td>69</td>
</tr>
<tr>
<td>Who Is Responsible for CIA?</td>
<td>72</td>
</tr>
<tr>
<td>Information Security Framework</td>
<td>72</td>
</tr>
<tr>
<td>What Is NIST’s Function?</td>
<td>72</td>
</tr>
<tr>
<td>What Does the ISO Do?</td>
<td>74</td>
</tr>
<tr>
<td>Can the ISO Standards and NIST Publications Be Used to Build a Framework?</td>
<td>75</td>
</tr>
<tr>
<td>References</td>
<td>90</td>
</tr>
<tr>
<td>Regulations Cited</td>
<td>90</td>
</tr>
<tr>
<td>ISO Research</td>
<td>90</td>
</tr>
<tr>
<td>NIST Research</td>
<td>91</td>
</tr>
<tr>
<td>Other References</td>
<td>91</td>
</tr>
</tbody>
</table>

**Chapter 4: Governance and Risk Management**

<table>
<thead>
<tr>
<th>Understanding Information Security Policies</th>
<th>93</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is Meant by Strategic Alignment?</td>
<td>94</td>
</tr>
<tr>
<td>Regulatory Requirements</td>
<td>94</td>
</tr>
<tr>
<td>User Versions of Information Security Policies</td>
<td>94</td>
</tr>
<tr>
<td>Vendor Versions of Information Security Policies</td>
<td>95</td>
</tr>
<tr>
<td>Client Synopsis of Information Security Policies</td>
<td>95</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Information Security Governance</td>
<td>100</td>
</tr>
<tr>
<td>What Is a Distributed Governance Model?</td>
<td>101</td>
</tr>
<tr>
<td>Regulatory Requirements</td>
<td>104</td>
</tr>
<tr>
<td>Information Security Risk</td>
<td>105</td>
</tr>
<tr>
<td>Is Risk Bad?</td>
<td>105</td>
</tr>
<tr>
<td>Risk Appetite and Tolerance</td>
<td>106</td>
</tr>
<tr>
<td>What Is a Risk Assessment?</td>
<td>106</td>
</tr>
<tr>
<td>Risk Assessment Methodologies</td>
<td>108</td>
</tr>
<tr>
<td>References</td>
<td>122</td>
</tr>
<tr>
<td>Regulations Cited</td>
<td>122</td>
</tr>
<tr>
<td>Other References</td>
<td>122</td>
</tr>
</tbody>
</table>

**Chapter 5: Asset Management**  

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Assets and Systems</td>
<td>125</td>
</tr>
<tr>
<td>Who Is Responsible for Information Assets?</td>
<td>126</td>
</tr>
<tr>
<td>Information Classification</td>
<td>128</td>
</tr>
<tr>
<td>How Does the Federal Government Classify Data?</td>
<td>129</td>
</tr>
<tr>
<td>Why Is National Security Information Classified Differently?</td>
<td>131</td>
</tr>
<tr>
<td>Who Decides How National Security Data Is Classified?</td>
<td>133</td>
</tr>
<tr>
<td>How Does the Private Sector Classify Data?</td>
<td>134</td>
</tr>
<tr>
<td>Can Information Be Reclassified or Even Declassified?</td>
<td>135</td>
</tr>
<tr>
<td>Labeling and Handling Standards</td>
<td>136</td>
</tr>
<tr>
<td>Why Label?</td>
<td>136</td>
</tr>
<tr>
<td>Why Handling Standards?</td>
<td>136</td>
</tr>
<tr>
<td>Information Systems Inventory</td>
<td>139</td>
</tr>
<tr>
<td>What Should Be Inventoried?</td>
<td>139</td>
</tr>
</tbody>
</table>
# Table of Contents

References .................................................................................................................. 154

Regulations Cited ........................................................................................................ 154

Executive Orders Cited ................................................................................................. 155

Other Research ........................................................................................................... 155

## Chapter 6: Human Resources Security  
156

The Employee Lifecycle ............................................................................................... 157

What Does Recruitment Have to Do with Security? ............................................... 158

What Happens in the Onboarding Phase? ................................................................. 165

What Is User Provisioning? ....................................................................................... 166

What Should an Employee Learn During Orientation? .......................................... 167

Why Is Termination Considered the Most Dangerous Phase? .............................. 168

The Importance of Employee Agreements ............................................................... 170

What Are Confidentiality or Non-disclosure Agreements? .................................. 170

What Is an Acceptable Use Agreement? .................................................................. 170

The Importance of Security Education and Training ............................................. 172

What Is the SETA Model? ....................................................................................... 173

References ............................................................................................................... 185

Regulations Cited ...................................................................................................... 186

Other Research ......................................................................................................... 186

## Chapter 7: Physical and Environmental Security  
188

Understanding the Secure Facility Layered Defense Model .................................. 190

How Do We Secure the Site? .................................................................................... 190

How Is Physical Access Controlled? ....................................................................... 192

Protecting Equipment ............................................................................................... 196

No Power, No Processing? ....................................................................................... 196

How Dangerous Is Fire? ......................................................................................... 198

What About Disposal? ............................................................................................. 200

Stop, Thief! ............................................................................................................... 203
Chapter 8: Communications and Operations Security  

Standard Operating Procedures (SOPs) ......................................................... 219
  Why Document SOPs? ................................................................. 220
  Developing SOPs ........................................................................ 220
Operational Change Control ........................................................................ 225
  Why Manage Change? ................................................................. 225
  Why Is Patching Handled Differently? ........................................... 228
Malware Protection .................................................................................... 230
  Are There Different Types of Malware? ......................................... 231
  How Is Malware Controlled? ......................................................... 233
  What Is Antivirus Software? .......................................................... 234
Data Replication .................................................................................... 235
  Is There a Recommended Backup or Replication Strategy? .......... 235
Secure Messaging ................................................................................... 237
  What Makes Email a Security Risk? ............................................... 237
  Are Email Servers at Risk? ............................................................ 240
Activity Monitoring and Log Analysis ..................................................... 242
  What Is Log Management? ............................................................. 242
Service Provider Oversight ..................................................................... 245
  What Is Due Diligence? ................................................................. 245
  What Should Be Included in Service Provider Contracts? ............ 247
References ............................................................................................. 261
  Regulations Cited .......................................................................... 261
  Other References .......................................................................... 261

Chapter 9: Access Control Management  

Access Control Fundamentals ................................................................. 265
  What Is a Security Posture? ............................................................. 266
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Is Identity Verified?</td>
<td>266</td>
</tr>
<tr>
<td>What Is Authorization?</td>
<td>270</td>
</tr>
<tr>
<td>Infrastructure Access Controls</td>
<td>272</td>
</tr>
<tr>
<td>Why Segment a Network?</td>
<td>272</td>
</tr>
<tr>
<td>Remote Access Security</td>
<td>277</td>
</tr>
<tr>
<td>User Access Controls</td>
<td>282</td>
</tr>
<tr>
<td>Why Manage User Access?</td>
<td>282</td>
</tr>
<tr>
<td>What Types of Access Should Be Monitored?</td>
<td>284</td>
</tr>
<tr>
<td>References</td>
<td>297</td>
</tr>
<tr>
<td>Regulations Cited</td>
<td>297</td>
</tr>
<tr>
<td>Other References</td>
<td>297</td>
</tr>
<tr>
<td>Chapter 10: Information Systems Acquisition, Development, and Maintenance</td>
<td>300</td>
</tr>
<tr>
<td>System Security Requirements</td>
<td>301</td>
</tr>
<tr>
<td>Secure Code</td>
<td>306</td>
</tr>
<tr>
<td>Cryptography</td>
<td>310</td>
</tr>
<tr>
<td>References</td>
<td>326</td>
</tr>
<tr>
<td>Regulations Cited</td>
<td>326</td>
</tr>
<tr>
<td>Other References</td>
<td>327</td>
</tr>
<tr>
<td>Chapter 11: Information Security Incident Management</td>
<td>328</td>
</tr>
<tr>
<td>Organizational Incident Response</td>
<td>329</td>
</tr>
<tr>
<td>What Is an Incident?</td>
<td>330</td>
</tr>
<tr>
<td>How Are Incidents Reported</td>
<td>334</td>
</tr>
<tr>
<td>What Is an Incident Response Program?</td>
<td>335</td>
</tr>
<tr>
<td>What Happened? Investigation and Evidence Handling</td>
<td>340</td>
</tr>
<tr>
<td>Data Breach Notification Requirements</td>
<td>345</td>
</tr>
<tr>
<td>Is There a Federal Breach Notification Law?</td>
<td>347</td>
</tr>
<tr>
<td>Does Notification Work?</td>
<td>351</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter 12: Business Continuity Management</th>
<th>370</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Preparedness</td>
<td>371</td>
</tr>
<tr>
<td>What Is a Resilient Organization?</td>
<td>372</td>
</tr>
<tr>
<td>Business Continuity Risk Management</td>
<td>374</td>
</tr>
<tr>
<td>What Is a Business Continuity Threat Assessment?</td>
<td>375</td>
</tr>
<tr>
<td>What Is a Business Continuity Risk Assessment?</td>
<td>376</td>
</tr>
<tr>
<td>What Is a Business Impact Assessment?</td>
<td>378</td>
</tr>
<tr>
<td>The Business Continuity Plan</td>
<td>380</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>381</td>
</tr>
<tr>
<td>Disaster Response Plans</td>
<td>384</td>
</tr>
<tr>
<td>Operational Contingency Plans</td>
<td>387</td>
</tr>
<tr>
<td>The Disaster Recovery Phase</td>
<td>388</td>
</tr>
<tr>
<td>The Resumption Phase</td>
<td>391</td>
</tr>
<tr>
<td>Plan Testing and Maintenance</td>
<td>392</td>
</tr>
<tr>
<td>Why Is Testing Important?</td>
<td>392</td>
</tr>
<tr>
<td>Plan Maintenance</td>
<td>393</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13: Regulatory Compliance for Financial Institutions</th>
<th>408</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Gramm-Leach-Bliley Act (GLBA)</td>
<td>409</td>
</tr>
<tr>
<td>What Is a Financial Institution?</td>
<td>410</td>
</tr>
<tr>
<td>What Are the Interagency Guidelines?</td>
<td>412</td>
</tr>
<tr>
<td>What Is a Regulatory Examination?</td>
<td>423</td>
</tr>
</tbody>
</table>
What Is the SAQ? ........................................................................................................502
Are There Penalties for Noncompliance? ..........................................................503
References .............................................................................................................514

**Appendix A: Information Security Program Resources** 516

| National Institute of Standards and Technology (NIST) Special Publications | 516 |
| Federal Financial Institutions Examination Council (FFIEC) IT Handbooks | 518 |
| Department of Health and Human Services HIPAA Security Series | 518 |
| Payment Security Standards Council Documents Library | 518 |

| Information Security Professional Development and Certification Organizations | 519 |

**Appendix B: Sample Information Security Policy** 520

| Introduction | 520 |
| Policy Exemptions | 521 |
| Policy Violation | 521 |
| Version Control | 521 |

| Section 1: Governance and Risk Management | 522 |
| Overview | 522 |
| Goals and Objectives for Section 1: Governance and Risk Management | 522 |
| Governance and Risk Management Policy Index | 522 |
| 1.0 Governance and Risk Management Policy | 523 |
| Supporting Resources and Source Material | 526 |

| Lead Author | 526 |

| Section 2: Asset Management | 527 |
| Overview | 527 |
| Goals and Objectives for Section 2: Asset Management | 527 |
| Asset Management Policy Index | 527 |
| 2.0 Asset Management Policy | 527 |

| Supporting Resources and Source Material | 529 |

| Lead Author | 529 |
## Table of Contents

Section 7: Information Systems Acquisition, Development, and Maintenance ..........................................................................................554
- Overview .................................................................................................554
- Goals and Objectives for Section 7: Information Systems Acquisition, Development, and Maintenance ...........................................................554
- Information Systems Acquisition, Development, and Maintenance Policy Index ..........................................................................................554
- 7.0 Information Systems Acquisition, Development, and Maintenance Policy ...............................................................................554
- Supporting Resources and Source Material ...........................................556
- Lead Author ............................................................................................556

Section 8: Incident Management .....................................................................557
- Overview .................................................................................................557
- Goals and Objectives for Section 8: Incident Management ....................557
- Incident Management Policy Index ..........................................................557
- 8.0 Incident Management Policy ...............................................................557
- Supporting Resources and Source Material ...........................................561
- Lead Author ............................................................................................561

Section 9: Business Continuity ........................................................................562
- Overview .................................................................................................562
- Goals and Objectives for Section 9: Business Continuity .......................562
- Business Continuity Policy Index ...............................................................562
- 9.0 Business Continuity Policy .................................................................563
- Supporting Resources and Source Material ...........................................567
- Lead Author ............................................................................................567

Appendix C: Information Systems Acceptable Use Agreement and Policy 568
- Information Systems Acceptable Use Agreement ...........................................568
- Distribution ..............................................................................................568
- Information Systems Acceptable Use Agreement ...........................................568
Acceptable Use of Information Systems Policy ..............................................569

1.0 Data Protection .......................................................................................569
2.0 Authentication and Password Controls..................................................570
3.0 Application Security .............................................................................571
4.0 Messaging Use and Security ................................................................571
5.0 Internet Use and Security ....................................................................572
6.0 Mobile Devices Security .......................................................................572
7.0 Remote Access Security ......................................................................573
8.0 Incident Detection and Reporting .......................................................573
About the Author

Sari Stern Greene was at the forefront of the security battlefield when she founded Sage Data Security in 2002. Sage’s award-winning portfolio of advisory, assessment, and assurance security services are designed to protect an organization’s information assets and ensure regulatory compliance. An entrenched security practitioner, Sari has amassed thousands of hours in the field working with a spectrum of technical, operational, and management personnel, as well as boards of directors, regulators, and service providers.

Sari provided expert witness testimony in the groundbreaking PATCO v. Ocean National Bank case. From 2006 through 2010, she served as the managing director for the MEAPC, a coalition of 24 financial institutions that embrace a mission of preventing information theft and fraud through public education and awareness. Since 2010, she has served as the chair of the annual Cybercrime Symposium held in Portsmouth, New Hampshire.

A recognized leader in the field of information security, Sari’s first book was Tools and Techniques for Securing Microsoft Networks, soon followed by the first edition of Security Policies and Procedures: Principles and Practices. She has published a number of articles related to information security and has been quoted in The New York Times, Wall Street Journal, CNN, and on CNBC. She speaks regularly at security conferences and workshops around the country and is a frequent guest lecturer.

Sari has an MBA from the University of New Hampshire system and has earned an array of government and industry certifications and accreditations, including ISACA Certification in Risk and Information Systems Control (CRISC), ISACA Certification in Security Management (CISM), ISC² Certification in Information Systems Security (CISSP), and Microsoft Certified Network Engineer (MCSE), and is certified by the National Security Agency to conduct NSA-IAM assessments for federal government agencies and contractors.

You can contact Sari at sari@sarigreene.com or follow her on Twitter @sari_greene.
Dedication

To all who honor the public trust.

Acknowledgments

Transforming raw material into a useful publication is a team effort. My colleagues at Sage Data Security generously and passionately shared their knowledge. Dr. Ron Gonzales of National University and Tatyana Zidarov of Kaplan University provided thoughtful feedback and recommendations. Senior Development Editor Chris Cleveland and Development Editor Jeff Riley expertly guided the process. The Fadiman family made available a wonderful workspace. The Captain, as always, waited patiently. To all, I am grateful.
We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we’re doing right, what we could do better, what areas you’d like to see us publish in, and any other words of wisdom you’re willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn’t like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book’s title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
      ATTN: Reader Feedback
      800 East 96th Street
      Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.
Chapter 4

Governance and Risk Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

■ Explain the importance of strategic alignment.
■ Know how to manage information security policies.
■ Describe information security–related roles and responsibilities.
■ Identify the components of risk management.
■ Create polices related to information security policy, governance, and risk management.

Information Security Policies (ISO 27002:2013 Section 5) and Organization of Information Security (ISO 27002:2013 Section 6) are closely related, so we address both domains in this chapter. The Information Security Policies domain focuses on information security policy requirements and the need to align policy with organizational objectives. The Organization of Information Security domain focuses on the governance structure necessary to implement and manage information security policy operations, across and outside of the organization. Included in this chapter is a discussion of risk management because it is a fundamental aspect of governance, decision making, and policy. Risk management is important enough that it warrants two sets of standards: ISO/IEC 27005 and ISO/IEC 31000.
FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 5 of ISO 27002:2013 is titled “Information Security Policies.” This domain addresses policy development and authorization. Section 6 of ISO 27002:2013 is titled “Organization of Information Security.” This domain addresses information security governance as well as enterprise roles and responsibilities. Risk management principles, risk assessment techniques, and information security risk management systems are described in ISO 27005:2005 and the ISO 31000 series.

Corresponding NIST guidance is provided in the following documents:

- SP 800-12: An Introduction to Computer Security: The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-30: Risk Management Guide for Information Technology Systems

Understanding Information Security Policies

Information security policies, standards, procedures, and plans exist for one reason—to protect the organization and, by extension, its constituents from harm. The lesson of the Information Security Policies domain is threefold:

- Information security directives should be codified in a written policy document.
- It is important that management participate in policy development and visibly support the policy.
- The necessity of strategically aligning information security with business requirements and relevant laws and regulations.

Internationally recognized standard security standards such as the ISO 27002:2013 can provide a framework, but ultimately each organization must construct its own security strategy and policy taking into consideration organizational objectives and regulatory requirements.
What Is Meant by Strategic Alignment?

The two approaches to information security are parallel and integrated. A parallel approach silos information security, assigns responsibility for being secure to the IT department, views compliance as discretionary, and has little or no organizational accountability. An integrated approach recognizes that security and success are intertwined. When strategically aligned, security functions as a business enabler that adds value. Security is an expected topic of discussion among decision makers and is given the same level of respect as other fundamental drivers and influencing elements of the business. This doesn’t happen magically. It requires leadership that recognizes the value of information security, invests in people and processes, encourages discussion and debate, and treats security in the same fashion as every other business requirement. It also requires that information security professionals recognize that the true value of information security is protecting the business from harm and achieving organizational objectives. Visible management support coupled with written policy formalizes and communicates the organizational commitment to information security.

Regulatory Requirements

In an effort to protect the citizens of the United States, legislators recognized the importance of written information security policies. Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Family Educational Rights and Privacy Act (FERPA), and the Federal Information Systems Management Act (FISMA) all require covered entities to have in place written policies and procedures that protect their information assets. They also require the policies to be reviewed on a regular basis. Each of these legislative acts better secured each person’s private information and the governance to reduce fraudulent reporting of corporate earnings.

Many organizations find that they are subject to more than one set of regulations. For example, publicly traded banks are subject to both GLBA and SOX requirements, whereas medical billing companies find themselves subject to both HIPAA and GLBA. Organizations that try to write their policies to match federal state regulations find the task daunting. Fortunately, the regulations published to date have enough in common that a well-written set of information security policies based on a framework such as the ISO 27002 can be mapped to multiple regulatory requirements. Policy administrative notations will often include a cross-reference to specific regulatory requirements.

User Versions of Information Security Policies

Information security policies are governance statements written with the intent of directing the organization. Correctly written, policies can also be used as teaching documents that influence behavior. An Acceptable Use Policy document and corresponding agreement should be developed specifically for distribution to the user community. The Acceptable Use Policy should include only pertinent information and, as appropriate, explanations and examples. The accompanying agreement requires users to acknowledge that they understand their responsibilities and affirm their individual commitment.
Vendor Versions of Information Security Policies

As we will discuss in Chapter 8, “Communications and Operations Security,” companies can outsource work but not responsibility or liability. Vendors or business partners (often referred to as “third parties”) that store, process, transmit, or access information assets should be required to have controls that meet or, in some cases, exceed organizational requirements. One of the most efficient ways to evaluate vendor security is to provide them with a vendor version of organizational security policies and require them to attest to their compliance. The vendor version should only contain policies that are applicable to third parties and should be sanitized as to not disclose any confidential information.

Client Synopsis of Information Security Policies

In this context, client refers to companies to which the organization provides services. A synopsis of the information security policy should be available upon request to clients. As applicable to the client base, the synopsis could be expanded to incorporate incident response and business continuity procedures, notifications, and regulatory cross-references. The synopsis should not disclose confidential business information unless the recipients are required to sign a non-disclosure agreement.

In Practice

Information Security Policy

**Synopsis:** The organization is required to have a written information security policy and supporting documents.

**Policy Statement:**

- The company must have written information security policies.
- Executive management is responsible for establishing the mandate and general objectives of the information security policy.
- The policies must support organizational objectives.
- The policies must comply with relevant statutory, regulatory, and contractual requirements.
- The policies must be communicated to all relevant parties both within and external to the company.
- As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of policy objectives and requirements.
- For the purpose of educating the workforce, user-level documents will be derived from the information security policy including but not limited to Acceptable Use Policy, Acceptable Use Agreement, and Information Handling Instructions.
- Any information security policy distributed outside the organization must be sanitized.
- All documentation will be retained for a period of six years from the last effective date.
Who Authorizes Information Security Policy?

A policy is a reflection of the organization’s commitment, direction, and approach. Information security policies should be authorized by executive management. Depending on the size, legal structure, and/or regulatory requirements of the organization, executive management may be defined as owners, directors, or executive officers.

Because executive management is responsible for and can be held legally liable for the protection of information assets, it is incumbent upon those in leadership positions to remain invested in the proper execution of the policy as well as the activities of oversight that ensure it. The National Association of Corporate Directors (NACD), the leading membership organization for Boards and Directors in the U.S., recommends four essential practices:

- Place information security on the Board’s agenda.
- Identify information security leaders, hold them accountable, and ensure support for them.
- Ensure the effectiveness of the corporation’s information security policy through review and approval.
- Assign information security to a key committee and ensure adequate support for that committee.

Policies should be reviewed at planned intervals to ensure their continuing suitability, adequacy, and effectiveness.
In tort law, duty of care is a legal standard applied to directors and officers of a corporation. In 1996, the shareholders of Caremark International, Inc., brought a derivative action, alleging that the Board of Directors breached their duty of care by failing to put in place adequate internal control systems. In response, the Delaware court defined a multifactor test designed to determine when duty of care is breached:

- The directors knew or should have known that violations of the law were occurring, and
- The directors took no steps in a good faith effort to prevent or remedy the situation, and
- Such failure proximately resulted in the losses complained of.

According to the firm of Orrick, Herrington and Sutcliffe, LLP, “in short, as long as a director acts in good faith, as long as she exercises proper due care and does not exhibit gross negligence, she cannot be held liable for failing to anticipate or prevent a cyber attack. However, if a plaintiff can show that a director failed to act in the face of a known duty to act, thereby demonstrating a conscious disregard for [her] responsibilities, it could give rise to a claim for breach of fiduciary duty.”

Revising Information Security Policies: Change Drivers

Because organizations change over time, policies need to be revisited. Change drivers are events that modify how a company does business. Change drivers can be demographic, economic, technological, and regulatory or personnel related. Examples of change drivers include company acquisition, new products, services or technology, regulatory updates, entering into a contractual obligation, and entering a new market. Change can introduce new vulnerabilities and risks. Change drivers should trigger internal assessments and ultimately a review of policies. Policies should be updated accordingly and subject to reauthorization.

Evaluating Information Security Policies

Directors and executive management have a fiduciary obligation to manage the company in a responsible manner. It is important that they be able to accurately gauge adherence to policy directives, the effectiveness of information security policies, and the maturity of the information security program. Standardized methodologies such as audits and maturity models can be used as evaluation and reporting mechanisms. Organizations may choose to conduct these evaluations using in-house personnel or engage independent third parties. The decision criteria include the size and complexity of the organization, regulatory requirements, available expertise, and segregation of duties. To be considered independent, assessors should not be responsible for, benefit from, or have in any way influenced the design, installation, maintenance, and operation of the target, or the policies and procedures that guide its operation.
Audit

An information security audit is a systematic, evidence-based evaluation of how well the organization conforms to established criteria such as Board-approved policies, regulatory requirements, and internationally recognized standards such as the ISO 27000 series. Audit procedures include interviews, observation, tracing documents to management policies, review of practices, review of documents, and tracing data to source documents. An audit report is a formal opinion (or disclaimer) of the audit team based on predefined scope and criteria. Audit reports generally include a description of the work performed, any inherent limitations of the work, detailed findings, and recommendations.

FYI: Certified Information Security Auditor (CISA)

The CISA certification is granted by ISACA (previously known as the Information Systems Audit and Control Association) to professionals who have demonstrated a high degree of audit-related knowledge and have verifiable work experience. The CISA certification is well respected across the globe, and the credibility of its continuing professional education (CPE) program ensures that CISA-certified professionals maintain their skill set. The American National Standards Institute (ANSI) accredited the CISA certification program under ISO/IEC 17024:2003: General Requirements for Bodies Operating Certification Systems of Persons. For more information about ISACA certification, visit www.isaca.org.

Capability Maturity Model (CMM)

A capability maturity model (CMM) is used to evaluate and document process maturity for a given area. The term maturity relates to the degree of formality and structure, ranging from ad hoc to optimized processes. Funded by the United States Air Force, the CMM was developed in the mid-1980s at the Carnegie Mellon University Software Engineering Institute. The objective was to create a model for the military to use to evaluate software development. It has since been adopted for subjects as diverse as information security, software engineering, systems engineering, project management, risk management, system acquisition, information technology (IT) services, and personnel management. It is sometimes combined with other methodologies such as ISO 9001, Six Sigma, Extreme Programming (XP), and DMAIC.

As documented in Table 4.1, a variation of the CMM can be used to evaluate enterprise information security maturity. Contributors to the application of the model should possess intimate knowledge of the organization and expertise in the subject area.
### TABLE 4.1 Capability Maturity Model (CMM) Scale

<table>
<thead>
<tr>
<th>Level</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Nonexistent</td>
<td>The organization is unaware of the need for policies or processes.</td>
</tr>
<tr>
<td>1</td>
<td>Ad-hoc</td>
<td>There are no documented policies or processes; there is sporadic activity.</td>
</tr>
<tr>
<td>2</td>
<td>Repeatable</td>
<td>Policies and processes are not fully documented; however, the activities occur on a regular basis.</td>
</tr>
<tr>
<td>3</td>
<td>Defined process</td>
<td>Policies and processes are documented and standardized; there is an active commitment to implementation.</td>
</tr>
<tr>
<td>4</td>
<td>Managed</td>
<td>Policies and processes are well defined, implemented, measured, and tested.</td>
</tr>
<tr>
<td>5</td>
<td>Optimized</td>
<td>Policies and process are well understood and have been fully integrated into the organizational culture.</td>
</tr>
</tbody>
</table>

As Figure 4.1 illustrates, the result is easily expressed in a graphic format and succinctly conveys the state of the information security program on a per-domain basis. The challenge with any scale-based model is that sometimes the assessment falls in between levels, in which case it is perfectly appropriate to use gradations (such as 3.5). This is an effective mechanism for reporting to those responsible for oversight, such as the Board of Directors or executive management. Process improvement objectives are a natural outcome of a CMM assessment.

![Information Security Program Maturity Assessment](image)

**FIGURE 4.1** Capability maturity model (CMM) assessment.
In Practice

Information Security Policy Authorization and Oversight Policy

Synopsis: Information security policies must be authorized by the Board of Directors. The relevance and the effectiveness of the policy must be reviewed annually.

Policy Statement:

- The Board of Directors must authorize the information security policy.
- An annual review of the information security policy must be conducted.
- The Chief Information Security Officer (CISO) is responsible for managing the review process.
- Changes to the policy must be presented to and approved by a majority of the Board of Directors.
- The Chief Operating Officer (COO) and the CISO will jointly present an annual report to the Board of Directors that provides them the information necessary to measure the organizations’ adherence to the information security policy objectives and the maturity of the information security program.
- When in-house knowledge is not sufficient to review or audit aspects of the information security policy, or if circumstances dictate independence, third-party professionals must be engaged.

Information Security Governance

*Governance* is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The ISO 27002:2013 Organization of Information Security domain objective is “to establish a management framework to initiate and control the implementation and operation of information security within the organization.” This domain requires organizations to decide who is responsible for security management, the scope of their authority, and how and when it is appropriate to engage outside expertise. Julie Allen, in her seminal work “Governing for Enterprise Security,” passionately articulated the importance of governance as applied to information security:

“Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization’s management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organization’s desired state of security will not be articulated, achieved or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.”
The Board of Directors (or organizational equivalent) is generally the authoritative policy-making body and responsible for overseeing the development, implementation, and maintenance of the information security program. The use of the term “oversee” is meant to convey the Board’s conventional supervisory role, leaving day-to-day responsibilities to management. Executive management should be tasked with providing support and resources for proper program development, administration, and maintenance as well as ensuring strategic alignment with organizational objectives.

**What Is a Distributed Governance Model?**

It is time to bury the myth that “security is an IT issue.” Security is not an isolated discipline and should not be siloed. Designing and maintaining a secure environment that supports the mission of the organization requires enterprise-wide input, decision making, and commitment. The foundation of a distributed governance model is the principle that stewardship is an organizational responsibility. Effective security requires the active involvement, cooperation, and collaboration of stakeholders, decision makers, and the user community. Security should be given the same level of respect as other fundamental drivers and influencing elements of the business.

**Chief Information Security Officer (CISO)**

Even in the most security-conscious organization, someone still needs to provide expert leadership. That is the role of the CISO. As a member of the executive team, the CISO is positioned to be a leader, teacher, and security champion. The CISO coordinates and manages security efforts across the company, including IT, human resources (HR), communications, legal, facilities management, and other groups. The most successful CISOs successfully balance security, productivity, and innovation. The CISO must be an advocate for security as a business enabler while being mindful of the need to protect the organizational from unrecognized harm. They must be willing to not be the most popular person in the room. This position generally reports directly to a senior functional executive (CEO, COO, CFO, General Counsel) and should have an unfiltered communication channel to the Board of Directors.

In smaller organizations, this function is often vested in the non-executive-level position of Information Security Officer (ISO). A source of conflict in many companies is whom the ISO should report to and if they should be a member of the IT team. It is not uncommon or completely out of the question for the position to report to the CIO. However, this chain of command can raise questions concerning adequate levels of independence. To ensure appropriate segregation of duties, the ISO should report directly to the Board or to a senior officer with sufficient independence to perform their assigned tasks. Security officers should not be assigned operational responsibilities within the IT department. They should have sufficient knowledge, background, and training, as well as a level of authority that enables them to adequately and effectively perform their assigned tasks. Security decision making should not be a singular task. Supporting the CISO or ISO should be a multidisciplinary committee that represents functional and business units.
In Practice

CISO Policy

Synopsis: To define the role of the CISO as well as the reporting structure and lines of communication.

Policy Statement:

- The COO will appoint the CISO.
- The CISO will report directly to the COO.
- At his or her discretion, the CISO may communicate directly with members of the Board of Directors.
- The CISO is responsible for managing the information security program, ensuring compliance with applicable regulations and contractual obligations, and working with business units to align information security requirements and business initiatives.
- The CISO will function as an internal consulting resource on information security issues.
- The CISO will chair the Information Security Steering Committee.
- The CISO will be a standing member of the Incident Response Team and the Continuity of Operations Team.
- Quarterly, the CISO will report to the executive management team on the overall status of the information security program. The report should discuss material matters, including such issues as risk assessment, risk management, control decisions, service provider arrangements, results of testing, security breaches or violations, and recommendations for policy changes.

Information Security Steering Committee

Creating a culture of security requires positive influences at multiple levels within an organization. Having an Information Security Steering Committee provides a forum to communicate, discuss, and debate on security requirements and business integration. Typically, members represent a cross-section of business lines or departments, including operations, risk, compliance, marketing, audit, sales, HR, and legal. In addition to providing advice and counsel, their mission is to spread the gospel of security to their colleagues, coworkers, subordinates, and business partners.
In Practice

Information Security Steering Committee Policy

Synopsis: The Information Security Steering Committee (ISC) is tasked with supporting the information security program.

Policy Statement:

- The Information Security Steering Committee serves in an advisory capacity in regards to the implementation, support, and management of the information security program, alignment with business objectives, and compliance with all applicable state and federal laws and regulations.
- The Information Security Steering Committee provides an open forum to discuss business initiatives and security requirements. Security is expected to be given the same level of respect as other fundamental drivers and influencing elements of the business.
- Standing membership will include the CISO (Chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives. Adjunct committee members may include but are not limited to representatives of HR, training, and marketing.
- The Information Security Steering Committee will meet on a monthly basis.

Organizational Roles and Responsibilities

In addition to the CISO and the Information Security Steering Committee, distributed throughout the organization are a variety of roles that have information security–related responsibilities. For example:

- **Compliance Officer**—Responsible for identifying all applicable information security–related statutory, regulatory, and contractual requirements.
- **Privacy Officer**—Responsible for the handling and disclosure of data as it relates to state, federal, and international law and customs.
- **Internal audit**—Responsible for measuring compliance with Board-approved policies and to ensure that controls are functioning as intended.
- **Incident response team**—Responsible for responding to and managing security-related incidents.
- **Data owners**—Responsible for defining protection requirements for the data based on classification, business need, legal, and regulatory requirements; reviewing the access controls; and monitoring and enforcing compliance with policies and standards.
Data custodians—Responsible for implementing, managing, and monitoring the protection mechanisms defined by data owners and notifying the appropriate party of any suspected or known policy violations or potential endangerments.

Data users—are expected to act as agents of the security program by taking reasonable and prudent steps to protect the systems and data they have access to.

Each of these responsibilities should be documented in policies, job descriptions, or employee manuals.

Regulatory Requirements
The necessity of formally assigning information security–related roles and responsibilities cannot be overstated. The requirement has been codified in numerous standards, regulations, and contractual obligations—most notably:

Gramm-Leach-Bliley (GLBA) Section 314.4: “In order to develop, implement, and maintain your information security program, you shall (a) Designate an employee or employees to coordinate your information security program.”

HIPAA/HITECH Security Rule Section 164.308(a): “Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity.”

Payment Card Industry Data Security Standard (PCI DDS) Section 12.5: “Assign to an individual or team the following information security management responsibilities: establish, document, and distribute security policies and procedures; monitor and analyze security alerts and information, and distribute to appropriate personnel; establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; administer user accounts, including additions, deletions, and modifications; monitor and control all access to data.”

201 CMR 17: Standards for the Protection of Personal Information of the Residents of the Commonwealth – Section 17.0.2: “Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to: (a) Designating one or more employees to maintain the comprehensive information security program.”

Creating a culture of security requires positive influences at multiple levels within an organization. Security champions reinforce by example the message that security policies and practices are important to the organization. The regulatory requirement to assign security responsibilities is a de facto mandate to create security champions.
Information Security Risk

Three factors influence information security decision making and policy development:

- Guiding principles
- Regulatory requirements
- Risks related to achieving their business objectives.

Risk is the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction. The motivation for “taking a risk” is a favorable outcome. “Managing risk” implies that other actions are being taken to either mitigate the impact of the undesirable or unfavorable outcome and/or enhance the likelihood of a positive outcome.

For example, a venture capitalist (VC) decides to invest a million dollars in a startup company. The risk (undesirable outcome) in this case is that the company will fail and the VC will lose part or all of her investment. The motivation for taking this risk is that the company becomes wildly successful and the initial backers make a great deal of money. To influence the outcome, the VC may require a seat on the Board of Directors, demand frequent financial reports, and mentor the leadership team. Doing these things, however, does not guarantee success. Risk tolerance is how much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit—in this case, how much money the VC is willing to lose. Certainly, if the VC believed that the company was destined for failure, the investment would not be made. Conversely, if the VC determined that the likelihood of a three-million-dollar return on investment was high, she may be willing to accept the tradeoff of a potential $200,000 loss.

Is Risk Bad?

Inherently, risk is neither good nor bad. All human activity carries some risk, although the amount varies greatly. Consider this: Every time you get in a car you are risking injury or even death. You manage the risk by keeping your car in good working order, wearing a seat belt, obeying the rules of the road, not texting, not being impaired, and paying attention. Your risk tolerance is that the reward for reaching your destination outweighs the potential harm.

Risk taking can be beneficial and is often necessary for advancement. For example, entrepreneurial risk taking can pay off in innovation and progress. Ceasing to take risks would quickly wipe out experimentation, innovation, challenge, excitement, and motivation. Risk taking can, however, be detrimental when ill considered or motivated by ignorance, ideology, dysfunction, greed, or revenge. The key is to balance risk against rewards by making informed decisions and then managing the risk commensurate with organizational objectives. The process of managing risk requires organizations to assign risk-management responsibilities, establish the organizational risk appetite and tolerance, adopt a standard methodology for assessing risk, respond to risk levels, and monitor risk on an ongoing basis.
Risk Appetite and Tolerance

Risk appetite is a strategic construct and broadly defined as the amount of risk an entity is willing to accept in pursuit of its mission. Risk tolerance is tactical and specific to the target being evaluated. Risk tolerance levels can be qualitative (for example, low, elevated, severe) or quantitative (for example, dollar loss, number of customers impacted, hours of downtime). It is the responsibility of the Board of Directors and executive management to establish risk tolerance criteria, set standards for acceptable levels of risk, and disseminate this information to decision makers throughout the organization.

In Practice

Information Security Risk Management Oversight Policy

Synopsis: To assign organizational roles and responsibilities with respect to risk management activities.

Policy Statement:

- Executive management, in consultation with the Board of Directors, is responsible for determining the organizational risk appetite and risk tolerance levels.
- Executive management will communicate the above to decision makers throughout the company.
- The CISO, in consultation with the Chief Risk Officer, is responsible for determining the information security risk assessment schedule, managing the risk assessment process, certifying results, jointly preparing risk reduction recommendations with business process owners, and presenting the results to executive management.
- The Board of Directors will be apprised by the COO of risks that endanger the organization, stakeholders, employees, or customers.

What Is a Risk Assessment?

An objective of a risk assessment is to evaluate what could go wrong, the likelihood of such an event occurring, and the harm if it did. In information security, this objective is generally expressed as the process of (a) identifying the inherent risk based on relevant threats, threat sources, and related vulnerabilities; (b) determining the impact if the threat source was successful; and (c) calculating the likelihood of occurrence, taking into consideration the control environment in order to determine residual risk.

- Inherent risk is the level of risk before security measures are applied.
- A threat is a natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact. Information security focuses on the threats to confidentiality (unauthorized use or disclosure), integrity (unauthorized or accidental modification), and availability (damage or destruction).
A **threat source** is either (1) intent and method targeted at the intentional exploitation of a vulnerability, such as criminal groups, terrorists, bot-net operators, and disgruntled employees, or (2) a situation and method that may accidentally trigger a vulnerability such as an undocumented process, severe storm, and accidental or unintentional behavior.

A **vulnerability** is a weakness that could be exploited by a threat source. Vulnerabilities can be physical (for example, unlocked door, insufficient fire suppression), natural (for example, facility located in a flood zone or in a hurricane belt), technical (for example, misconfigured systems, poorly written code), or human (for example, untrained or distracted employee).

**Impact** is the magnitude of harm.

The **likelihood of occurrence** is a weighted factor or probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).

A **control** is a security measure designed to prevent, deter, detect, or respond to a threat source.

**Residual risk** is the level of risk after security measures are applied. In its most simple form, residual risk can be defined as the likelihood of occurrence after controls are applied, multiplied by the expected loss. Residual risk is a reflection of the actual state. As such, the risk level can run the gamut from severe to nonexistent.

Let’s consider the threat of obtaining unauthorized access to protected customer data. A threat source could be a cybercriminal. The vulnerability is that the information system that stores the data is Internet facing. We can safely assume that if no security measures were in place, the criminal would have unfettered access to the data (**inherent risk**). The resulting harm (**impact**) would be reputational damage, cost of responding to the breach, potential lost future revenue, and perhaps regulatory penalties. The security measures in place include data access controls, data encryption, ingress and egress filtering, an intrusion detection system, real-time activity monitoring, and log review. The **residual risk** calculation is based on the likelihood that the criminal (**threat source**) would be able to successfully penetrate the security measures, and if so what the resulting harm would be. In this example, because the stolen or accessed data are encrypted, one could assume that the residual risk would be low (unless, of course, they were also able to access the decryption key). However, depending on the type of business, there still might be an elevated reputation risk associated with a breach.

**FYI: Business Risk Categories**

In a business context, risk is further classified by category, including strategic, financial, operational, personnel, reputational, and regulatory/compliance risk:

- **Strategic** risk relates to adverse business decisions.
- **Financial** (or investment) risk relates to monetary loss.
- **Reputational** risk relates to negative public opinion.
Operational risk relates to loss resulting from inadequate or failed processes or systems.

Personnel risk relates to issues that affect morale, productivity, recruiting, and retention.

Regulatory/compliance risk relates to violations of laws, rules, regulations, or policy.

Risk Assessment Methodologies

Components of a risk assessment methodology include a defined process, a risk model, an assessment approach, and standardized analysis. The benefit of consistently applying a risk assessment methodology is comparable and repeatable results. The three most well-known information security risk assessment methodologies are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed at the CERT Coordination Center at Carnegie Mellon University), FAIR (Factor Analysis of Information Risk), and the NIST Risk Management Framework (RMF). The NIST Risk Management Framework includes both risk assessment and risk management guidance.

NIST Risk Assessment Methodology

Federal regulators and examiners often refer to NIST SP 800-30 and SP 800-39 in their commentary and guidance. The NIST Risk Assessment methodology, as defined in SP 800-30: Guide to Conducting Risk Assessments, is divided into four steps: Prepare for the assessment, conduct the assessment, communicate the results, and maintain the assessment. It is unrealistic that a single methodology would be able to meet the diverse needs of private and public sector organizations. The expectation set forth in NIST SP 800-39 and 800-30 is that each organization will adapt and customize the methodology based on size, complexity, industry sector, regulatory requirements, and threat vector.

In Practice

Information Security Risk Assessment Policy

Synopsis: To assign responsibility for and set parameters for conducting information security risk assessments.

Policy Statement:

- The company must adopt an information security risk assessment methodology to ensure consistent, repeatable, and comparable results.
- Information security risk assessments must have a clearly defined and limited scope. Assessments with a broad scope become difficult and unwieldy in both their execution and the documentation of the results.
- The CISO is charged with developing an information security risk assessment schedule based on the information system’s criticality and information classification level.
In addition to scheduled assessments, information security risk assessments must be conducted prior to the implementation of any significant change in technology, process, or third-party agreement.

The CISO and the business process owner are jointly required to respond to risk assessment results and develop risk reduction strategies and recommendations.

Risk assessment results and recommendations must be presented to executive management.

What Is Risk Management?

*Risk management* is the process of determining an acceptable level of risk (risk appetite and tolerance), calculating the current level of risk (risk assessment), accepting the level of risk (risk acceptance), or taking steps to reduce risk to the acceptable level (risk mitigation). We discussed the first two components in the previous sections.

**Risk Acceptance**

*Risk acceptance* indicates that the organization is willing to accept the level of risk associated with a given activity or process. Generally, but not always, this means that the outcome of the risk assessment is within tolerance. There may be times when the risk level is not within tolerance but the organization will still choose to accept the risk because all other alternatives are unacceptable. Exceptions should always be brought to the attention of management and authorized by either the executive management or the Board of Directors.

**Risk Mitigation**

Risk mitigation implies one of four actions—reducing the risk by implementing one or more countermeasures (risk reduction), sharing the risk with another entity (risk sharing), transferring the risk to another entity (risk transference), modifying or ceasing the risk-causing activity (risk avoidance), or a combination thereof.

*Risk mitigation* is a process of reducing, sharing, transferring, or avoiding risk. *Risk reduction* is accomplished by implementing one or more offensive or defensive controls in order to lower the residual risk. An *offensive control* is designed to reduce or eliminate vulnerability, such as enhanced training or applying a security patch. A *defensive control* is designed to respond to a threat source (for example, a sensor that sends an alert if an intruder is detected). Prior to implementation, risk reduction recommendations should be evaluated in terms of their effectiveness, resource requirements, complexity impact on productivity and performance, potential unintended consequences, and cost. Depending on the situation, risk reduction decisions may be made at the business unit level, by management or by the Board of Directors.
Risk transfer or risk sharing is undertaken when organizations desire and have the means to shift risk liability and responsibility to other organizations. **Risk transfer** shifts the entire risk responsibility or liability from one organization to another organization. This is often accomplished by purchasing insurance. **Risk sharing** shifts a portion of risk responsibility or liability to other organizations. The caveat to this option is that regulations such as GLBA (financial institutions) and HIPAA/HITECH (healthcare organizations) prohibit covered entities from shifting compliance liability.

Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk appetite and tolerance, and a determination has been made not to make an exception. **Risk avoidance** involves taking specific actions to eliminate or significantly modify the process or activities that are the basis for the risk. It is unusual to see this strategy applied to critical systems and processes because both prior investment and opportunity costs need to be considered. However, this strategy may be very appropriate when evaluating new processes, products, services, activities, and relationships.

### In Practice

#### Information Security Risk Response Policy

**Synopsis:** To define information security risk response requirements and authority.

**Policy Statement:**

- The initial results of all risk assessments must be provided to executive management and business process owner within seven days of completion.
- Low risks can be accepted by business process owners.
- Elevated risks and severe risks (or comparable rating) must be responded to within 30 days. Response is the joint responsibility of the business process owner and the CISO. Risk reduction recommendations can include risk acceptance, risk mitigation, risk transfer, risk avoidance, or a combination thereof. Recommendations must be documented and include an applicable level of detail.
- Severe and elevated risks can be accepted by executive management.
- The Board of Directors must be informed of accepted severe risk. At their discretion, they can choose to overrule acceptance.
FYI: Cyber Insurance

Two general categories of risks and potential liabilities are covered by cyber-insurance: first-party risks and third-party risks:

- **First-party risks** are potential costs for loss or damage to the policyholder’s own data, or lost income or business.

- **Third-party risks** include the policyholder’s potential liability to clients or to various governmental or regulatory entities.

- A company’s optimal cyber-security policy would contain coverage for both first- and third-party claims. A 2013 Ponemon Institute Study commissioned by Experian Data Breach Resolution found that of 683 surveys completed by risk management professionals across multiple business sectors that have considered or adopted cyber-insurance, 86% of policies covered notification costs, 73% covered legal defense costs, 64% covered forensics and investigative costs, and 48% covered replacement of lost or damaged equipment. Not everything was always covered, though, as companies said only 30% of policies covered third-party liability, 30% covered communications costs to regulators, and 8% covered brand damages.

FYI: Small Business Note

Policy, governance, and risk management are important regardless of the size of the organization. The challenge for small organizations is who is going to accomplish these tasks. A small (or even a mid-size) business may not have a Board of Directors, C-level officers, or directors. Instead, as illustrated in Table 4.2, tasks are assigned to owners, managers, and outsourced service providers. What does not change regardless of size is the responsibilities of data owners, data custodians, and data users.

**TABLE 4.2 Organizational Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Small Business Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of Directors</td>
<td>Owner(s).</td>
</tr>
<tr>
<td>Executive management</td>
<td>Owner(s) and/or management.</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>A member of the management team whose responsibilities include information security. If</td>
</tr>
<tr>
<td></td>
<td>internal expertise does not exist, external advisors should be engaged.</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>A member of the management team whose responsibilities include evaluating risk. If</td>
</tr>
<tr>
<td></td>
<td>internal expertise does not exist, external advisors should be engaged.</td>
</tr>
<tr>
<td>Compliance Officer</td>
<td>A member of the management team whose responsibilities include ensuring compliance with</td>
</tr>
<tr>
<td></td>
<td>applicable laws and regulations. If internal expertise does not exist, external advisors</td>
</tr>
<tr>
<td></td>
<td>should be engaged.</td>
</tr>
<tr>
<td>Director of IT</td>
<td>IT manager. If internal expertise does not exist, external service providers should be</td>
</tr>
<tr>
<td></td>
<td>engaged.</td>
</tr>
<tr>
<td>Internal audit</td>
<td>If this position is required, it is generally outsourced.</td>
</tr>
</tbody>
</table>
Summary

Information security is not an end unto itself. Information security is a business discipline that exists to support business objectives, add value, and maintain compliance with externally imposed requirements. This type of relationship is known as strategic alignment. Organizational commitment to information security practices should be codified in a written policy. The information security policy is an authoritative document that informs decision making and practices. As such, it should be authorized by the Board of Directors or equivalent body. Derivative documents for specific audiences should be published and distributed. This includes an Acceptable Use Policy and Agreement for users, a third-party version for vendors and service providers, and a synopsis for business partners and clients.

It is essential that information security policies remain relevant and accurate. At a minimum, policies should be reviewed and reauthorized annually. Change drivers are events that modify how a company operates and are a trigger for policy review. Compliance with policy requirements should be assessed and reported to executive management.

An information security audit is a systematic evidence-based evaluation of how well the organization conforms to established criteria. Audits are generally conducted by independent auditors, which implies that the auditor is not responsible for, benefited from, or in any way influenced by the audit target. A capability maturity model (CMM) assessment is an evaluation of process maturity for a given area. In contrast to an audit, the application of a CMM is generally an internal process. Audits and maturity models are good indicators of policy acceptance and integration.

Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The Board of Directors is the authoritative policy making body. Executive management is tasked with providing support and resources. Endorsed by the Board of Directors and executive management, the CISO (or equivalent role) is vested with information security program management responsibility and accountability. The chain of command for the CISO should be devoid of conflict of interest. The CISO should have the authority to communicate directly with the Board of Directors.

Discussion, debate, and thoughtful deliberation result in good decision making. Supporting the CISO should be an Information Security Steering Committee, whose members represent a cross-section of the organization. The steering committee serves in an advisory capacity with particular focus on the alignment of business and security objectives. Distributed throughout the organization are a variety of roles that have information security–related responsibilities. Most notably, data owners are responsible for defining protection requirements, data custodians are responsible for managing the protection mechanisms, and data users are expected to act in accordance with the organization’s requirements and to be stewards of the information in their care.

Three factors influence information security decision making and policy development: guiding principles, regulatory requirements, and risks related to achieving their business objectives. Risk is the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or
Test Your Skills

inaction. Risk tolerance is how much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit. Risk management is the process of determining an acceptable level of risk, identifying the level of risk for a given situation, and determining if the risk should be accepted or mitigated. A risk assessment is used to calculate the level of risk. A number of publically available risk assessment methodologies are available for organizations to use and customize. Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process. Risk mitigation implies that one of four actions (or a combination of actions) will be undertaken: risk reduction, risk sharing, risk transference, or risk avoidance.


---

**MULTIPLE CHOICE QUESTIONS**

1. When an information security program is said to be “strategically aligned,” this indicates that ____________.
   
   A. It supports business objectives  
   B. It adds value  
   C. It maintains compliance with regulatory requirements  
   D. All of the above

2. How often should information security policies be reviewed?
   
   A. Once a year  
   B. Only when a change needs to be made  
   C. At a minimum, once a year and whenever there is a change trigger  
   D. Only as required by law

3. Information security policies should be authorized by ____________.
   
   A. the Board of Directors (or equivalent)  
   B. business unit managers  
   C. legal counsel  
   D. stockholders
4. Which of the following statements best describes policies?
   A. Policies are the implementation of specifications.
   B. Policies are suggested actions or recommendations.
   C. Policies are instructions.
   D. Policies are the directives that codify organizational requirements.

5. Which of the following statements best represents the most compelling reason to have an employee version of the comprehensive information security policy?
   A. Sections of the comprehensive policy may not be applicable to all employees.
   B. The comprehensive policy may include unknown acronyms.
   C. The comprehensive document may contain confidential information.
   D. The more understandable and relevant a policy is, the more likely users will positively respond to it.

6. Which of the following is a common element of all federal information security regulations?
   A. Covered entities must have a written information security policy.
   B. Covered entities must use federally mandated technology.
   C. Covered entities must self-report compliance.
   D. Covered entities must notify law enforcement if there is a policy violation.

7. Organizations that choose to adopt the ISO 27002:2013 framework must ________________.
   A. use every policy, standard, and guideline recommended
   B. create policies for every security domain
   C. evaluate the applicability and customize as appropriate
   D. register with the ISO

8. Evidence-based techniques used by information security auditors include which of the following elements?
   A. Structured interviews, observation, financial analysis, and documentation sampling
   B. Structured interviews, observation, review of practices, and documentation sampling
   C. Structured interviews, customer service surveys, review of practices, and documentation sampling
   D. Casual conversations, observation, review of practices, and documentation sampling
9. Which of the following statements best describes independence in the context of auditing?
   A. The auditor is not an employee of the company.
   B. The auditor is certified to conduct audits.
   C. The auditor is not responsible for, benefited from, or in any way influenced by the audit target.
   D. Each auditor presents his or her own opinion.

10. Which of the following states is not included in a CMM?
   A. Average
   B. Optimized
   C. Ad hoc
   D. Managed

11. Which of the following activities is not considered a governance activity?
   A. Managing
   B. Influencing
   C. Evaluating
   D. Purchasing

12. To avoid conflict of interest, the CISO could report to which of the following individuals?
   A. The Chief Information Officer (CIO)
   B. The Chief Technology Officer (CTO)
   C. The Chief Financial Officer (CFO)
   D. The Chief Compliance Officer (CCO)

13. Which of the following statements best describes the role of the Information Security Steering Committee?
   A. The committee authorizes policy.
   B. The committee serves in an advisory capacity.
   C. The committee approves the InfoSec budget.
   D. None of the above.

14. Defining protection requirements is the responsibility of _____________.
   A. the ISO
   B. the data custodian
   C. data owners
   D. the Compliance Officer
15. Designating an individual or team to coordinate or manage information security is required by __________.
   A. GLBA
   B. MA CMR 17 301
   C. PCI DSS
   D. All of the above

16. Which of the following terms best describes the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction?
   A. Threat
   B. Risk
   C. Vulnerability
   D. Impact

17. Inherent risk is the state before _________________.
   A. an assessment has been conducted
   B. security measures have been implemented
   C. the risk has been accepted
   D. None of the above

18. Which of the following terms best describes the natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact?
   A. Risk
   B. Threat source
   C. Threat
   D. Vulnerability

19. Which of the following terms best describes a disgruntled employee with intent to do harm?
   A. Risk
   B. Threat source
   C. Threat
   D. Vulnerability
20. Which if the following activities is not considered an element of risk management?
   A. The process of determining an acceptable level of risk
   B. Assessing the current level of risk for a given situation
   C. Accepting the risk
   D. Installing risk-mitigation safeguards

21. How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit is known as ________.
   A. risk acceptance
   B. risk tolerance
   C. risk mitigation
   D. risk avoidance

22. Which of the following statements best describes a vulnerability?
   A. A vulnerability is a weakness that could be exploited by a threat source.
   B. A vulnerability is a weakness that can never be fixed.
   C. A vulnerability is a weakness that can only be identified by testing.
   D. A vulnerability is a weakness that must be addressed regardless of the cost.

23. A control is a security measure that is designed to ________ a threat source.
   A. detect
   B. deter
   C. prevent
   D. All of the above

24. Which of the following is not a risk-mitigation action?
   A. Risk acceptance
   B. Risk sharing or transference
   C. Risk reduction
   D. Risk avoidance

25. Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?
   A. Inherent risk
   B. Expected risk
   C. Residual risk
   D. Accepted risk
26. Which of the following risk types best describes an example of insurance?
   A. Risk avoidance
   B. Risk transfer
   C. Risk acknowledgement
   D. Risk acceptance

27. Which of the following risk types relates to negative public opinion?
   A. Operational risk
   B. Financial risk
   C. Reputation risk
   D. Strategic risk

28. Compliance risk as it relates to federal and state regulations can never be ____________.
   A. avoided
   B. transferred
   C. accepted
   D. None of the above

29. Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?
   A. They must have different policies for each regulation.
   B. They must have multiple ISOs.
   C. They must ensure that their information security program includes all applicable requirements.
   D. They must choose the one regulation that takes precedence.

30. Which of the following terms best describes “duty of care” as applied to corporate directors and executive officers?
   A. It’s a legal obligation.
   B. It’s an outdated requirement.
   C. It’s ignored by most organizations.
   D. It’s a factor only when there is a loss greater than $1,000.
EXERCISES

EXERCISE 4.1: Understanding ISO 27002:2005

The introduction to ISO 27002:2005 includes this statement: “This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required.”

1. Explain how this statement relates to the concept of strategic alignment.

2. The risk assessment domain was included in the ISO 27002:2005 edition and then removed in ISO 27002:2013. Why do you think they made this change?

3. What are the major topics of ISO 27005?

EXERCISE 4.2: Understanding Policy Development and Authorization

Three entrepreneurs got together and created a website design hosting company. They will be creating websites and social media sites for their customers, from simple “Hello World” pages to full-fledged e-commerce solutions. One entrepreneur is the technical guru, the second is the marketing genius, and the third is in charge of finances. They are equal partners. The entrepreneurs also have five web developers working for them as independent contractors on a per-project basis. Customers are requesting a copy of their security policies.

1. Explain the criteria they should use to develop their policies. Who should authorize the policies?

2. Should the policies apply to the independent contractors? Why or why not?

3. What type of documentation should they provide their customers?

EXERCISE 4.3: Understanding Information Security Officers

1. ISOs are in high demand. Using online job hunting sites (such as Monster.com, Dice.com, and TheLadders.com), research available positions in your geographic area.

2. Is there a common theme in the job descriptions?

3. What type of certifications, education, and experience are employers seeking?

EXERCISE 4.4: Understanding Risk Terms and Definitions

1. Define each of the following terms: inherent risk, threat, threat source, vulnerability, likelihood, impact, and residual risk.

2. Provide examples of security measures designed to (a) deter a threat source, (b) prevent a threat source from being successful, and (c) detect a threat source.

3. Explain risk avoidance and why that option is generally not chosen.
EXERCISE 4.5: Understanding Insurance

1. What is cyber-insurance and what does it generally cover?
2. Why would an organization purchase cyber-insurance?
3. What is the difference between first-party coverage and third-party coverage?

PROJECTS

PROJECT 4.1: Analyzing a Written Policy

1. Many organizations rely on institutional knowledge rather than written policy. Why do you think all major information security regulations require a written information security policy? Do you agree? Explain your opinion.

2. We are going to test the conventional wisdom that policy should be documented conducting an experiment.
   a. Write down or print out these three simple policy statements. Or, if you would prefer, create your own policy statements.

      The Board of Directors must authorize the Information Security Policy.
      An annual review of the Information Security Policy must be conducted.
      The CISO is responsible for managing the review process.

   b. Enlist four subjects for your experiment.

      Give two of the subjects the written policy. Ask them to read document. Have them keep the paper.

      Read the policy to the two other subjects. Do not give them a written copy.

   c. Within 24 hours, contact each subject and ask them to recall as much of the policy as possible. If they ask, let the first two subjects know that they can consult the document you gave them. Document your findings. Does the outcome support your answer to Question 1?

PROJECT 4.2: Analyzing Information Security Management

1. Does your school or workplace have a CISO or an equivalent position? Who does the CISO (or equivalent) report to? Does he or she have any direct reports? Is this person viewed as a security champion? Is he or she accessible to the user community?

2. It is important that CISOs stay current with security best practices, regulations, and peer experiences. Research and recommend (at least three) networking and educational resources.

3. If you were tasked with selecting an Information Security Steering Committee at your school or workplace to advise the CISO (or equivalent), who would you choose and why?
PROJECT 4.3: Using Risk Assessment Methodologies

The three most well-known information security risk assessment methodologies are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed at the CERT Coordination Center at Carnegie Mellon University), FAIR (Factor Analysis of Information Risk), and the NIST Risk Management Framework (RMF).

1. Research and write a description of each (including pros and cons).
2. Are they in the public domain, or is there a licensing cost?
3. Is training available?

Case Study

Determining the Likelihood and Impact of Occurrence

One of the most challenging aspects of a risk assessment is determining the likelihood of occurrence and impact. NIST SP 800-30 defines the likelihood of occurrence as follows: A weighted risk factor based on an analysis of the probability that a given threat source is capable of exploiting a given vulnerability (or set of vulnerabilities). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary intent; (ii) adversary capability; and (iii) adversary targeting. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors. Organizations typically employ a three-step process to determine the overall likelihood of threat events:

- Organizations assess the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events).
- Organizations assess the likelihood that the threat events, once initiated or occurring, will result in adverse impacts or harm to organizational operations and assets, individuals, other organizations, or the nation.
- Organizations assess the overall likelihood as a combination of likelihood of initiation/occurrence and likelihood of resulting in adverse impact.

Identify two threat sources—one adversarial and one non-adversarial—that could exploit a vulnerability at your school or workplace and would result in disruption of service. An adversarial event is the intentional exploitation of a vulnerability by criminal groups, terrorists, bot-net operators, or disgruntled employees. A non-adversarial event is the accidental exploit of a vulnerability, such as an undocumented process, a severe storm, or accidental or unintentional behavior.

1. For each (using your best judgment), answer the following questions:
   a) What is the threat?
   b) What is the threat source?
   c) Is the source adversarial or non-adversarial?
d) What vulnerability could be exploited?

e) How likely is the threat source to be successful and why?

f) If the threat source is successful, what is the extent of the damage caused?

2. Risk assessments are rarely conducted by one individual working alone. If you were hosting a workshop to answer the preceding questions, who would you invite and why?

References

Regulations Cited


Other References


Symbols

201 CMR 17: Standards for the Protection of Personal Information of Residents of the Commonwealth, 15

27002:2013 series (ISO/IEC), 74-75
  access controls, 265
  asset management, 125
  business continuity, 371
  communications, 219
  cryptography, 301
  domains, 75-80
  GLBA requirements, 416
  human resources, 157
  information security policies guidance, 93
  ISADM, 300
  operations, 219
  origins, 74
  physical/environmental security, 189
  regulation compliance, 409, 443
  security incidents, 329

A

ABCP (Associate Business Continuity Professional), 384

Acceptable Use Policy, 568
  agreement, 170-171, 568
  applications, 571
  authentication, 570
  data protection, 569-570
distribution, 568
incident detection/reporting, 573
Internet, 572
messaging, 571
mobile devices, 572
password controls, 570
remote access, 573
acceptance (risk), 109
access controls, 77
authentication, 265
   factors, 266
      Google 2-step verification, 269
   inherence, 269
   knowledge-based, 267
   possession, 268
authorization, 265, 270
   discretionary, 271
   mandatory, 270
   policy statement, 271
   role-based, 271
   rule-based, 271
defined, 265
e-mail, 239
HIPAA compliance, 449-450, 458-459
identification schemes, 265
infrastructure, 272
   layered border security, 273-277
   network segmentation, 272-273
ISO 27002:2013 series, 265
least privilege, 266
lists, 270
need-to-know, 266
NIST, 265
objects, 265
PCI DSS measures, 492-493
physical security, 192
   documents, 194-195
   entry, 192, 536
   facilities, 455
insider theft, 195
secure areas, 194
workspaces, 193
remote, 277
   authentication, 278
   authorization, 279
NIST, 278
   policy statement, 279-280
   portals, 278
teleworking, 280-281, 298
VPNs, 278
resource websites, 297
sample policy, 546
   administrative/privileged accounts, 551
   authentication, 547
   authorization, 548
   border devices, 548-549
   goals/objectives, 546
   index, 546
   lead author, 553
   network segmentation, 548
   remote access, 549-550
   supporting resources/source material, 552
   system, monitoring, 552
teleworking, 550
users, 551
security posture, 266
small businesses, 286
subjects, 265
user, 282
   administrative accounts, 283
   importance, 282
   monitoring, 284-285
   policy statement, 282
Yahoo! password compromise, 267, 297
accidents, 371
accountability, 71
account data (payment card industry), 484
accounting, 71
acquisition/development phase (SDLC), 302
Active Directory domain controller recovery procedure, 389
active voice, 51-52
ADA (Americans with Disabilities Act), 163, 186
adaptability, 11-12
ADCR (Account Data Compromise Recovery), 503
addresses
  implementation specifications, 446
  IP, 274
  IPv4, 141
  MAC, 141
  whitelists/blacklists, 275
administrators
  accounts
    controls, 283
    sample policy, 551
  safeguards, 413
standards (HIPAA), 446
  assigned security responsibility, 448
  business associate contracts and other arrangements, 453
  contingency plans, 451-452
  evaluation, 452-453
  information access management, 449-450
  security awareness and training, 450-451
  security incident procedures, 451
  security management process, 447-448
  summary, 454
  workforce security, 448-449
adapting policies, 19-20
advanced persistent threats (APTs), 230
Advanced Research Project Agency (ARPA), 237
Aeneas Internet and Telephone F4 tornado, 373
AES (Advanced Encryption Standard), 312
Affinity Health Plan HIPAA photocopier breach, 467
AICPA (American Institute of CPAs), 246
Allen, Julia, 122
alpha phase (software), 304
Americans with Disabilities Act (ADA), 163, 186
analyzing logs, 243
ancient policies, 4-5
antivirus software, 234
“A Plain English Handbook: How to create clear SEC disclosure documents” website, 48
apparent data files, 200
applications. See software
Approved Scanning Vendors (ASVs), 501
APTs (advanced persistent threats), 230
ARPA (Advanced Research Project Agency), 237
ARPANET, 237
assessing. See evaluating
assessors, 97
asset management, 77
classifications
  Bell-Lapadula model, 128
  Biba model, 128
  declassification, 135
defined, 128
  Freedom of Information Act, 129
  government, 129-131
  handling standards, 136-139
  labeling, 136, 139
  lifecycle, 128
  military, 128
  national security information, 131-133
  non-public personal information, 134
  policy statement, 135
  private sector, 128, 134
  reclassification, 136
  small business data example, 142-143
  defined, 8, 125
descriptions, 140-142
  hardware, 141
inventory, 139
  asset descriptions, 140-142
  choosing items to include, 139
  controlling entities, 142
  disposal/destruction of assets, 142
  hardware assets, 140-141
  logical addresses, 141
  policy statement, 142
  software assets, 140-142
  unique identifiers, 140
ISO 27002:2013 guidance, 125
NIST guidance, 125
ownership, 126-127
sample policy, 527
  goals/objectives, 527
  index, 527
  information classification, 528
  information ownership, 527
  inventory, 529
  lead author, 529
  policy statement, 142
  software, 140-142
assigned security responsibility standard (HIPAA), 448
Associate Business Continuity Professional (ABCP), 384
assurance, 71, 419
ASVs (Approved Scanning Vendors), 501
asymmetric keys, 313, 327
attacks. See incidents
audience, 36
audits
  business continuity, 393-394
  CISA (Certified Information Security Auditor), 98
  financial institutions testing, 419
  HIPAA technical compliance, 459
  information security policies, 98
  reports, 98
  service providers, 246

authentication
  Acceptable Use Policy, 570
  access controls, 265
    factors, 266
    Google 2-step verification, 269
    inherence, 269
    knowledge-based, 267
    possession, 268
  broken, 310
  defined, 71
  HIPAA technical compliance, 460
  Internet banking, 427
  remote access, 278
  sample policy, 547
  server logs, 244

authorization
  access controls, 265, 270
    discretionary, 271
    mandatory, 270
    policy statement, 271
    role-based, 271
    rule-based, 271
  CDLC implementation phase, 303
  defined, 71
  HIPAA Workforce Security, 449
  incident response, 559
  information security policies, 96, 100
  physical access, 192
  remote access, 279
  sample policy, 548, 551
  SOPs, documenting, 220

availability, 69
  defined, 69
  distributed denial of service (DDoS) attacks, 70
  government data classification, 130
  SLAs, 70
  threats, 70

awareness (security), 174
background checks, 161-162
  bankruptcies, 163
  consent, 162
  credit history, 164
  criminal history, 163-164
  educational, 163-164
  employee rights, 162
  employment, 164
  financial history, 163
  licenses/certifications, 164
  motor vehicle records, 163
  policy statement, 164
  Sarbanes-Oxley Act, 162-164
  social media, 162
  websites, 186
  workers’ compensation history, 163
backups (data), 235-236
Bangladesh building collapse website, 29
Bank Holding Company Act of 1956, 409
Banking Act of 1933, 409
bankruptcy protection, 163
Bank Service Company Act (BSCA), 420
baselines, 34
BCP (business continuity plan), 380
  policy statement, 381
  responsibilities, 381
    Business Continuity Team (BCTs), 381
    governance, 381
    policy statement, 383
    tactical, 382
BCTs (Business Continuity Teams), 381
Bejtlich, Richard’s blog, 122
Bell-Lapadula classification model, 128
benefits data protection, 166
beta phase (software), 305
BIA (business impact assessment), 378-379
Biba classification model, 128
biometrics, 269
black box assurance tests, 419
blacklists, 241, 275
blackouts, 198
blended threats, 234
Blue Teaming, 276
Board of Directors. See executive management
border devices
  administration/management, 275
  content filtering, 275
  firewalls, 273-274
  IDSs/IPSs, 274-275
  penetration testing, 276
  policy statement, 276-277
  sample policy, 548-549
Boston Marathon Bombings websites, 407
botnets, 70, 232
bots, 232
breaches
  2013 investigations report, 514
  data cards with malware, 491
  Global Payments PCI data breach, 503
  HIPAA notifications, 468
    breach definition, 468
    requirements, 469
    websites, 481
    reporting/notifications
      HIPAA, 468-469
      sample policy, 560
broken authentication, 310
brownouts, 198
browser-based data, 200
BSCA (Bank Service Company Act), 420
Bush, President, HSPD-7, 373
business associates contracts and other arrangements standard (HIPAA), 444, 453, 461-462
business as usual (PCI DSS), 487
business continuity, 80
  audits, 393-394
certifications, 384
disaster recovery, 388
  Active Directory domain controller example, 389
  communications, 389
  facilities, 389
  infrastructure, 389
  mainframe, 389
  network, 389
  policy statement, 391
procedures, 389
resource websites, 407
service provider dependencies, 390
disaster response plans, 384
  command and control centers, 385
  communication, 385
  organizational structure, 384
  policy statement, 386-387
relocation strategies, 385-386
resource websites, 406
  small businesses, 394
education/training, 384
emergency preparedness
  disasters, 371-372
  policy statement, 374
  regulatory requirements, 372-373
resilience, 372
  Tennessee F4 tornado example, 373
ISO/IEC 27002:2013, 371
maintenance, 393-394, 567
management, 564-565
NIST, 371
operational contingency plans, 387-388
  plans, 380
    policy statement, 381
    sample policy, 564
resource websites, 406
responsibilities, 381
  Business Continuity Teams (BCTs), 381
governance, 381
  policy statement, 383
tactical, 382
resumption phase, 391
risk management, 374
  impact assessment, 378-380
  risk assessments, 376-377
  threat assessments, 375
sample policy, 562
  BIA, 563
  continuity testing/maintenance, 567
disaster recovery, 566
  emergency preparedness, 563
  emergency response, 565
goals/objectives, 562
index, 562
lead author, 567
management, 564-565
  operational contingency plan, 565
  plan, 564
  supporting resources/source material, 567
testing
  importance, 392
  methodologies, 392-393
  policy statement, 394
  sample policy, 567
Business Continuity Teams (BCTs), 381
business risk categories, 107

C

C&A (certification and accreditation), 303
CA (Certification Authority), 313
Caesar Cipher, 311
California Security Breach Information Act, 15, 30, 350
candidate data, 159-160
capability maturity model (CMM), 98-99, 122-123
cardholder data protection. See PCI DSS
CBCP (Certified Business Continuity Professional), 384
C&C (command and control server), 231
CCFP (Certified Cyber Forensics Professional), 343
certificates (digital)
  compromises, 315
  defined, 313
  resource websites, 327
  viewing, 314
certificates of destruction, 202
certification and accreditation (C&A), 303
Certification Authority (CA), 313
certification background checks, 164
Certified Business Continuity Professional (CBCP), 384
Certified Cyber Forensics Professional (CCFP), 343
Certified Functional Continuity Professional (CFCP), 384
Certified Information Security Auditor (CISA), 98
CERT Insider Threat Blog entry, 195
CFCP (Certified Functional Continuity Professional), 384
chain of custody, 202, 343-344
championing policies, 19
change control, 225
  change management processes, 225
  communicating changes, 227
  documentation, 227
  emergency situations, 227
  implementing changes, 227
  importance, 225
  management processes, 225
  monitoring, 227
  patches, 228-229
plans, 226
policy statement, 228
resource website, 262
RFCs, 226
sample policy, 541
change drivers, 97, 123
Chief Information Security Officer (CISO), 101-102, 524
CIA (confidentiality, integrity, availability) triad, 65-66
  availability, 69-70
  confidentiality, 66-68
cryptography
  Caesar Cipher, 311
cipher text, 311
decryption, 311
  defined, 310
digital signatures, 311
  encryption, 311-312
  hashing, 311
  keys. See keys
  message integrity, 311
  policy statement, 315
  small businesses, 316
  high potential impact, 129
  integrity, 68-69
  low potential impact, 129
  moderate potential impact, 129
  responsibility, 72
cipher text, 311
CISA (Certified Information Security Auditor), 98
CISO (Chief Information Security Officer), 101-102
Clarity Index, 52
Clarke, Richard, 13
class A fires, 199
class B fires, 199
class C fires, 199
class D fires, 199
classifications
- assets, 528
- Bell-Lapadula model, 128
- Biba model, 128
- corporate cultures, 6
- declassification, 135
- defined, 128
- Freedom of Information Act, 129
- government, 129-131
- handling standards, 136-138
  - policy statement, 139
  - sample matrix, 137
- incidents, 333-335, 558
- labeling, 136, 139
- lifecycle, 128
- military, 128
- national security information
  - derivative classification, 133
  - Executive Order 13536, 131
  - listing of classifications, 132-133
  - original classification, 133
- non-public personal information, 134
- policy statement, 135
- private sector, 128
- reclassification, 136
- small business data example, 142-143
- workspaces, 193, 536

**clear desks/screens, 194-195, 537**

**client nodes, 313**

**client synopsis, 95**

**Clinton, President, PDD-63, 372**

**closure (incidents), 336**

**cloud storage, 236**

**CMM (capability maturity model), 98-99, 122-123**

**code (secure)**
- broken authentication, 310
- defined, 306
- dynamic data verification, 309
- injection, 308
- input validation, 308
- output validation, 309
- OWASP, 307-308
- policy statement, 310
- SAMM, 307
- session management, 310

**cognitive passwords, 267**

**cold sites, 386**

**command and control centers (disaster response plans), 385**

**command and control server (C&C), 231**

**commercial off-the-shelf software (COTS)**
- policy statement, 306
- releases, 304
- SDLC, 304
- testing environments, 305-306
- updates, 305

**communication, 79**
- changes, 227, 262
- customer communication business impact assessment, 379
- data breach notifications, 353
- disasters
  - recovery, 389
  - response plans, 385
- email
  - access, controlling, 239
  - ARPANET, 237
  - encryption, 238
  - hoaxes, 240
  - IMAP, 237
  - malware, 238
  - metadata, 238
  - policy statement, 241
  - POP3, 237
  - servers, 240-241
  - SMTP, 237
  - user errors, 240
communications, 140

facilities, 538

incidents, 336, 339

Internet, 274

ISO 27002:2013 series guidance, 219

patches, 228-229

sample policy, 540

change control, 541

data replication, 543

email, 543

goals/objectives, 540

index, 540

lead author, 545

logs, 543

malware, 542

patch management, 542

service providers, 544

supporting resources/source material, 545

SOPs, 219

developing, 220

documenting, 220

formats, 220-223

policy statement, 225

writing resource, 224

transmission security, 460

compliance, 80

culture, 19

officers, 103

Omnibus Rule, 464-465, 480

risks, 108, 415

components (policy documents), 38

enforcement clauses, 45

exceptions, 44

exemptions, 44

goals/objectives, 42

headings, 42

introductions, 39-41

Policy Definition section, 47

statements, 43

version control, 38-39

computer equipment, 140

confidentiality, 66-67, 132-134

agreements, 170

cybercrimes, 68

government data classification, 130

hacktivism, 68

Manning WikiLeaks example, 67

protecting, 67

confidentiality, integrity, availability. See CIA triad

consolidated policies, 37

Constitution of the United States of America, 5

consumer information, 15, 413

containment (incidents), 336

content filtering, 275

contingency plans, 380, 451-452

continuity planning, 374

contracts (service providers), 247

corporate account takeover, 425, 428, 440

corporate cultures

classifications, 6

defined, 5

honoring the public trust, 7

corporate identity theft, 424-425

corporate account takeovers, 428, 440

GLBA Interagency Guidelines Supplement A requirements, 425-426

Identity Theft Data Clearinghouse, 426

Internet banking safeguards, 427

corporate officers. See executive management
correlation (logs), 243

COTS (commercial off-the-shelf software)

policy statement, 306

releases, 304

SDLC, 304

testing environments, 305-306

updates, 305

covered entities (HIPAA), 444, 461-462

CPTED (Crime Prevention Through Environmental Design), 191
credit cards. See also PCI DSS
  background checks, 164
  elements, 484
  fraud, 483
  growth website, 514
  primary account numbers, 484
  skimming, 493-494, 514

criminal history background checks, 164
criminal records, 163
critical infrastructure sectors, 2-3
cryptography, 78
  asymmetric, 327
  Caesar Cipher, 311
  cipher text, 311
decryption, 311
defined, 310
digital signatures, 311
encryption, 311
  AES, 312
  email, 327
  importance, 312
  regulatory requirements, 312
  resource websites, 327
hashing, 311
keys, 311-312
  asymmetric, 313
  best practices, 314-315
  keyspace, 312
  NIST, 314
  PKI (Public Key Infrastructure), 313, 327
  policy statement, 315
  sample policy, 556
  symmetric, 313
message integrity, 311
NIST, 301
PKI, 313, 327
small businesses, 316

customers
  communication business impact assessment, 379
  information system, 413
cyber, 13
cyber attack liability website, 123
cybercrimes, 68
cyber-insurance, 111, 123
cybersecurity, 111, 123
cryptography, 301

data
  apparent files, 200
  at rest, 459
  availability, 69-70
  backups, 235-236
  breach notifications, 345-346, 560
    2013 investigations report, 514
    chronology, 346
    federal agencies, 349
    federal law, 347
    GLBA, 347-348
    HIPAA/HITECH, 348-349
    New Hampshire law, 352
    policy statement, 352
    public relations, 353
    regulations, 345
    resource websites, 368-369
    small businesses, 353
    state laws, 350-351
    success, 351-352
    Veterans Administration, 349-350
  browser-based, 200
caches, 200
cardholder protection. See PCI DSS
centers, 190, 538
classifications
  Bell-Lapadula model, 128
  Biba model, 128
declassification, 135
  defined, 128
Freedom of Information Act, 129
government, 129-131
handling standards, 136-139
labeling, 136, 139
lifecycle, 128
military, 128
national security information, 131-133
non-public personal information, 134
policy statement, 135
private sector, 128, 134
reclassification, 136
small business example, 142-143
cloud storage, 236
cryptography
  Caesar Cipher, 311
cipher text, 311
decryption, 311
defined, 310
digital signatures, 311
encryption, 311-312
hashing, 311
keys, 311
  keys. See keys
message integrity, 311
policy statement, 315
small businesses, 316
custodians, 104
de-identification, 306
deleting from drives, 201
destruction, 201
dummy, 306
dynamic data verification, 309
employee payroll/benefits protection, 166
hidden files, 200
in motion, 460
integrity, 69
job candidates, 159-160
logs
  analyzing, 243
  authentication server, 244
  firewall, 243
  inclusion selections, 242
  policy statement, 244
  prioritization, 242
  review regulations, 243
  sample policy, 543
  syslogs, 242
  user access, monitoring, 284-285
  web server, 244
metadata, 200
owners, 103, 126
replication, 235-236, 543
temporary files, 200
users, 104
web caches, 200
Data Compromise Recovery Solution (DCRS), 503
DCRS (Data Compromise Recovery Solution), 503
DDoS (distributed denial of service) attacks, 70, 91, 331-332
debit/credit card fraud, 483
decision states (IDSs/IPSs), 275
decryption, 311
default allow security posture, 266
default deny security posture, 266
defense in depth, 233
defensive controls, 109
definition sections, 53
degaussing, 201
de-identification, 306
deleting data
  before equipment disposal, 200
  from drives, 201
delivery business functions, 385
Department of Health and Human Services
HIPAA security series website, 518
Department of Homeland Security
U.S. Citizenship and Immigration Services
Form I-9 Employment Eligibility Verification, 166
“What Is Critical Infrastructure?” website, 29
derivative classification, 133
designated incident handlers (DIHs), 338
destruction (equipment), 201
detection control, 233, 336
development, 17-18
  implementation/maintenance, 555
SDLC, 302
  development/acquisition phase, 302
disposal, 303
  implementation phase, 303, 555
  initiation phase, 302
  operations/maintenance phase, 303, 555
  policy statement, 304
  sample policy, 554
secure code
  broken authentication, 310
defined, 306
dynamic data verification, 309
injection, 308
input validation, 308
output validation, 309
OWASP, 307-308
policy statement, 310
SAMM, 307
  session management, 310
software, 304
  releases, 304
  sample policy, 555
  updates, 305
SOPs, 220
  formats, 220-223
  policy statement, 225
writing resource, 224
testing environments, 305-306
device and media controls standard (HIPAA compliance), 456-457
digital certificates
  compromises, 315
defined, 313
  resource websites, 327
  viewing, 314
digital non-public personally identifiable information (NPPI), 15-16
digital signatures, 311
DIHs (designated incident handlers), 338
Disaster Recovery Institute website, 519
Disasters, 371-372
  operational contingency plans, 387-388
recovery, 388
  Active Directory domain controller example, 389
  communications, 389
  facilities, 389
  infrastructure, 389
  mainframe, 389
  network, 389
  policy statement, 391
  procedures, 389
  resource websites, 407
  sample policy, 566
  service provider dependencies, 390
response plans, 384
  command and control centers, 385
communication, 385
  organizational structure, 384
  policy statement, 386-387
  relocation strategies, 385-386
  resource websites, 406
  small businesses, 394
  resumption phase, 391
discretionary access controls (DACs), 271

disgruntled ex-network administrator termination example, 169

disk wiping, 201

disposal (equipment), 200, 303
  chain of custody, 202
  data deletion, 200
  deleting data from drives, 201
  physical destruction, 201
  policy statement, 203
  sample policy, 539
  unscrubbed hard drives, 202

disseminating policies, 19

distributed denial of service. See DDoS attacks

distributed governance model, 101
  Chief Information Security Officer, 101-102
  Information Security Officer, 101
  Information Security Steering Committee, 102-103

DMZs, 272

documentation
  changes, 227
  controls, 194-195
  HIPAA policies and procedures, 463-464
  incidents, 336, 341
  plain language, 63
  SOPs, 220

documents (policy)
  components, 38
    enforcement clauses, 45
    exceptions, 44
    exemptions, 44
    goals/objectives, 42
    headings, 42
    introductions, 39-41
    Policy Definition section, 47
    statements, 43
    version control, 38-39
  definition sections, 53
  enforcement clauses, 53
  formats, 36-38
  plain language, 48
    active/passive voice, 51-52
    Clarity Index, 52
    fisheries example, 49
    guidelines, 50-51
    PLAIN, 50-51, 63
  “A Plain English Handbook: How to create clear SEC disclosure documents,” 48
  Plain Language Movement, 49
  Plain Writing Act, 49, 62
  reference websites, 63
  SOP development, 220
  styles, 48

domain names, 141
Do-Not-Track Online Act of 2013, 232
DoS attacks, 241
DPPA (Drivers Privacy Protection Act), 163, 186
DRI (Disaster Recovery Institute) website, 384, 519
dual control administrative accounts, 283
due care, 247
due diligence, 245-246
dummy data, 306
duty of care, 97, 122
dynamic data verification, 309

education, 174
  background checks, 164
  business continuity management, 384
  records, 163
EFTA (Electronic Fund Transfer Act), 483
egress network traffic, 274
electronic monitoring, 532
electronic protected health information (ePHI), 444

email
Acceptable Use Policy, 571
ARPANET, 237
cryptogram, 238, 327
policy statement, 241
risks
access, controlling, 239
hoaxes, 240
IMAP, 237
malware, 238
metadata, 238
POP3, 237
SMTP, 237
user errors, 240
sample policy, 543
servers, 240-241

emergency preparations
disasters, 371-372
policy statement, 374
regulatory requirements, 372-373
resilience, 372
sample policy, 563
Tennessee F4 tornado example, 373

emergency response plans, 384, 565
command and control centers, 385
communication, 385
operational contingency plans, 387-388
organizational structure, 384
policy statement, 386-387
recovery, 388

Active Directory domain controller example, 389
communications, 389
facilities, 389
infrastructure, 389
mainframe, 389
network, 389

employees
agreements, 170-171, 533
background checks
bankruptcies, 163
consent, 162
credit history, 164
criminal, 163-164
educational, 163-164
employment, 164
financial history, 163
licenses/certifications, 164
motor vehicle records, 163
right to privacy, 162
social media, 162
workers’ compensation history, 163
electronic monitoring, 532
incident management, 337-340
information security training, 533
lifecycle, 157-158, 185
onboarding, 165-166
orientations, 167-168
recruitment, 158
candidate data, 159-160
government clearances, 165
interviews, 160
job postings, 159
policy statement, 161
prospective employees, screening, 161-164, 186
risk, 108
screenings, 531
security clearances, 185
security education, training, and awareness model, 174
   HIPAA, 173
      importance, 172
      policy statement, 175
small businesses, 175
termination, 168-169
   disgruntled ex-network administrator example, 169
      policy statement, 169
      sample policy, 532
      websites, 186
user provisioning, 166-167
**enclave networks, 272**
**encryption**
   AES, 312
   defined, 311
   email, 238, 327
   importance, 312
   ransomware, 232
   regulatory requirements, 312
   resource websites, 327
   small businesses, 316
**endorsement, 9**
**energy. See power**
**Energy Star, 197, 215**
**enforcement, 12**
   clauses, 45, 53
**HIPAA**
   proactive, 467
      State Attorneys General authority, 466
      violations, 466-467
      websites, 480
**HITECH Act**
   proactive, 467
      State Attorneys General authority, 466
      violations, 466-467
      websites, 480
**PCI DSS compliance, 503-504**
**entry authorization, 192**
**environmental disasters, 371**
**environmental security, 189**
   access controls, 192
      documents, 194-195
      entry authorization, 192
      insider theft, 195
      secure areas, 194
      workspaces, 193
**CPTED, 191**
equipment, 196
   chain of custody, 202
   disposal, 200-203
   fire prevention controls, 198-199
   power, 196-199, 215
   resources, 216
   theft, 203-205
facilities, 190
   locations, 190
   perimeters, 191
   resources, 216
**HIPAA compliance**
   device and media controls, 456-457
   facility access control, 455
   summary, 457
   workstation security, 456
   workstation use, 456
**ISO 27002:2013 series guidelines, 189**
safeguards, 413
   sample policy, 535
   clear desk/clear screen, 537
   data centers/communications facilities, 538
   entry controls, 536
   equipment disposal, 539
   goals/objectives, 535
   index, 535
   lead author, 539
   mobile devices/media, 539
physical perimeter, 536
power consumption, 537
secure areas, 537
supporting resources/source material, 539
workspace classification, 536
threats, 375
ePHI (electronic protected health information), 444
equipment, 196
border devices, 548-549
chain of custody, 202
device and media controls standard (HIPAA compliance), 456-457
disposal, 200
data deletion, 200
deleting data from drives, 201
physical destruction, 201
policy statement, 203
sample policy, 539
unscrubbed hard drives, 202
fire prevention controls, 198-199
mobile devices/media, 539
passwords, 286
power, 196, 215
consumption, 196-198
fluctuations, 197-198
policy statement, 199
resources, 216
theft, 203-205
eradicating incidents, 336
Ethernet, 273
Euronet processing system data breach, 491
evacuation plans, 385
evaluating
business continuity
impact, 378-380
risks, 376-377
threats, 375
financial institution testing, 419
HIPAA evaluation standards, 452-453
information security policies, 97-100
audits, 98
capability maturity model, 98-99
independent assessors, 97
PCI DSS compliance, 500
fines/penalties, 503-504
process, 500
report, 501
SAQ, 502
websites, 514
risk
business risk categories, 107
controls, 107
financial institutions, 415-416
HIPAA, 447
impact, 107
information security, 106-107
methodologies, 108
NIST methodology, 108
policy statement, 108
residual risk, 107
sample policy, 525
threats, 106-107
vulnerabilities, 107
threats, 415
evidence handling (incidents), 336
chain of custody, 343-344
documentation, 341
evidence storage/retention, 344
forensics, 342-343
law enforcement cooperation, 341-342
policy statement, 345
resource websites, 368-369
sample policy, 560
exceptions, 44

executive management

Chief Information Security Officer, 101-102, 524
cyber attack liability website, 123
duty of care, 97
evaluating information security policies, 97-100
audits, 98
capability maturity model, 98-99
independent assessors, 97
GLBA compliance, 413-415
information security governance, 101
information security policy authorization, 96, 100

Executive Order 13256, 132, 155
exemptions, 44, 521
Exploit Wednesday, 229

F

facilities

communications, 538
data centers, 538
entry controls, 536
HIPAA compliance, 455
layered defense model, 190
access controls, 192-195
locations, 190
perimeters, 191
perimeters, 536
power consumption, 537
recovery, 389
resources, 216
secure areas, 537

FACTA (Fair and Accurate Credit Transaction Act of 2003), 163, 186

FAIR (Factor Analysis of Information Risk), 108
false negative/positive decision state, 275

Family Educational Rights and Privacy Act of 1974 (FERPA), 15, 30, 122, 163

FCBA (Fair Credit Billing Act), 483
FCRA (Fair Credit Reporting Act), 163, 186

FDIC information security standards website, 122

federal agencies data breach notifications, 349
Federal Continuity Directive 1, 373
Federal Information Processing Standard 199, 129-131
Federal Information Processing Standards (FIPS), 73

Federal Information Security Management Act (FISMA) website, 90
Federal Register, 412

Federal Trade Commission (FTC) Safeguards Act, 411
FERPA (Family Educational Rights and Privacy Act of 1974), 15, 30, 122, 163
FFIEC (Federal Financial Institutions Examination Council), 245, 394

FFIEC (Federal Financial Institutions Examination Council) IT Handbook, 262, 417, 518


filtering content, 275

financial history protection, 163


financial institutions (GLBA compliance), 13-14, 409

Board of Directors involvement, 413-415
FFIEC IT InfoBase, 417
financial institutions definition, 410
identity theft, 424-427, 440-441
Interagency Guidelines, 412
Privacy Rule, 409
program effectiveness, monitoring, 421
regulatory

agencies/rules, 411
examination, 423-424
oversight, 410
GLBA (Gramm-Leach-Bliley Act) 591

Information Assurance Framework, 73
information security publications, 73
resource websites, 91
PCI DSS, 486
fraud
corporate account takeover fraud advisory, 428, 440
credit/debit card, 483
hyperlinks, 239
Freedom of Information Act (FOIA), 129
FTC (Federal Trade Commission)
identity theft, 426, 440
Safeguards Act, 411
full-scale testing (business continuity), 393
functional exercises (business continuity), 392

G

GE (General Electric) Candidate Data Protection Standards, 160
general availability (software), 305
Genesco v. Visa lawsuit, 504
Glass-Steagall Act, 409
GLBA (Gramm-Leach-Bliley), 13-14, 409
data breach notifications, 347-348
FFIEC IT InfoBase, 417
financial institutions definition, 410
Interagency Guidelines, 412
Board of Directors involvement, 413-415
identity theft, 424-427, 440-441
program effectiveness, monitoring, 421
reports, 422
risks, 415-418
service provider oversight, 420-421, 440
testing, 419-420
threat assessment, 415
training, 418-419
threat assessment, 415
training, 418-419

ISO 27002:2013 requirements, 416
logs, 243
Privacy Rule, 409
regulatory
  agencies/rules, 411
  examination, 423-424
  oversight, 410
Safeguards Act, 411
Security Guidelines, 409
Global Payments, Inc. data breach, 491, 503
go live (software), 305
Google
  2-step password verification process, 269
data centers website, 190
governance
  business continuity, 381
  defined, 100-101
distributed model, 101
  Chief Information Security Officer, 101-102
  Information Security Officer, 101
  Information Security Steering Committee, 102-103
  organizational roles/responsibilities, 103
regulatory requirements, 104
sample policy, 522-523
  authorization/oversight, 523
  Chief Information Security Officer, 524
  goals/objectives, 522
  index, 522
  Information Security Steering Committee, 524
  lead author, 526
  supporting resources/source material, 526
web site, 123
Gramm-Leach-Bliley Act. See GLBA
graphic format, 222
group-based access, 450
guest networks, 272
guiding principles
  defined, 5
  information security policies, 96
  Toyota, 6

H
hacktivism, 68, 91
handling standards, 136-138
  policy statement, 139
  sample matrix, 137
Hannaford Bros. Supermarkets data breach, 491
hard drives
  data, deleting, 201
  unscrubbed, 202
hardware assets, 140-141
hashing, 311
headings (policies), 42
healthcare. See HIPAA; HITECH Act
health clearinghouses/plans, 444
Health Information Technology for Economic and Clinical Health. See HITECH Act
Health Insurance Portability and Accountability Act of 1996. See HIPAA
Heartland Payment Systems data breach, 491
HHS HIPAA security series website, 518
hidden files, 200
hierarchical format, 221
hierarchy (policies), 33
  baselines, 34
  guidelines, 34
  plans, 36
  procedures, 35
  standards, 33-34
high potential impact, 129
HIPAA (Health Insurance Portability and Accountability Act of 1996), 14, 444
  administrative standards, 446
  assigned security responsibility, 448
  business associate contracts and other arrangements, 453
contingency plans, 451-452
evaluation, 452-453
information access management, 449-450
security awareness and training, 450-451
security incident procedures, 451
security management process, 447-448
summary, 454
workforce security, 448-449
breach notifications, 348-349, 468-469
business associates changes, 465
categories, 445
covered entities, 444
Department of Health and Human Services
HIPAA security series website, 518
enforcement/compliance, 445
  Affinity Health Plan photocopier breach, 467
  proactive, 467
  State Attorneys General authority, 466
  violations, 466
  websites, 480
implementation specifications, 446
log reviews, 243
objective, 444-445
organizational requirements, 461-463
physical standards, 455
  device and media controls, 456-457
  facility access control, 455
  summary, 457
  workstations, 456
policies and procedures standards, 463-464
resource websites, 479
security awareness and training requirement,
  173
subcontractor liability, 465
technical standards, 458
  access control, 458-459
  audit controls, 459
  integrity controls, 459
  person or entity authentication, 460
summary, 461
transmission security, 460
website, 30, 122

history of policies, 3-5
HITECH (Health Information Technology for
Economic and Clinical Health) Act, 14, 348
  breach notifications, 348-349, 468-469
  business associates, 465
  enforcement
    proactive, 467
    State Attorneys General authority, 466
    violations, 466
    websites, 480
  overview, 464
  resource websites, 480
  subcontractor liability, 465
hoaxes, 240
honoring the public trust, 7
host-based IDSs/IPs, 275
hot sites, 386
Huffington Post Edward Snowden article
website, 155
human resources, 77
  background checks
    bankruptcies, 163
    consent, 162
    credit history, 164
    criminal, 163-164
    educational, 163-164
    employee right to privacy, 162
    employment, 164
    financial history, 163
    licenses/certifications, 164
    motor vehicle records, 163
    social media, 162
    workers’ compensation history, 163
  employee
    agreements, 170-171
    lifecycle, 157-158, 185
ISO 27002:2013/NIST guidance, 157
onboarding, 165-166
orientations, 167-168
recruitment, 158
  candidate data, 159-160
government clearances, 165
  interviews, 160
job postings, 159
policy statement, 161
  prospective employees, screening, 161-164, 186
sample policy, 530
  electronic monitoring, 532
employee agreements, 533
employee termination, 532
goals/objectives, 530
index, 530
  information security training, 533
lead author, 534
personnel screenings, 531
recruitment, 531
  supporting resources/source material, 534
user provisioning, 532
security clearances, 185
security education, training, and awareness model, 174
  HIPAA, 173
  importance, 172
  NIST SP 800-16 SETA model, 173
policy statement, 175
small businesses, 175
termination, 168-169
  disgruntled ex-network administrator example, 169
  policy statement, 169
websites, 186
  user provisioning, 166-167
Hurricane Sandy websites, 407
hybrid malware, 231
hyperlinks, 239

I-9 form, 166
ICA (International CPTED Association), 191
identification
  access controls, 265
  incidents, 330-331
  subjects. See authentication
identity-based access, 450
identity theft, 424-425
  corporate account takeovers, 428, 440
  GLBA Interagency Guidelines Supplement A requirements, 425-426
  Identity Theft Data Clearinghouse, 426
  Internet banking safeguards, 427
  resource websites, 440-441
IDBs (intrusion detection systems), 274-275, 297
IMAP (Internet Message Access Protocol), 237
Immigration Reform and Control Act of 1986 (IRCA), 166
impact assessment (business continuity), 378
  customer communication example, 379
  defined, 378
  high potential, 129
  information security risk, 107
  low potential, 129
  metrics, 378
  moderate potential, 129
  policy statement, 380
  process, 378
implementation, 20
  changes, 227
  HIPAA, 446
  SDLC, 303
  systems, 555
inappropriate usage incidents, 333
incidents
  Acceptable Use Policy, 573
  classification, 558
communicating, 339
data breach notifications, 345-346
chronology, 346
federal agencies, 349
federal law, 347
GLBA, 347-348
HIPAA/HITECH, 348-349
New Hampshire law, 352
policy statement, 352
public relations, 353
regulations, 345
resource websites, 368-369
small businesses, 353
state laws, 350-351
success, 351-352
Veterans Administration, 349-350
DDoS attacks, 331-332
definition, 557
HIPAA compliance, 451
identifying, 330-331
inappropriate usage, 333
intentional unauthorized access, 331
investigating
chain of custody, 343-344
documentation, 341
evidence storage/retention, 344
forensics, 342-343
law enforcement cooperation, 341-342
policy statement, 345
resource websites, 368-369
ISO 27002:2013, 329
malware, 332
management personnel, 337-340
NIST, 329
organizational responses, 329
reporting, 334
responses
authority, 559
coordinators (IRCs), 338
plans (IRPs), 559
programs, 335-336
teams (IRTs), 103, 338
training, 340
sample policy, 557
classification, 558
data breach/notifications, 560
definition, 557
evidence handling, 560
goals/objectives, 557
index, 557
IRP, 559
lead author, 561
response authority, 559
supporting resources/source material, 561
severity levels, 333-335
US-CERT (United States-Computer Emergency Readiness Team), 330
inclusive information security policies, 12
independent assessors, 97
independent audit reports, 246
indicators (incidents), 336
information, 8
assets. See asset management
Assurance Framework, 73
custodians, 72
owners, 72
information security, 76
Audit and Control Association (ISACA), 98, 519
authorization, 96, 100
championing, 19
change drivers, 97
characteristics, 8
adaptable, 11-12
attainable, 11
endorsed, 9
enforceable, 12
inclusive, 12
realistic, 10
relevant, 10
CIA (confidentiality, integrity, availability).
See CIA
client synopsis, 95
defined, 7
digital non-public personally identifiable information, 15-16
duty of care, 97
evaluating, 97-100
  audits, 98
  capability maturity model, 98-99
  independent assessors, 97
FDIC standards, 122
Five A’s, 71
governance
  Chief Information Security Officer, 101-102
defined, 100-101
distributed model, 101
Gramm-Leach-Bliley (GLBA), 13-14
Health Insurance Portability and Accountability Act of 1996 (HIPAA), 14
Information Security Officer, 101
Information Security Steering Committee, 102-103
organizational roles/responsibilities, 103
regulatory requirements, 104
websites, 122-123
guiding principles, 96
integrated approaches, 94
ISO/IEC 27002:2013, 74-75
lifecycle
  adoption, 19-20
  defined, 16
  development, 17-18
  publication, 18-19
  review, 20
NIST guidance, 93
objective, 8
parallel approaches, 94
regulatory requirements, 94
risk
acceptance, 109
appetite, 106
assessment methodologies, 108
controls, 107
cyber-insurance, 111
defined, 105
evaluating, 106-108
impact, 107
inherent, 106
likelihood of occurrence, 107
management, 109, 123
mitigation, 109-110
NIST assessment methodology, 108
residual risk, 107
response policy statement, 110
risk management oversight policy statement, 106
taking risks, 105
threats, 106-107
tolerance, 105-106
vulnerabilities, 107
Steering Committee, 102-103, 524
strategic alignment, 94
student records, 15
user versions, 94
vendor versions, 95
Information Security Officer (ISO), 101, 122
information systems
Acceptable Use Policy, 568
  agreement, 568
  applications, 571
  authentication, 570
data protection, 569-570
distribution, 568
incident detection/reporting, 573
Internet, 572
messaging, 571
mobile devices, 572
password controls, 570
remote access, 573
access controls. See access controls
acquisition, development, and maintenance. See SDLC
commercial off-the-shelf software/open source software, 304-306
defined, 126
inventory, 139
asset descriptions, 140-142
choosing items to include, 139
controlling entities, 142
disposal/destruction of assets, 142
hardware assets, 140-141
logical addresses, 141
policy statement, 142
software assets, 140-142
unique identifiers, 140
ISADM, 300
secure code
broken authentication, 310
defined, 306
dynamic data verification, 309
injection, 308
input validation, 308
output validation, 309
OWASP, 307-308
policy statement, 310
SAMM, 307
session management, 310
Security Association, Inc. (ISSA) website, 519
systems development lifecycle, 302
development/acquisition phase, 302
disposal phase, 303
implementation phase, 303, 555
initiation phase, 302
operations/maintenance phase, 303, 555
policy statement, 304
testing environments, 305-306

Information Technology Laboratory (ITL), 72-73
infrastructure access controls, 272
disaster recovery, 389
equipment, 140
layered border security, 273
border device administration/management, 275
content filtering, 275
firewalls, 273-274
IDSs/IPSs, 274-275
penetration testing, 276
policy statement, 276-277
network segmentation, 272-273
remote, 277
authentication, 278
authorization, 279
NIST, 278
policy statement, 279-280
remote access portals, 278
teleworking, 280-281, 298
VPNs, 278
ingress network traffic, 274
inherence authentication, 269
inherent risk, 106
initial responses (incidents), 336
initiation phase (SDLC), 302
injection, 308
input validation, 308
insecure code, 306
insider theft, 195
Institute of Internal Auditors website, 519
integrated approaches, 94
integrity, 68-69
data, 69
government data classification, 130
HIPAA technical compliance, 459
system, 69
threats, 69
intentional unauthorized access incidents, 331

Interagency Guidelines (financial institutions), 412
  Board of Directors involvement, 413-415
  identity theft, 424-425
    Identity Theft Data Clearinghouse, 426
  Internet banking safeguards, 427
  resource websites, 440-441
  Supplement A requirements, 425-426
  program effectiveness, monitoring, 421
  reports, 422
  risks, 415-418
  service provider oversight, 420-421, 440
  testing, 419-420
  threat assessment, 415
  training, 418-419

internal auditors, 103

Internal Revenue Service Form W-4 Employee’s Withholding Allowance Certificate, 166

Internal Security Assessors (ISAs), 501

internal use data, 134

International CPTED Association (ICA), 191

International Information Systems Security Certification Consortium (ISC2) website, 519

International Organization for Standardization.
  See ISO

Internet
  Acceptable Use Policy, 572
  applications security risks, 308
    broken authentication, 310
    dynamic data verification, 309
    injection, 308
    input validation, 308
    output validation, 309
    policy statement, 310
    session management, 310
  banking safeguards, 427
  caches, 200
  communications, 274
  Message Access Protocol (IMAP), 237
  server logs, 244

interviews (job), 160

introductions, 39-41

intrusion detection systems (IDSs), 274-275, 297

intrusion prevention systems (IPSs), 274-275, 297

inventories, 139
  assets, 529
    descriptions, 140-142
    disposal/destruction, 142
    hardware, 140-141
    software, 140-142
  choosing items to include, 139
  controlling entities, 142
  logical addresses, 141
  policy statement, 142
  unique identifiers, 140

investigating incidents, 336
  chain of custody, 343-344
  documentation, 341
  evidence storage/retention, 344
  forensics, 342-343
  law enforcement cooperation, 341-342
  policy statement, 345
  resource websites, 368-369

IP (Internet Protocol)
  addresses, 274
  domain names, 141
  IPsec, 278
  IPv4 addresses, 141
  IPv6 addresses, 141

IPSs (intrusion prevention systems), 274-275, 297

IRCA (Immigration Reform and Control Act of 1986) website, 186

IRCs (incident response coordinators), 338
IRPs (incident response plans), 559
IRTs (incident response teams), 338
ISACA (Information Systems Audit and Control Association), 98, 519
ISADM (information systems acquisition, development, and maintenance). See SDLC
ISAs (Internal Security Assessors), 501
ISC2 (International Information Systems Security Certification Consortium) website, 519
ISO (Information Security Officer), 101
ISO (International Organization for Standardization), 72-74
    27002:2013, 74-75
        access controls, 265
        asset management, 125
        business continuity management, 371
        communications, 219
        cryptography, 301
        domains, 75-80
        GLBA requirements, 416
        healthcare regulation compliance, 443
        human resources, 157
        information security policies guidance, 93
        ISADM, 300
        operations, 219
        origins, 74
        physical/environmental security, 189
        regulation compliance, 409
        security incidents, 329
        members, 74
        responsibilities, 127
        websites, 75, 90
ISSA (Information Systems Security Association, Inc.) website, 519
IT InfoBase, 417
ITL (Information Technology Laboratory) bulletins, 73
IT Security Standards comparison website, 91

J
Jackson, Tennessee F4 tornado, 373
job postings, 159

K
keyloggers, 231
keys, 312
    asymmetric, 313, 327
    best practices, 314-315
    defined, 311
    keyspace, 312
    management, 556
    NIST, 314
    PKI (Public Key Infrastructure), 313, 327
    symmetric, 313
knowledge-based authentication, 267
Krebs, Brian blog, 428

L
labeling
    classifications, 136
    policy statement, 139
language (regulations), 412
LANs (local area networks), 273
layered border security, 273
    border device administration/management, 275
    content filtering, 275
    firewalls, 273-274
    IDSs/IPSs, 274-275
    penetration testing, 276
    policy statement, 276-277
layered defense model, 190
    access controls, 192
        documents, 194-195
        entry authorization, 192
        insider theft, 195
        secure areas, 194
        workspaces, 193
least privilege access controls, 266
license background checks, 164
lifecycles
classification, 128
employees, 157-158, 185
  onboarding, 165-166
  orientations, 167-168
  recruitment. See recruitment
termination, 168-169
  user provisioning, 166-167
policies
  adoption, 19-20
  defined, 16
  development, 17-18
  publication, 18-19
  review, 20
  systems development. See SDLC
likelihood of occurrence, 107
Linux root, 232
local area networks (LANs), 273
location threats, 376
lockscreen ransomware, 232
logs
  analyzing, 243
  authentication server, 244
  data inclusion selections, 242
  data prioritization, 242
  defined, 242
  firewall, 243
  management, 242
  policy statement, 244
  review regulations, 243
  sample policy, 543
  syslogs, 242
  user access, monitoring, 284-285
  web server, 244
low potential impact, 129

M
MAC (Media Access Control) addresses, 141
MACs (mandatory access controls), 270
mainframe recovery, 389
maintenance
  business continuity, 393-394, 567
  payment card industry
    information security policies, 495-496
    vulnerability management programs, 490-491
  SDLC, 303
  systems, 555
malware, 230, 332
  antivirus software, 234
  APTS (advanced persistent threats), 230
categories, 231-232
  bots, 232
  hybrid, 231
  ransomware, 232, 262
  rootkits, 232
  spyware, 232, 262
  Trojans, 231
  viruses, 231
  worms, 231
controlling, 233
data card breaches, 491
e-mail, 238
  policy statement, 235
  resource websites, 261-262
  sample policy, 542
managing
  border devices, 275
  business continuity, 564-565
cryptography keys, 314-315
  keys, 556
  logs, 242
  risks
    acceptance, 109
cyber-insurance, 111
defined, 109
financial institutions, 416-418
mitigation, 109-110
websites, 123, 155
mandatory access controls (MACs), 270
Manning, Private Bradley, 67
Massachusetts
  Security Breach Notification Law, 350
  Standards for the Protection of Personal Information of Residents of the Commonwealth, 15, 30
maximum tolerable downtime (MTD), 378
MBCP (Master Business Continuity Professional), 384
mean time to repair (MTTR), 247
Media Access Control (MAC) addresses, 141
medical records, protecting, 14
member information system, 413
memory cards, 268
merchants. See PCI DSS
Merriam-Webster Online cyber definition website, 30
message integrity, 311
messaging. See email
metadata, 200, 238
Microsoft patches, 229
Miller, Andrew James, 342
mitigating risk, 109-110
mobile devices/media, 205
  Acceptable Use Policy, 572
  sample policy, 539
  websites, 386
moderate potential impact, 129
monitoring
  changes, 227
  financial institutions security programs, 421
  payment card industry networks, 494-495
  service providers, 247
  systems, 552
  user access, 284-285
motor vehicle records, 163
MTD (maximum tolerable downtime), 378
MTTR (mean time to repair), 247
multifactor authentication, 266
multilayer authentication, 266

N

NACD (National Association of Corporate Directors), 96
NACHA Corporate Account Takeover Resource Center website, 428
NAC (network access control) systems, 279
National Institute of Standards and Technology. See NIST
national security information classifications
derivative classification, 133
Executive Order 13536, 131
listing of classifications, 132-133
original classification, 133
NCAS (National Cyber Awareness System), 330
NCCIC (National Cybersecurity and Communications Integration Center), 330
need-to-know access controls, 266
negative corporate cultures, 6
networks
  access control (NAC) systems, 279
  border devices, 548-549
  disaster recovery, 389
  equipment, 140
  IDSs/IPSs, 274-275
  infrastructure, 272
  layered border security, 273
    border device administration/management, 275
    content filtering, 275
    firewalls, 273-274
    IDSs/IPSs, 274-275
    penetration testing, 276
    policy statement, 276-277
monitoring, 552
payment card industry, 494-495
remote access controls, 277
  authentication, 278
  authorization, 279
  NIST, 278
  policy statement, 279-280
remote access portals, 278
sample policy, 549-550
teleworking, 280-281, 298, 550
VPNs, 278
segmentation, 272-273
  policy statement, 273
  sample policy, 548
neutral corporate cultures, 6
New Hampshire data breach notification website, 352
New York cybersecurity websites, 63
NIST (National Institute of Standards and Technology), 72
  access controls, 265
  asset management, 125
  business continuity management, 371
  communications guidance, 219
  Computer Security Division mission, 72
  cryptography, 301, 314
  data at rest/in motion, 459-460
digital forensics, 342
firewalls, 274
human resources guidance, 157
Information Assurance Framework, 73
information security
guidance, 93
  publications, 73
intrusion detection and prevention systems, 275
malware protection, 230
operations guidance, 219
physical/environmental security, 189
regulation compliance, 409, 443
remote access controls, 278
resource websites, 91
Risk Management Framework (RMF), 108
security incidents, 329
SP 800-16 SETA model, 173
special publications website, 516
teleworking, 280
non-disclosure agreements, 170
non-discretionary access controls, 271
non-public personally identifiable information. See NPPI
notifications
data breach, 345-346
  chronology, 346
  federal agencies, 349
  federal law, 347
  GLBA, 347-348
  HIPAA/HITECH, 348-349
  New Hampshire law, 352
  policy statement, 352
  public relations, 353
  regulations, 345
  resource websites, 368-369
  sample policy, 560
  small businesses, 353
  state laws, 350-351
  success, 351-352
  Veterans Administration, 349-350
HIPAA breach, 468-469
  breach definition, 468
  requirements, 469
  Safe Harbor Provisions, 468
  websites, 481
identity theft requirements, 426
incidents, 336
NPPI (non-public personally identifiable information), 15-16, 134
defined, 134
  elements, 134
GLBA protection, 409
job candidates, 159-160

objectives (policies), 42
objects
  access controls, 265
  capability authorization model, 270
OCR (Office of Civil Rights), 445
OCSP (Online Certificate Status Protocol), 315
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), 108
OEPs (occupant emergency plans), 385
offensive controls, 109
Old Testament of the Bible, 4-5
Omnibus Rule, 464-465, 480
onboarding employees, 165-166
one-time passcodes (OTPs), 268
Online Certificate Status Protocol (OCSP), 315
open mail relay, 240
open security posture, 266
open source software
  policy statement, 306
  releases, 304
  SDLT, 304
  updates, 305-306
Open Web Application Security Project.  
See OWASP
operating system software, 140
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 108
OPERATION PAYBACK DDoS attack, 332
operations, 78
  business functions, 386
  change control, 225, 262
    change management processes, 225
    communicating changes, 227
    documentation, 227
    emergency situations, 227
implementing changes, 227
importance, 225
monitoring, 227
patches, 228-229
plans, 226
policy statement, 228
RFCs, 226
contingency plans, 387
examples, 387
operating procedures, 388
policy statement, 388
sample policy, 565
data backups/replication
policy statement, 236
recommendations, 235
testing, 236
delivery functions, 385
disasters, 371
email
  access, controlling, 239
  ARPANET, 237
  encryption, 238
  hoaxes, 240
  IMAP, 237
  malware, 238
  metadata, 238
  policy statement, 241
  POP3, 237
  servers, 240-241
  SMTP, 237
  user error, 240
ISO 27002:2013 series guidance, 219
logs
  analyzing, 243
  authentication server, 244
data inclusion selections, 242
data prioritization, 242
defined, 242
defined, 242
firewall, 243
management, 242
policy statement, 244
review regulations, 243
syslogs, 242
web server, 244
malware, 230
antivirus software, 234
APTs (advanced persistent threats), 230
categories, 231-232
controlling, 233
email, 238
policy statement, 235
resource websites, 261-262
risks, 108, 415
sample policy, 540
change control, 541
data replication, 543
email, 543
goals/objectives, 540
index, 540
lead author, 545
logs, 543
malware, 542
patch management, 542
service providers, 544
SOP, 541
supporting resources/source material, 545
SDLC, 303
service provider oversight, 245
contracts, 247
due diligence, 245-246
independent audit reports, 246
monitoring, 247
policy statement, 248
SOPs, 219
developing, 220
documenting, 220
formats, 220-223
policy statement, 225
writing resource, 224
oral law, 3
organizations
business associate contracts and other arrange-
ments HIPAA compliance, 453
data breach notifications public relations, 353
disaster response structure, 384
HIPAA compliance standards, 461-463
incident responses, 329
resilience, 372
orientations (employee), 167-168
original classification, 133
OTPs (one-time passcodes), 268
out-of-band authentication, 268
out-of-wallet questions, 267
output validation, 309
OWASP (Open Web Application Security
Project), 307
defined, 307
security risks, 308
broken authentication, 310
dynamic data verification, 309
injection, 308
input validation, 308
output validation, 309
policy statement, 310
session management, 310
websites, 307, 327
ownership (assets), 126
data owners, 126
Information Security Officer role, 127
management, 527
policy statement, 127
PANs (primary account numbers), 484
parallel approaches, 94
passive voice, 51-52
passwords
Acceptable Use Policy, 570
cognitive, 267
equipment, 286
Google 2-step verification process, 269
Yahoo! compromise, 267, 297
patches, 228, 305
managing, 229
Microsoft, 229
sample policy, 542
Patch Tuesday, 229
Payment Card Industry Data Security Standard. See PCI DSS
payroll data protection, 166
PCI DSS (Payment Card Industry Data Security Standard), 104, 483
account data, 484
business as usual, 487
cardholder data environment, 484
compliance, 499
assessment, 500-501
fines/penalties, 503-504
merchants required, 499
SAQ, 502
validation levels, 499-500
websites, 514
credit card elements, 484
framework, 486
Global Payments data breach, 503
log reviews, 243
malware breaches, 491
payment security standards council documents
library website, 518
primary account numbers, 484
requirements, 487-488
resource websites, 515
six core principles, 486
build and maintain secure network/systems, 488-489
implement strong access control measures, 492-493
maintain information security policy, 495-496
maintain vulnerability management program, 490-491
protect cardholder data, 489-490
regularly monitor and test networks, 494-495
skimming, 493-494, 514
system components, 484
version 3.0 updates, 487
PCI Security Standards Council website, 501
PDD-63 (Presidential Decision Directive 63) Critical Infrastructure Protection, 372
penetration testing (border devices), 276
perimeter networks, 272
perimeter security, 191, 536
personal health records, 348
personal identity theft, 424-425
personal records reported compromised example, 203
personnel. See employees
person or entity authentication standard (HIPAA compliance), 460
physical security, 78, 189
access controls, 192
documents, 194-195
time authorization, 192
insider theft, 195
secure areas, 194
workspaces, 193
CPTED, 191
equipment, 196
chain of custody, 202
disposal, 200-203
fire prevention controls, 198-199
power, 196-199, 215
resources, 216
theft, 203-205
facilities, 190
locations, 190
perimeters, 191
resources, 216
HIPAA compliance
device and media controls, 456-457
facility access control, 455
summary, 457
workstation security, 456
workstation use, 456
ISO 27002:2013 series guidelines, 189
safeguards, 413
sample policy, 535
clear desk/clear screen, 537
data centers/communications facilities, 538
data entry controls, 536
equipment disposal, 539
goals/objectives, 535
index, 535
lead author, 539
mobile devices/media, 539
physical perimeter, 536
power consumption, 537
secure areas, 537
supporting resources/source material, 539
workspace classification, 536
threats, 375
PKI (Public Key Infrastructure), 313, 327
plain language
active/passive voice, 51-52
Clarity Index, 52
defined, 48
fisheries example, 49
guidelines, 50-51
PLAIN, 50-51, 63
“A Plain English Handbook: How to create clear SEC disclosure documents,” 48
Plain Language Movement, 49
Plain Writing Act, 49, 62
reference websites, 63
SOP development, 220
PLAIN (Plain Language Action and Information Network), 50-51, 63
plans, 36
business continuity, 380
audits, 393-394
certifications, 384
disaster recovery, 388-391, 407
disaster response, 384-385
education/training, 384
maintenance, 393-394
policy statement, 381, 386-387
relocation strategies, 385-386
resource websites, 406
responsibilities, 381-383
resumption phase, 391
sample policy, 564
small businesses, 394
testing, 392-394
disaster recovery, 566
operational contingency, 387
examples, 387
operating procedures, 388
policy statement, 388
sample policy, 565
policies
championing, 19
components, 38
enforcement clauses, 45
exceptions, 44
exemptions, 44
goals/objectives, 42
headings, 42
introductions, 39-41
Policy Definition section, 47
  statements, 43
  version control, 38-39
definition sections, 53
disseminating, 19
enforcement clauses, 53
formats, 36
  audience, 36
  types, 37-38
good characteristics, 8
  adaptable, 11-12
  attainable, 11
  endorsed, 9
  enforceable, 12
  inclusive, 12
  realistic, 10
  relevant, 10
hierarchy, 33
  baselines, 34
  guidelines, 34
  plans, 36
  procedures, 36
  standards, 33-34
history, 3-5
lifecycle
  adoption, 19-20
  defined, 16
  development, 17-18
  publication, 18-19
  review, 20
plain language, 48
  active/passive voice, 51-52
  Clarity Index, 52
defined, 48
  fisheries example, 49
guidelines, 50-51
PLAIN, 50-51, 63
“A Plain English Handbook: How to create clear SEC disclosure documents,” 48
Plain Language Movement, 49
Plain Writing Act, 49, 62
reference websites, 63
SOP development, 220
styles, 48
POP3 (Post Office Protocol), 237
ports, 274
positive corporate cultures, 7
possession authentication, 268
post-incident activity, 336
power, 196
  blackouts, 198
  brownouts, 198
  consumption, 196-198, 537
  fluctuations, 197-198
  policy statement, 199
  resources, 215
  spikes, 198
  surges, 198
precursors (incidents), 336
presidential policies/directives
  critical infrastructure sectors, 3, 30
  Executive Order 13563-Improving Regulation and Regulatory Review, 62
  Executive Order-Improving Government Regulations, 62
  HSPD-7 Critical Infrastructure Identification, Prioritization, and Protection, 373
  Memorandum on Plain Language in Government Writing, 62
  PDD 63 Critical Infrastructure Protection, 372
prevention control (malware), 233
primary account numbers (PANs), 484
principle of least privilege website, 297
printers, 140
prioritizing log data, 242
privacy
  employee rights, 162, 167-168
  honoring the public trust, 7
officers, 103
user account monitoring, 285

Privacy Rule (GLBA), 409
private sector data classifications, 134
privileged accounts, 283, 551
procedures, 35
productivity software, 140
programs. See plans
prospective employee screening, 161-162
    bankruptcies, 163
    consent, 162
    credit history, 164
    criminal history, 163-164
    education, 163-164
    employment, 164
    financial history, 163
    licenses/certifications, 164
    motor vehicle records, 163
    policy statement, 164
    right to privacy, 162
    Sarbanes-Oxley Act, 162-164
    social media, 162
    websites, 186
    workers’ compensation history, 163
protected data, 134
protocols, 274
    IMAP, 237
    IP
        addresses, 274
        domain names, 141
        IPsec, 278
        Ipv4 addresses, 141
        Ipv6 addresses, 141
    OCSP, 315
    POP3, 237
    SMTP, 237
public data, 134
Public Doublespeak Committee, 49
public key cryptography, 313, 327

Public Key Infrastructure (PKI), 313, 327
publishing policies, 18-19

Q – R

QSAs (Qualified Security Assessors), 501

ransomware, 232, 262
RA (Registration Authority), 313
ratings (regulatory examinations), 423-424
RBACs (role-based access controls), 271, 450
RCs (release candidates), 305
realistic information security policies, 10
recovery
    business continuity, 380
    disasters, 388
        Active Directory domain controller exam- ple, 389
        communications, 389
        facilities, 389
        infrastructure, 389
        mainframe, 389
        network, 389
        policy statement, 391
        procedures, 389
        resource websites, 407
        resumption phase, 391
        sample policy, 566
        service provider dependencies, 390
        emergencies, 372
        incidents, 336
    payment card data breaches, 503
    point objective (RPO), 378
    time objective (RTO), 378
recruitment, 158
    candidate data, 159-160
    government clearances, 165
    interviews, 160
    job postings, 159
    policy statement, 161
prospective employees, screening, 161-162
bankruptcies, 163
consent, 162
credit history, 164
criminal history, 163-164
education, 163-164
employment, 164
financial history, 163
licenses/certifications, 164
motor vehicle records, 163
policy statement, 164
right to privacy, 162
Sarbanes-Oxley Act, 162-164
social media, 162
websites, 186
workers’ compensation history, 163
sample policy, 531

Red Teaming, 276
 reducing
  power consumption, 197-198
  risk, 109
Registration Authority (RA), 313
 regulations
  agencies, 411
  compliance
    ISO/IEC 27002:2013, 409, 443
    NIST, 409, 443
data breach notifications, 345
  federal agencies, 349
  GLBA, 347-348
  HIPAA/HITECH, 348-349
  state laws, 350-351
  success, 351-352
  Veterans Administration, 349-350
defined, 13
digital non-public personally identifiable information, protecting, 15-16
emergency preparedness requirements, 372-373
encryption, 312
examination, 423-424
FERPA (Family Educational Rights and Privacy Act of 1974), 15
GLBA. See GLBA
Health Insurance Portability and Accountability Act of 1996. See HIPAA
HITECH Act. See HITECH Act
language, 412
log reviews, 243
Omnibus Rule, 464-465, 480
PCI DSS. See PCI DSS
requirements
  governance, 104
  information security, 94
  risk, 108
release candidates (RCs), 305
relocation strategies (disaster response), 385-386
remote access controls, 277
 Acceptable Use Policy, 573
 authentication, 278
 authorization, 279
 NIST, 278
 policy statement, 279-280
 portals, 278
 remote access portals, 278
 sample policy, 549-550
 teleworking, 280
   NIST, 280
   policy statement, 281
   sample policy, 550
   websites, 298
   Yahoo! telecommuting ban, 281
VPNs, 278
reporting
 audits, 98
 compliance, 500-501
 data breaches, 560
 financial institutions regulation compliance, 422
Business Continuity Teams (BCTs), 381
governance, 381
policy statement, 383
tactical, 382
data owners, 126
incident management personnel, 338
Information Security Officer, 127
information security roles, 103

Resumption plans
business continuity, 380
disaster recovery, 391

Reviewing policies, 20
RFCs (Requests for Change), 226

Risk Management Framework (RMF), 108

Risks
assessment, 447
avoidance, 110
continuity planning, 374
impact assessment, 378-380
risk assessments, 376-377
threat assessments, 375
cyber-insurance, 111

Email
access, 239
encryption, 238
hoaxes, 240
IMAP, 237
malware, 238
metadata, 238
POP3, 237
servers, 240-241
SMTP, 237
user errors, 240

evaluating, 106-107
business risk categories, 107
controls, 107
impact, 107
inherent risk, 106
likelihood of occurrence, 107

Responsibilities
asset ownership, 126-127
assigned security, 448
business continuity, 381
methodologies, 108
NIST methodology, 108
policy statement, 108
residual risk, 107
threats, 106-107
vulnerabilities, 107
financial institutions
assessment, 415-416
management, 416-418
information security
acceptance, 109
appetite, 106
assessment methodologies, 108
controls, 107
cyber-insurance, 111
defined, 105
evaluating, 106-108
impact, 107
inherent, 106
likelihood of occurrence, 107
management, 109, 123
mitigation, 109-110
NIST assessment methodology, 108
residual risk, 107
response policy statement, 110
risk management oversight policy statement, 106
taking risks, 105
threats, 106-107
tolerance, 105-106
vulnerabilities, 107
management
acceptance, 109
defined, 109
mitigation, 109-110
websites, 123, 155
reducing, 109
response policy statement, 110
sample policy, 522-523
assessment, 525
authorization/oversight, 523
goals/objectives, 522
index, 522
lead author, 526
management oversight, 525
response, 525
supporting resources/source material, 526
sharing, 110
transfers, 110
“Risk, Threat, and Vulnerability 101” website, 122
RMF (Risk Management Framework), 108
ROC (Report on Compliance), 500-501
role-based access controls (RBACs), 271, 450
roles
incident management personnel, 338
information security responsibilities, 103
rollback strategies (software), 305
rootkits, 232
root (Unix/Linux), 232
RPO (recovery point objective), 378
RTO (recovery time objective), 378
rule-based access controls, 271

S
S. 418: Do-Not-Track Online Act of 2013, 232
Safeguards Act, 411
Safe Harbor Provision (HIPAA), 468
SAMM (Software Assurance Maturity Model), 307, 327
SANS Institute website, 519
SAQ (self-assessment questionnaire), 502
Sarbanes-Oxley Act of 2002 (SoX), 162-164, 186
SB 1386: California Security Breach Information Act, 15
SBA disaster response resources, 395
screen scrapers, 231
SDLC (systems development lifecycle), 302
commercial off-the-shelf software/open source software, 304
policy statement, 306
releases, 304
testing environments, 305-306
updates, 305
development/acquisition phase, 302
disposal phase, 303
implementation phase, 303, 555
initiation phase, 302
operations/maintenance phase, 303, 555
policy statement, 304
sample policy, 554
testing environments, 305-306

secret data classification, 132

sector-based regulations
data breach notifications
GLBA, 347-348
HIPAA/HITECH, 348-349
emergency preparedness, 373

secure areas
controls, 194
sample policy, 537

secure code
broken authentication, 310
defined, 306
dynamic data verification, 309
injection, 308
input validation, 308
output validation, 309
OWASP, 307-308
policy statement, 310
SAMM, 307
session management, 310

security
awareness, 174, 450-451
clearances, 165, 185
domains, 65
education/training, 172-174
frameworks. See frameworks
incidents. See incidents
posture, 266

Security Information and Event Management (SIEM), 242

segmenting networks, 548
segregation of duties, 283
self-assessment questionnaire (SAQ), 502
semi-trusted networks, 272
sensitive but unclassified data classification, 133

sensitive customer information. See NPPI

sequencing logs, 243

servers
email, 240-241
farms, 190

service level agreements (SLAs), 70, 390

service providers, 245, 413
contracts, 247
dependencies
disaster recovery, 390
threats, 375-376
due diligence, 245-246
financial institutions oversight, 420-421, 440
independent audit reports, 246
monitoring, 247
policy statement, 248
sample policy, 544

session management, 310

SETA (security education, training, and awareness), 174
HIPAA, 173
importance, 172
NIST SP 800-16 SETA model, 173
policy statement, 175

severity levels (incidents), 333-335
sharing risk, 110

shelter-in-place plans, 385
shoulder surfing, 194

SIEM (Security Information and Event Management), 242
signatures (logs), 243
Simple Mail Transfer Protocol (SMTP), 237
simple step format, 221
simulations (business continuity testing), 392
single-factor authentication, 266
singular policies, 37
six PCI DSS core principles, 486
build and maintain secure network/systems, 488-489
implementing strong access control measures, 492-493
maintain information security policy, 495-496
protect cardholder data, 489-490
regularly monitor and test networks, 494-495
requirements, 487-488
vulnerability management program maintenance, 490-491
skimming, 493-494, 514
slammer worm website, 261
SLAs (service level agreements), 70, 390
sloppy code, 306
Small Business Administration disaster response resources, 395
small businesses
access control, 286
corporate account takeover website, 428
data breach notifications, 353
data classification/handling example, 142-143
disaster response plans, 394
encryption, 316
IT security staff, 249
SMTP (Simple Mail Transfer Protocol), 237
Snowden, Edward, 133, 155
SOC1 reports, 246
SOC2 reports, 246
SOC3 reports, 246

software
Acceptable Use Policy, 571
antivirus, 234
assets, 140-142
commercial off-the-shelf. See COTS development, 302
commercial off-the-shelf software/open source software, 304
development/acquisition phase, 302
disposal, 303
implementation phase, 303, 555
initiation phase, 302
operations/maintenance phase, 303, 555
policy statement, 304
sample policy, 555
malware, 230, 332
antivirus, 234
APTs (advanced persistent threats), 230
categories, 231-232
controlling, 233
data card breaches, 491
data cardholder data, 489-490
data protection, 489-490
data classification/handling example, 142-143
disaster response plans, 394
disaster recovery plans, 394
encryption, 316
email, 238
email security, 238
email threat, 238
email virus, 238
fear, 238
firewall, 238
firewall rule, 238
firewall software, 238
government, 238
healthcare, 238
infected email, 238
infected email threat, 238
infected email virus, 238
intelligence threat, 238
leak, 238
malware, 238
network access control, 238
network security, 238
operating system, 238
operating system threat, 238
operating system virus, 238
organization, 238
organization threat, 238
organization virus, 238
overuse, 238
policy, 238
policy statement, 310
sample policy, 542
SLAs (service level agreements), 70, 390
simulations (business continuity testing), 392
single-factor authentication, 266
secure code
broken authentication, 310
defined, 306
dynamic data verification, 309
injection, 308
input validation, 308
output validation, 309
OWASP, 307-308
policy statement, 310
SAMM, 307
session management, 310
testing environments, 305-306
updates, 305
Software Assurance Maturity Model (SAMM), 307
SOPs (standard operating procedures), 219
developing, 220
formats, 220-223
policy statement, 225
writing resource, 224
documenting, 220
sample policy, 541
SoX (Sarbanes-Oxley Act), 162-164, 186
Special Publication 800 series, 73
spyware, 232, 262
SSAE16 (Standards for Attestation Engagements 16) audit reports, 246
standard operating procedures. See SOPs
State Attorneys General HIPAA enforcement, 466
state data breach notification laws, 350-351
statements (policies), 43
storage
cloud, 236
evidence, 344
media, 140
strategic alignment, 94
strategic risks, 107, 415
structured reviews (business continuity), 392
student records, protecting, 15
Stuxnet, 234
subcontractor liability (HIPAA), 465
subjects (access controls), 265
authorization, 270-271
identification, 266
inherence authentication, 269
knowledge-based authentication, 267
possession authentication, 268
Supplement to the Authentication in an Internet Banking Environment Guidance, 427
Supplier Relationship domain, 79
symmetric key cryptography, 313
syslogs, 242
systems
availability, 69-70
commercial off-the-shelf software/open source software, 304
policy statement, 306
releases, 304
SDLC, 304
testing environments, 305-306
updates, 305
development lifecycle, 302
development/acquisition phase, 302
disposal phase, 303
implementation phase, 303, 555
initiation phase, 302
operations/maintenance phase, 303, 555
policy statement, 304
sample policy, 554
testing environments, 305-306
information
defined, 126
inventory, 139-142
integrity, 69
monitoring, 552
payment card industry, 484
secure code
broken authentication, 310
defined, 306
dynamic data verification, 309
injection, 308
input validation, 308
output validation, 309
OWASP, 307-308
policy statement, 310
SAMM, 307
session management, 310
testing environments, 305-306
Tabletop exercises (business continuity), 392

tactical business continuity responsibilities, 382

Target data breach, 491

technical safeguards, 413

technology service providers (TSPs), 420

Telework Enhancement Act of 2010, 280

Teleworking access controls, 280

NIST, 280

policy statement, 281

sample policy, 550

websites, 298

Yahoo! telecommuting ban, 281

temporary files, 200

Tennessee F4 tornado, 373

termination (employees), 168-169, 186

testing

business continuity plans

audits, 393-394

importance, 392

methodologies, 392-393

policy statement, 394

sample policy, 567

financial institutions regulation compliance, 419-420

information systems, 305-306

payment card industry networks, 494-495

Texas Breach Notification Law, 350

theft (equipment), 203-205

third-parties. See vendors

threats

availability, 70

business continuity, 375

confidentiality, 68

financial institutions, 415

information security risk, 106

integrity, 69

sources, 107

Title 11 of the U.S. Bankruptcy Code, 163
tolerance (risk), 105-106

Tomlinson, Ray, 237
top secret data classification, 132

Torah, 4-5

Toyota guiding principles, 6, 29

training, 174

business continuity management, 384

employees, 533

financial institutions regulation compliance, 418-419

HIPAA compliance, 450-451

incident response, 340

transactional risks, 415

transfers (risk), 110

transmission security standard (HIPAA compliance), 460

trend analysis (logs), 243

Trojans, 231

trusted networks, 272

TSPs (technology service providers), 420

Tufts University Information Technology Resource Security Policy website, 62

TSPs (technology service providers), 420

Tufts University Information Technology Resource Security Policy website, 62

Ubuntu (operating system), 61

unclassified data classification, 132

unique identifiers (assets), 140

United States

Army Clarity Index, 52

Computer Emergency Readiness Team (US-CERT), 330

Constitution, 5


Unix root, 232

unscrubbed hard drives, 202

The Untouchables, 68

untrusted networks, 272

updates (software), 305
**W**

W-4 form, 166

W32.Stuxnet, 234

waiver process, 44

warm sites, 386

war rooms (disaster response plans), 385

web. See Internet

websites

- 2013 data breach investigations, 514
- access control resources, 297
- Americans with Disabilities Act, 186
- asymmetric key cryptography, 327
- background checks, 186
- Bangladesh building collapse, 29
- Boston Marathon Bombings, 407
- business continuity resources, 406
- California Security Breach Information Act, 30
- CCFP, 343
- certificates, 327
- change control resources, 262
- change drivers, 123
- CMM, 122-123
- corporate account takeovers, 440
- CPTED, 191
- credit card growth, 514
- cyber attack liability, 123
- cyber-insurance, 123
- data breach notifications resources, 368-369
- DDoS attacks, 91
- Department of Health and Human Services
  HIPAA security series, 518

- disasters
  - recovery, 407
  - response, 406
- Do-Not-Track Online Act of 2013, 232
- DPPA, 186
- DRI, 384, 519

**V**

validation

- disaster recovery resumption phase, 391
- levels (PCI compliance), 499-500

vendors

- disaster recovery dependencies, 390
- financial institutions oversight, 420-421, 440
- information security policies versions, 95
- risks, 111
- sample policy, 544
- service provider oversight, 420-421, 440

version control (information security policies), 38-39, 94-95, 521

Veterans Administration data breach notifications, 349-350

Veterans Affairs Information Security Act, 349

viruses, 231

visitor management systems, 192

voice (active/passive), 51-52

VPNs (virtual private networks), 278

vulnerabilities. See risks

**URSIT (Uniform Rating System for Information Technology), 423-424**

users

- access controls, 282
  - administrative accounts, 283
  - importance, 282
  - monitoring, 284-285
  - policy statement, 282
  - sample policy, 551
- authentication, 547
- authorization, 548
- data users, 104
- information security policies versions, 94
- provisioning, 166-167, 532

**V**

validation

- disaster recovery resumption phase, 391
- levels (PCI compliance), 499-500

vendors

- disaster recovery dependencies, 390
- financial institutions oversight, 420-421, 440
- information security policies versions, 95
- risks, 111
- sample policy, 544
- service provider oversight, 420-421, 440

version control (information security policies), 38-39, 94-95, 521

Veterans Administration data breach notifications, 349-350

Veterans Affairs Information Security Act, 349

viruses, 231

visitor management systems, 192

voice (active/passive), 51-52

VPNs (virtual private networks), 278

vulnerabilities. See risks
duty of care, 122
email encryption, 327
employee
  lifecycle, 185
  terminations, 186
encryption, 327
Energy Star, 215
environmental security protection resources, 216
equipment passwords, 286
Executive Order 13256, 155
Fair and Accurate Credit Transactions Act of 2003, 186
FCRA, 186
FDIC information security standards, 122
Federal Register, 412
FERPA, 30, 122
FFIEC, 245, 394
FFIEC IT Handbook, 262, 417, 518
FISMA (Federal Information Security Management Act), 90
Five Principles of Organizational Resilience, 406
Freedom of Information Act, 129
FTC identity theft, 440
GE Candidate Data Protection Standards, 160
Google data centers, 190
governance, 123
Gramm-Leach-Bliley Act, 30
hacktivism, 91
hashing, 327
HIPAA, 30, 122
  breach notifications, 481
  resources, 479
HITECH Act, 480
Huffington Post Edward Snowden article, 155
Hurricane Sandy, 407
I-9 form, 166
identity theft, 440-441
IDSs/IPSs, 297
incident evidence handling, 368-369
Information Security Officer role, 122
Institute of Internal Auditors, 519
IRCA, 186
ISACA, 98, 519
ISC2, 519
ISO, 75, 90
ISSA, 519
IT Security Standards comparison website, 91
Krebs, Brian blog, 428
malware resources, 261-262
Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 30
Merriam-Webster Online cyber definition, 30
NACHA Corporate Account Takeover Resource Center, 428
New Hampshire data breach notifications, 352
New York cybersecurity, 63
NIST
  resources, 91
  special publications, 516
Omnibus Rule, 480
OWASP, 307, 327
PCI DSS resources, 515
PCI Security Standards Council, 501, 518
PKI, 313, 327
plain language
  Action and Information Network, 50-51
  fisheries example, 50
  PLAIN, 63
  Plain Writing Act of 2010, 62
  resources, 63
power resources, 215
presidential critical infrastructure security policies, 30
  Executive Order 13563-Improving Regulation and Regulatory Review, 62
Executive Order-Improving Government Regulations, 62
HSPD-7, 373
Memorandum on Plain Language in Government Writing, 62
principle of least privilege, 48, 297
ransomware, 262
risk management, 123, 155
“Risk, Threat, and Vulnerability 101,” 122
SAMM, 307, 327
SANS Institute, 519
Sarbanes-Oxley Act of 2002, 162, 186
security clearances, 185
service provider oversight, 440
skimming, 494, 514
slammer worm, 261
Small Business Administration disaster response resources, 395
spyware, 262
state security breach notification laws, 351
teleworking, 298
Toyota guiding principles, 6, 29
Tufts University Information Technology Resource Security Policy, 62
WikiLeaks, 91
Yahoo! password compromise, 267, 297
white-box assurance tests, 419
whitelists, 275
WikiLeaks, 67, 91
willful damage disasters, 371
wireless IDSs/IPSs, 275
WLANs (wireless local area networks), 273
workers’ compensation history protection, 163
workforce
defined, 448
security standard (HIPAA), 448-449
workspaces, 193
classification, 536

standards (HIPAA compliance), 456
worms, 231
writing SOPs resource, 224
writing style. See plain language

Y – Z

Yahoo!
password compromise, 267, 297
telecommuting ban, 281

zero-day exploit, 238