

WILLIAM STALLINGS



# EFFECTIVE CYBERSECURITY

A Guide to Using Best Practices  
and Standards



# **Effective Cybersecurity**

*This page intentionally left blank*

# **Effective Cybersecurity**

## **Understanding and Using Standards and Best Practices**

William Stallings

◆◆ Addison-Wesley

Upper Saddle River, NJ • Boston • San Francisco • New York  
Toronto • Montreal • London • Munich • Paris • Madrid  
Cape Town • Sydney • Tokyo • Singapore • Mexico City

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

Visit us on the Web: [informit.com/aw](http://informit.com/aw)

Library of Congress Control Number: 2018941168

Copyright © 2019 Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit [www.pearsoned.com/permissions/](http://www.pearsoned.com/permissions/).

ISBN-13: 978-0-13-477280-6

ISBN-10: 0-13-477280-6

1 18

**Executive Editor**

Brett Bartow

**Development Editor**

Marianne Bartow

**Managing Editor**

Sandra Schroeder

**Senior Project Editor**

Lori Lyons

**Copy Editor**

Kitty Wilson

**Project Manager**

Dhayanidhi Karunanidhi

**Indexer**

Ken Johnson

**Proofreader**

Jeanine Furino

**Technical Reviewers**

Akhil Behl

Michael Shannon

**Cover Designer**

Chuti Praertsith

**Compositor**

codemantra

*To Tricia, my loving wife,  
the kindest and gentlest person.*

*This page intentionally left blank*

# Contents at a Glance

Preface .....	xxvii
CHAPTER 1 Best Practices, Standards, and a Plan of Action. ....	2
<b>PART I PLANNING FOR CYBERSECURITY</b>	<b>41</b>
CHAPTER 2 Security Governance .....	42
CHAPTER 3 Information Risk Assessment .....	74
CHAPTER 4 Security Management .....	136
<b>PART II MANAGING THE CYBERSECURITY FUNCTION</b>	<b>157</b>
CHAPTER 5 People Management .....	160
CHAPTER 6 Information Management .....	178
CHAPTER 7 Physical Asset Management .....	210
CHAPTER 8 System Development .....	248
CHAPTER 9 Business Application Management .....	280
CHAPTER 10 System Access .....	304
CHAPTER 11 System Management .....	366
CHAPTER 12 Networks and Communications .....	392
CHAPTER 13 Supply Chain Management and Cloud Security .....	448
CHAPTER 14 Technical Security Management .....	482
CHAPTER 15 Threat and Incident Management .....	546
CHAPTER 16 Local Environment Management .....	602
CHAPTER 17 Business Continuity .....	622



**PART III SECURITY ASSESSMENT 665**

CHAPTER 18 Security Monitoring and Improvement..... 666

Appendix A: References and Standards ..... 694

Appendix B: Glossary ..... 708

Index ..... 726

**Appendix C (Online Only): Answers to Review Questions**

You can find Appendix C at [informit.com/title/9780134772806](http://informit.com/title/9780134772806).  
Click the Downloads tab to access the PDF file.

# Table of Contents

<b>Preface</b>	<b>xxvii</b>
<b>Chapter 1: Best Practices, Standards, and a Plan of Action</b>	<b>2</b>
1.1 Defining Cyberspace and Cybersecurity . . . . .	3
1.2 The Value of Standards and Best Practices Documents . . . . .	6
1.3 The Standard of Good Practice for Information Security . . . . .	7
1.4 The ISO/IEC 27000 Suite of Information Security Standards. . . . .	12
ISO 27001 . . . . .	15
ISO 27002 . . . . .	17
1.5 Mapping the ISO 27000 Series to the ISF SGP. . . . .	18
1.6 NIST Cybersecurity Framework and Security Documents . . . . .	21
NIST Cybersecurity Framework . . . . .	22
NIST Security Documents . . . . .	25
1.7 The CIS Critical Security Controls for Effective Cyber Defense. . . . .	27
1.8 COBIT 5 for Information Security . . . . .	29
1.9 Payment Card Industry Data Security Standard (PCI DSS) . . . . .	30
1.10 ITU-T Security Documents . . . . .	32
1.11 Effective Cybersecurity . . . . .	34
The Cybersecurity Management Process . . . . .	34
Using Best Practices and Standards Documents . . . . .	36
1.12 Key Terms and Review Questions . . . . .	38
Key Terms . . . . .	38
Review Questions . . . . .	38
1.13 References . . . . .	39

<b>Part I: Planning for Cybersecurity</b>	<b>41</b>
<b>Chapter 2: Security Governance</b>	<b>42</b>
2.1 Security Governance and Security Management . . . . .	43
2.2 Security Governance Principles and Desired Outcomes . . . . .	45
Principles . . . . .	45
Desired Outcomes. . . . .	46
2.3 Security Governance Components. . . . .	47
Strategic Planning . . . . .	47
Organizational Structure . . . . .	51
Roles and Responsibilities . . . . .	55
Integration with Enterprise Architecture . . . . .	58
Policies and Guidance . . . . .	63
2.4 Security Governance Approach . . . . .	63
Security Governance Framework. . . . .	63
Security Direction . . . . .	64
Responsible, Accountable, Consulted, and Informed (RACI) Charts. . . . .	66
2.5 Security Governance Evaluation. . . . .	68
2.6 Security Governance Best Practices . . . . .	69
2.7 Key Terms and Review Questions . . . . .	70
Key Terms . . . . .	70
Review Questions . . . . .	71
2.8 References . . . . .	71
<b>Chapter 3: Information Risk Assessment</b>	<b>74</b>
3.1 Risk Assessment Concepts. . . . .	75
Risk Assessment Challenges . . . . .	78
Risk Management . . . . .	80
Structure of This Chapter . . . . .	84

3.2 Asset Identification . . . . .	85
Hardware Assets . . . . .	85
Software Assets . . . . .	85
Information Assets . . . . .	86
Business Assets . . . . .	87
Asset Register . . . . .	87
3.3 Threat Identification . . . . .	89
The STRIDE Threat Model . . . . .	89
Threat Types . . . . .	90
Sources of Information . . . . .	92
3.4 Control Identification . . . . .	98
3.5 Vulnerability Identification . . . . .	102
Vulnerability Categories . . . . .	103
National Vulnerability Database and Common Vulnerability Scoring System . . . . .	103
3.6 Risk Assessment Approaches . . . . .	107
Quantitative Versus Qualitative Risk Assessment . . . . .	107
Simple Risk Analysis Worksheet . . . . .	113
Factor Analysis of Information Risk . . . . .	114
3.7 Likelihood Assessment . . . . .	116
Estimating Threat Event Frequency . . . . .	118
Estimating Vulnerability . . . . .	119
Loss Event Frequency . . . . .	121
3.8 Impact Assessment . . . . .	122
Estimating the Primary Loss . . . . .	124
Estimating the Secondary Loss . . . . .	125
Business Impact Reference Table . . . . .	126
3.9 Risk Determination . . . . .	128

3.10 Risk Evaluation . . . . .	128
3.11 Risk Treatment . . . . .	129
Risk Reduction . . . . .	130
Risk Retention . . . . .	130
Risk Avoidance . . . . .	130
Risk Transfer . . . . .	131
3.12 Risk Assessment Best Practices . . . . .	131
3.13 Key Terms and Review Questions . . . . .	132
Key Terms . . . . .	132
Review Questions . . . . .	133
3.14 References . . . . .	134
<b>Chapter 4: Security Management</b>	<b>136</b>
4.1 The Security Management Function . . . . .	137
Security Planning . . . . .	140
Capital Planning . . . . .	142
4.2 Security Policy . . . . .	145
Security Policy Categories . . . . .	146
Security Policy Document Content . . . . .	147
Management Guidelines for Security Policies . . . . .	151
Monitoring the Policy . . . . .	151
4.3 Acceptable Use Policy . . . . .	152
4.4 Security Management Best Practices . . . . .	154
4.5 Key Terms and Review Questions . . . . .	154
Key Terms . . . . .	154
Review Questions . . . . .	155
4.6 References . . . . .	155

<b>PART II: Managing the Cybersecurity Function</b>	<b>157</b>
<b>Chapter 5: People Management</b>	<b>160</b>
5.1 Human Resource Security . . . . .	161
Security in the Hiring Process . . . . .	162
During Employment. . . . .	164
Termination of Employment . . . . .	165
5.2 Security Awareness and Education . . . . .	166
Security Awareness. . . . .	168
Cybersecurity Essentials Program. . . . .	173
Role-Based Training . . . . .	173
Education and Certification . . . . .	174
5.3 People Management Best Practices . . . . .	175
5.4 Key Terms and Review Questions . . . . .	176
Key Terms . . . . .	176
Review Questions . . . . .	176
5.5 References . . . . .	177
<b>Chapter 6: Information Management</b>	<b>178</b>
6.1 Information Classification and Handling. . . . .	179
Information Classification . . . . .	179
Information Labeling . . . . .	185
Information Handling. . . . .	186
6.2 Privacy. . . . .	186
Privacy Threats . . . . .	189
Privacy Principles and Policies . . . . .	191
Privacy Controls . . . . .	196

6.3 Document and Records Management . . . . .	198
Document Management . . . . .	200
Records Management. . . . .	202
6.4 Sensitive Physical Information . . . . .	204
6.5 Information Management Best Practices. . . . .	205
6.6 Key Terms and Review Questions . . . . .	206
Key Terms . . . . .	206
Review Questions . . . . .	207
6.7 References . . . . .	208
<b>Chapter 7: Physical Asset Management</b>	<b>210</b>
7.1 Hardware Life Cycle Management . . . . .	211
Planning . . . . .	213
Acquisition . . . . .	214
Deployment . . . . .	214
Management . . . . .	215
Disposition . . . . .	216
7.2 Office Equipment . . . . .	217
Threats and Vulnerabilities . . . . .	217
Security Controls. . . . .	219
Equipment Disposal . . . . .	222
7.3 Industrial Control Systems . . . . .	223
Differences Between IT Systems and Industrial Control Systems . . . . .	225
ICS Security . . . . .	227
7.4 Mobile Device Security . . . . .	231
Mobile Device Technology . . . . .	233
Mobile Ecosystem. . . . .	234
Vulnerabilities. . . . .	236

Mobile Device Security Strategy . . . . .	238
Resources for Mobile Device Security. . . . .	243
7.5 Physical Asset Management Best Practices . . . . .	244
7.6 Key Terms and Review Questions . . . . .	245
Key Terms . . . . .	245
Review Questions . . . . .	245
7.7 References . . . . .	246
<b>Chapter 8: System Development</b>	<b>248</b>
8.1 System Development Life Cycle . . . . .	248
NIST SDLC Model . . . . .	249
The SGP's SDLC Model . . . . .	252
DevOps . . . . .	254
8.2 Incorporating Security into the SDLC . . . . .	259
Initiation Phase . . . . .	260
Development/Acquisition Phase . . . . .	264
Implementation/Assessment Phase . . . . .	266
Operations and Maintenance Phase . . . . .	270
Disposal Phase . . . . .	272
8.3 System Development Management . . . . .	273
System Development Methodology. . . . .	274
System Development Environments . . . . .	275
Quality Assurance . . . . .	277
8.4 System Development Best Practices . . . . .	278
8.5 Key Terms and Review Questions . . . . .	278
Key Terms . . . . .	278
Review Questions . . . . .	279
8.6 References . . . . .	279



<b>Chapter 9: Business Application Management</b>	<b>280</b>
9.1 Application Management Concepts . . . . .	281
Application Life Cycle Management . . . . .	281
Application Portfolio Management . . . . .	283
Application Performance Management . . . . .	285
9.2 Corporate Business Application Security . . . . .	287
Business Application Register . . . . .	287
Business Application Protection . . . . .	288
Browser-Based Application Protection . . . . .	289
9.3 End User-Developed Applications (EUDAs) . . . . .	295
Benefits of EUDAs . . . . .	296
Risks of EUDAs . . . . .	296
EUDA Security Framework . . . . .	297
9.4 Business Application Management Best Practices . . . . .	300
9.5 Key Terms and Review Questions . . . . .	301
Key Terms . . . . .	301
Review Questions . . . . .	302
9.6 References . . . . .	302
<b>Chapter 10: System Access</b>	<b>304</b>
10.1 System Access Concepts . . . . .	304
Authorization . . . . .	306
10.2 User Authentication . . . . .	307
A Model for Electronic User Authentication . . . . .	307
Means of Authentication . . . . .	310
Multifactor Authentication . . . . .	311
10.3 Password-Based Authentication . . . . .	312
The Vulnerability of Passwords . . . . .	313
The Use of Hashed Passwords . . . . .	315

Password Cracking of User-Chosen Passwords . . . . .	317
Password File Access Control . . . . .	319
Password Selection. . . . .	320
10.4 Possession-Based Authentication . . . . .	322
Memory Cards. . . . .	322
Smart Cards. . . . .	323
Electronic Identity Cards. . . . .	325
One-Time Password Device. . . . .	328
Threats to Possession-Based Authentication. . . . .	329
Security Controls for Possession-Based Authentication. . . . .	330
10.5 Biometric Authentication . . . . .	330
Criteria for Biometric Characteristics. . . . .	331
Physical Characteristics Used in Biometric Applications . . . . .	332
Operation of a Biometric Authentication System . . . . .	333
Biometric Accuracy. . . . .	335
Threats to Biometric Authentication . . . . .	337
Security Controls for Biometric Authentication. . . . .	339
10.6 Risk Assessment for User Authentication . . . . .	341
Authenticator Assurance Levels. . . . .	341
Selecting an AAL. . . . .	342
Choosing an Authentication Method. . . . .	345
10.7 Access Control. . . . .	347
Subjects, Objects, and Access Rights . . . . .	348
Access Control Policies . . . . .	349
Discretionary Access Control. . . . .	350
Role-Based Access Control . . . . .	351
Attribute-Based Access Control . . . . .	353
Access Control Metrics. . . . .	358

10.8 Customer Access . . . . .	360
Customer Access Arrangements . . . . .	360
Customer Contracts . . . . .	361
Customer Connections . . . . .	361
Protecting Customer Data . . . . .	361
10.9 System Access Best Practices . . . . .	362
10.10 Key Terms and Review Questions . . . . .	363
Key Terms . . . . .	363
Review Questions . . . . .	363
10.11 References . . . . .	364
<b>Chapter 11: System Management</b>	<b>366</b>
11.1 Server Configuration . . . . .	368
Threats to Servers . . . . .	368
Requirements for Server Security . . . . .	368
11.2 Virtual Servers . . . . .	370
Virtualization Alternatives . . . . .	371
Virtualization Security Issues . . . . .	374
Securing Virtualization Systems . . . . .	376
11.3 Network Storage Systems . . . . .	377
11.4 Service Level Agreements . . . . .	379
Network Providers . . . . .	379
Computer Security Incident Response Team . . . . .	381
Cloud Service Providers . . . . .	382
11.5 Performance and Capacity Management . . . . .	383
11.6 Backup . . . . .	384
11.7 Change Management . . . . .	386
11.8 System Management Best Practices . . . . .	389

11.9 Key Terms and Review Questions . . . . .	390
Key Terms . . . . .	390
Review Questions . . . . .	390
11.10 References . . . . .	391
<b>Chapter 12: Networks and Communications</b>	<b>392</b>
12.1 Network Management Concepts . . . . .	393
Network Management Functions. . . . .	393
Network Management Systems. . . . .	399
Network Management Architecture. . . . .	402
12.2 Firewalls . . . . .	404
Firewall Characteristics. . . . .	404
Types of Firewalls . . . . .	406
Next-Generation Firewalls . . . . .	414
DMZ Networks. . . . .	414
The Modern IT Perimeter . . . . .	416
12.3 Virtual Private Networks and IP Security . . . . .	417
Virtual Private Networks . . . . .	417
IPsec. . . . .	418
Firewall-Based VPNs. . . . .	420
12.4 Security Considerations for Network Management . . . . .	421
Network Device Configuration . . . . .	421
Physical Network Management . . . . .	423
Wireless Access . . . . .	426
External Network Connections. . . . .	427
Firewalls . . . . .	428
Remote Maintenance . . . . .	429

12.5 Electronic Communications . . . . .	430
Email . . . . .	430
Instant Messaging . . . . .	436
Voice over IP (VoIP) Networks . . . . .	438
Telephony and Conferencing . . . . .	444
12.6 Networks and Communications Best Practices . . . . .	444
12.7 Key Terms and Review Questions . . . . .	445
Key Terms . . . . .	445
Review Questions . . . . .	445
12.8 References . . . . .	446
<b>Chapter 13: Supply Chain Management and Cloud Security</b>	<b>448</b>
13.1 Supply Chain Management Concepts . . . . .	449
The Supply Chain . . . . .	449
Supply Chain Management . . . . .	451
13.2 Supply Chain Risk Management. . . . .	453
Supply Chain Threats . . . . .	456
Supply Chain Vulnerabilities . . . . .	459
Supply Chain Security Controls . . . . .	460
SCRM Best Practices . . . . .	463
13.3 Cloud Computing . . . . .	466
Cloud Computing Elements . . . . .	466
Cloud Computing Reference Architecture . . . . .	470
13.4 Cloud Security . . . . .	473
Security Considerations for Cloud Computing . . . . .	473
Threats for Cloud Service Users . . . . .	474
Risk Evaluation . . . . .	475
Best Practices . . . . .	476
Cloud Service Agreement. . . . .	477

13.5 Supply Chain Best Practices . . . . .	478
13.6 Key Terms and Review Questions . . . . .	479
Key Terms . . . . .	479
Review Questions . . . . .	479
13.7 References . . . . .	480
<b>Chapter 14: Technical Security Management</b>	<b>482</b>
14.1 Security Architecture . . . . .	483
14.2 Malware Protection Activities . . . . .	487
Types of Malware. . . . .	487
The Nature of the Malware Threat . . . . .	490
Practical Malware Protection . . . . .	490
14.3 Malware Protection Software . . . . .	494
Capabilities of Malware Protection Software . . . . .	494
Managing Malware Protection Software . . . . .	495
14.4 Identity and Access Management . . . . .	496
IAM Architecture . . . . .	497
Federated Identity Management . . . . .	498
IAM Planning . . . . .	500
IAM Best Practices . . . . .	501
14.5 Intrusion Detection. . . . .	502
Basic Principles. . . . .	503
Approaches to Intrusion Detection . . . . .	504
Host-Based Intrusion Detection Techniques. . . . .	505
Network-Based Intrusion Detection Systems. . . . .	506
IDS Best Practices . . . . .	508
14.6 Data Loss Prevention. . . . .	509
Data Classification and Identification . . . . .	509
Data States . . . . .	510

14.7 Digital Rights Management . . . . .	512
DRM Structure and Components. . . . .	513
DRM Best Practices . . . . .	515
14.8 Cryptographic Solutions . . . . .	517
Uses of Cryptography. . . . .	517
Cryptographic Algorithms. . . . .	518
Selection of Cryptographic Algorithms and Lengths . . . . .	525
Cryptography Implementation Considerations. . . . .	526
14.9 Cryptographic Key Management . . . . .	528
Key Types. . . . .	530
Cryptoperiod . . . . .	532
Key Life Cycle . . . . .	534
14.10 Public Key Infrastructure . . . . .	536
Public Key Certificates . . . . .	536
PKI Architecture. . . . .	538
Management Issues . . . . .	540
14.11 Technical Security Management Best Practices . . . . .	541
14.12 Key Terms and Review Questions . . . . .	543
Key Terms . . . . .	543
Review Questions . . . . .	543
14.13 References . . . . .	544
<b>Chapter 15: Threat and Incident Management</b>	<b>546</b>
15.1 Technical Vulnerability Management . . . . .	547
Plan Vulnerability Management . . . . .	547
Discover Known Vulnerabilities . . . . .	548
Scan for Vulnerabilities . . . . .	549
Log and Report . . . . .	551
Remediate Vulnerabilities . . . . .	551

15.2	Security Event Logging . . . . .	554
	Security Event Logging Objective . . . . .	556
	Potential Security Log Sources . . . . .	556
	What to Log . . . . .	557
	Protection of Log Data . . . . .	557
	Log Management Policy . . . . .	558
15.3	Security Event Management . . . . .	559
	SEM Functions . . . . .	560
	SEM Best Practices . . . . .	561
15.4	Threat Intelligence . . . . .	563
	Threat Taxonomy . . . . .	564
	The Importance of Threat Intelligence . . . . .	566
	Gathering Threat Intelligence . . . . .	568
	Threat Analysis . . . . .	569
15.5	Cyber Attack Protection . . . . .	570
	Cyber Attack Kill Chain . . . . .	570
	Protection and Response Measures . . . . .	573
	Non-Malware Attacks . . . . .	576
15.6	Security Incident Management Framework . . . . .	577
	Objectives of Incident Management . . . . .	579
	Relationship to Information Security Management System . . . . .	579
	Incident Management Policy . . . . .	580
	Roles and Responsibilities . . . . .	581
	Incident Management Information . . . . .	583
	Incident Management Tools . . . . .	583
15.7	Security Incident Management Process . . . . .	584
	Preparing for Incident Response . . . . .	585
	Detection and Analysis . . . . .	586



Containment, Eradication, and Recovery . . . . .	587
Post-Incident Activity . . . . .	588
15.8 Emergency Fixes . . . . .	590
15.9 Forensic Investigations. . . . .	592
Prepare. . . . .	593
Identify . . . . .	594
Collect . . . . .	594
Preserve . . . . .	595
Analyze. . . . .	595
Report. . . . .	596
15.10 Threat and Incident Management Best Practices . . . . .	597
15.11 Key Terms and Review Questions . . . . .	598
Key Terms . . . . .	598
Review Questions . . . . .	599
15.12 References . . . . .	599
<b>Chapter 16: Local Environment Management</b>	<b>602</b>
16.1 Local Environment Security. . . . .	602
Local Environment Profile. . . . .	603
Local Security Coordination . . . . .	604
16.2 Physical Security . . . . .	606
Physical Security Threats . . . . .	606
Physical Security Officer. . . . .	609
Defense in Depth. . . . .	610
Physical Security: Prevention and Mitigation Measures . . . . .	612
Physical Security Controls . . . . .	615
16.3 Local Environment Management Best Practices. . . . .	619

16.4 Key Terms and Review Questions . . . . .	620
Key Terms . . . . .	620
Review Questions . . . . .	620
16.5 References . . . . .	621
<b>Chapter 17: Business Continuity</b>	<b>622</b>
17.1 Business Continuity Concepts . . . . .	625
Threats . . . . .	626
Business Continuity in Operation. . . . .	628
Business Continuity Objectives . . . . .	629
Essential Components for Maintaining Business Continuity . . . . .	630
17.2 Business Continuity Program . . . . .	630
Governance . . . . .	631
Business Impact Analysis. . . . .	631
Risk Assessment. . . . .	632
Business Continuity Strategy . . . . .	634
17.3 Business Continuity Readiness. . . . .	637
Awareness . . . . .	637
Training. . . . .	638
Resilience. . . . .	639
Control Selection. . . . .	640
Business Continuity Plan . . . . .	642
Exercising and Testing . . . . .	647
Performance Evaluation . . . . .	650
17.4 Business Continuity Operations . . . . .	655
Emergency Response. . . . .	655
Crisis Management . . . . .	656
Business Recovery/Restoration. . . . .	657

17.5 Business Continuity Best Practices . . . . .	660
17.6 Key Terms and Review Questions . . . . .	661
Key Terms . . . . .	661
Review Questions . . . . .	661
17.7 References . . . . .	662

## **Part III: Security Assessment 665**

### **Chapter 18: Security Monitoring and Improvement 666**

18.1 Security Audit . . . . .	666
Security Audit and Alarms Model. . . . .	667
Data to Collect for Auditing . . . . .	668
Internal and External Audit . . . . .	672
Security Audit Controls . . . . .	673
18.2 Security Performance . . . . .	678
Security Performance Measurement . . . . .	678
Security Monitoring and Reporting . . . . .	686
Information Risk Reporting. . . . .	688
Information Security Compliance Monitoring . . . . .	690
18.3 Security Monitoring and Improvement Best Practices . . . . .	691
18.4 Key Terms and Review Questions . . . . .	692
Key Terms . . . . .	692
Review Questions . . . . .	692
18.5 References . . . . .	693

### **Appendix A: References and Standards 694**

### **Appendix B: Glossary 708**

### **Index 726**

### **Appendix C (Online Only): Answers to Review Questions**

You can find Appendix C at [informit.com/title/9780134772806](http://informit.com/title/9780134772806).  
Click the Downloads tab to access the PDF file.

## Preface

*There is the book, Inspector. I leave it with you, and you cannot doubt that it contains a full explanation.*

—*The Adventure of the Lion's Mane*, by Sir Arthur Conan Doyle

---

## Background

Effective cybersecurity is very difficult. A number of organizations, based on wide professional input, have developed best-practices types of documents as well as standards for implementing and evaluating cybersecurity. On the standards side, the most prominent player is the National Institute of Standards and Technology (NIST). NIST has created a huge number of security publications, including 9 Federal Information Processing Standards (FIPS) and well over 100 active Special Publications (SP) that provide guidance on virtually all aspects of cybersecurity. Equally important is the International Organization for Standardization (ISO) 27000 series of standards on information security management systems. Other organizations that have produced cybersecurity standards and guidelines include:

- **ISACA/COBIT:** The COBIT-5 for information security and related documents are widely used by the industry.
- **ITU Telecommunication Standardization Sector (ITU-T):** Most important are the series X.1050 through X.1069 on security management.
- **Internet Society (ISOC):** A number of published standards and RFCs relate to cybersecurity.

In addition, a number of professional and industry groups have produced best-practices documents and guidelines. The most important such document is *The Standard of Good Practice for Information Security* (SGP), produced by the Information Security Forum (ISF). This almost 300-page document provides a wide range of best practices based on the consensus of industry and government organizations. Another key organization is the Center for Internet Security (CIS), which has published detailed lists of industry-approved security controls and metrics. Other respected organizations have also produced a number of similar documents.

Thus, there is an immense amount of practical, widely accepted material available. The problem is that the amount of information is so massive that it is difficult for cybersecurity practitioners to take advantage of it to build and maintain effective cybersecurity systems and policies.

The objective of this book is to organize, consolidate, and explain all this material to enable the security practitioner to make effective use of it.

This book is addressed to people in both IT and security management, people tasked with maintaining IT security, and a wide range of others interested in cybersecurity and information security.

## Organization of the Book

The book consists of three parts:

- **Part I, “Planning for Cybersecurity”:** This part of the book provides guidelines for effectively managing the cybersecurity mission, including security governance and security requirements. The ISF defines *security governance* as “the framework by which policy and direction is set, providing senior management with assurance that security management activities are being performed correctly and consistently.” Part I of this book provides guidance in developing a set of risk and security requirements to ensure that there are no gaps in an organization's cybersecurity practices.
- **Part II, “Managing the Cybersecurity Function”:** This part of the book examines in detail the security controls intended to satisfy the defined security requirements. The 13 chapters in this part encompass the broad range of management, operational, and technical means used to achieve effective cybersecurity.
- **Part III, “Security Assessment”:** This part of the book discusses techniques for auditing and monitoring the performance of cybersecurity controls, with a view to spotting gaps in the system and devising improvements.

## Supporting Websites

The author maintains a companion website at [WilliamStallings.com/Cybersecurity](http://WilliamStallings.com/Cybersecurity) that includes a list of relevant links organized by chapter and an errata sheet for the book.

The author also maintains the Computer Science Student Resource Site at [ComputerScienceStudent.com](http://ComputerScienceStudent.com). The purpose of this site is to provide documents, information, and links for computer science students and professionals. Links and documents are organized into seven categories:

- **Math:** Includes a basic math refresher, a queuing analysis primer, a number system primer, and links to numerous math sites.
- **How-to:** Provides advice and guidance for solving homework problems, writing technical reports, and preparing technical presentations.
- **Research resources:** Provides links to important collections of papers, technical reports, and bibliographies.
- **Other useful:** Provides a variety of other useful documents and links.
- **Computer science careers:** Lists useful links and documents for those considering a career in computer science.



WilliamStallings.  
com/Cybersecurity  
Companion website



ComputerScience  
Student.com  
Computer Science  
Student  
Resource Site

- **Writing help:** Provides help in becoming a clearer, more effective writer.
- **Miscellaneous topics and humor:** You have to take your mind off your work once in a while.

## Register This Book

Register your copy of *Effective Cybersecurity* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to [informit.com/register](http://informit.com/register) and log in or create an account. Enter the product ISBN (9780134772806) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

## Acknowledgments

This book has benefited from review by a number of people, who gave generously of their time and expertise. I especially thank Akhil Behl and Michael Shannon, who each devoted an enormous amount of time to a detailed review of the entire manuscript. I also thank the people who provided thoughtful reviews of the initial book proposal: Steven M. Bellovin, Kelley Dempsey, Charles A. Russell, Susan Sand, and Omar Santos.

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Sohail Awad, Vinay Banakar, Vilius Benetis, Rodrigo Ristow Branco, Michael Brown, Herve Carpentier, Jim Fenton, Adri Jovin, Joseph Kellegher, Adnan Kilic, Edward Lane, Junior Lazuardi, Matt Nichols, Omar Olivos, ShanShan Pa, Venkatesh Ramamoorthy, Antonius Ruslan, Jose Samuel, Jigar Savla, Matias Siri, and Dauda Sule. Nikhil Bhargava developed the review questions and answers.

Finally, I would like to thank the many people at Pearson responsible for the publication of the book. This includes the staff at Pearson, particularly Executive Editor Brett Bartow, Development Editor Marianne Bartow, and Senior Project Editor Lori Lyons. Thanks also to the marketing and sales staffs at Pearson, without whose efforts this book would not be in front of you.

With all this assistance, little remains for which I can take full credit. However, I am proud to say that, with no help whatsoever, I selected all the quotations.

## About the Author and Contributors

**Dr. William Stallings** has made a unique contribution to understanding the broad sweep of technical developments in computer security, computer networking, and computer architecture. He has authored 18 textbooks, and, counting revised editions, a total of 70 books on various aspects of these subjects.

His writings have appeared in numerous ACM and IEEE publications, including the *Proceedings of the IEEE* and *ACM Computing Reviews*. He has 13 times received the award for the best computer science textbook of the year from the Text and Academic Authors Association.

With more than 30 years in the field, he has been a technical contributor, a technical manager, and an executive with several high-technology firms. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from micro-computers to mainframes. Currently, he is an independent consultant whose clients have included computer and networking manufacturers and customers, software development firms, and leading-edge government research institutions.

He created and maintains the Computer Science Student Resource Site at [ComputerScienceStudent.com](http://ComputerScienceStudent.com). This site provides documents and links on a variety of subjects of general interest to computer science students (and professionals). He is a member of the editorial board of *Cryptologia*, a scholarly journal devoted to all aspects of cryptology.

Dr. Stallings holds a Ph.D. from M.I.T. in computer science and a B.S. from Notre Dame in electrical engineering.

## Technical Editors

**Akhil Behl**, CCIE No. 19564, is a passionate IT executive with a key focus on cloud and security. He has more than 15 years of experience in the IT industry, working in several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specialization includes cloud, security, infrastructure, data center, and business communication technologies.

Akhil is a published author. Over the past few years, Akhil has authored multiple titles on security and business communication technologies. He has contributed as a technical editor for more than a dozen books on security, networking, and information technology. He has published several research papers in national and international journals, including IEEE Xplore, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passions.

Akhil holds CCIE (Collaboration and Security), CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and a master's in business administration.

**Michael J. Shannon** began his IT career when he transitioned from being a recording studio engineer to a network technician for a major telecommunications company in the early 1990s. He soon began to focus on security and was one of the first 10 people to attain the HIPAA Certified Security Specialist designation. Throughout his 30 years in IT, he has worked as an employee, a contractor, a trainer, and a consultant for a number of companies, including Platinum Technologies, Fujitsu, IBM, State Farm, Pearson, MindSharp, Thomson/NetG, and Skillsoft. Mr. Shannon has authored several books and training manuals, published articles, and produced dozens of CBT titles over the years as well. For security purposes, he has attained the CISSP, CCNP Security, SSCP, Security+, and ITIL Intermediate SO and RCV certifications. He is also a licensed insurance agent, specializing in cyber insurance on behalf of large insurers and numerous companies throughout Texas.



# Chapter 2

## Security Governance

*A prince or general can best demonstrate his genius by managing a campaign exactly to suit his objectives and his resources, doing neither too much nor too little. But the effects of genius show not so much in novel forms of action as in the ultimate success of the whole.*

—On War, Carl Von Clausewitz

---

### *Learning Objectives*

**After studying this chapter, you should be able to:**

- Explain the concept of security governance and how it differs from security management.
- Provide an overview of the key components of security governance.
- Discuss the topics that should be covered in a strategic security plan.
- Discuss the topics that should be covered in an information security report.
- Explain the roles and responsibilities that are part of security governance.
- Present an overview of the concepts of information security architecture.
- Present an overview of security governance best practices.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, defines information security governance as follows:

#### **Information security governance**

The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

ITU-T X.1054, *Governance of Information Security*, defines information security governance as “the system by which an organization’s information security-related activities are directed and controlled.”

More generally, the term *security governance* encompasses **governance** concerns for cybersecurity, information security, and network security.

### **governance**

Establishment of policies and continuous monitoring of their proper implementation by the members of the governing body of an organization. Governance includes the mechanisms required to balance the powers of the members (with the associated accountability) and their primary duty of enhancing the prosperity and viability of the organization.

## **2.1 Security Governance and Security Management**

To better understand the role of security governance, it is useful to distinguish between information security governance (previously defined), information security management, and information security implementation/operations. ISO 27000 defines **information security management** as follows:

The supervision and making of decisions necessary to achieve business objectives through the protection of the organization’s information assets. Management of information security is expressed through the formulation and use of information security policies, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

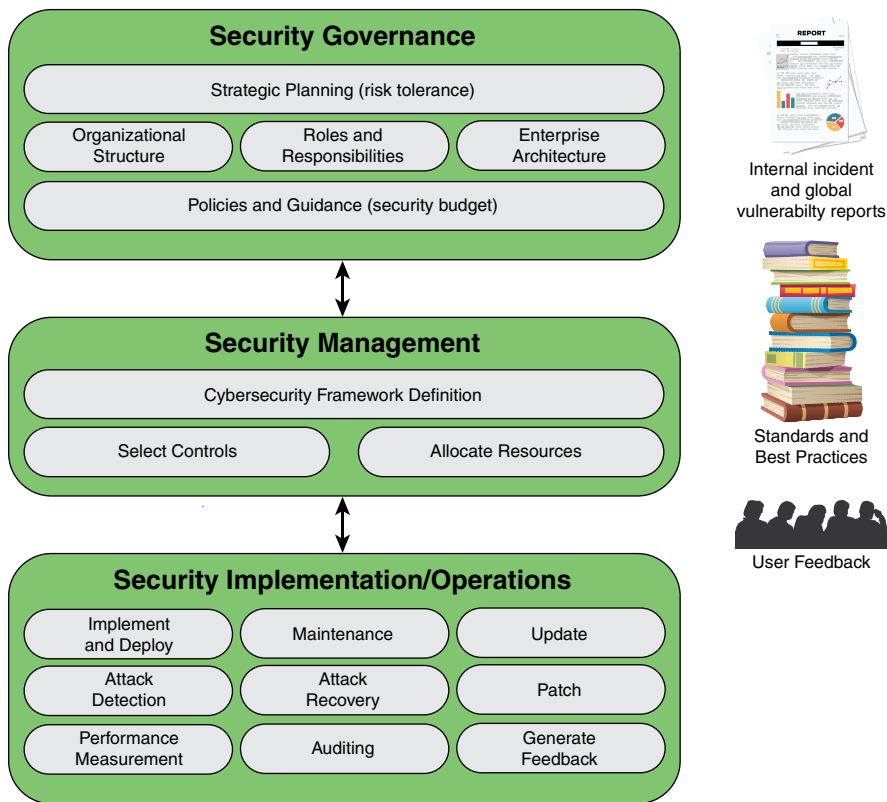
And **information security implementation/operations** can be defined in this fashion:

The implementation, deployment and ongoing operation of security controls defined within a cybersecurity framework.

Figure 2.1 suggests the hierarchical relationship between these three concepts. The security governance level communicates the mission priorities, available resources, and overall risk tolerance to the security management level. In essence, security governance is the process of developing a **security program** that adequately meets the strategic needs of the business. The security management level uses the information as inputs into the risk management process that realizes the security program. It then collaborates with the implementation/operations level to communicate security requirements and create a cybersecurity profile. The implementation/operations level integrates this profile into the system development life cycle and continuously monitors security performance. It executes or manages security-related processes related to current infrastructure on a day-to-day basis. The security management level uses monitoring information to assess the current profile and reports the outcomes of that assessment to the governance level to inform the organization’s overall risk management process.

### **security program**

The management, operational, and technical aspects of protecting information and information systems. A security program encompasses policies, procedures, and management structure and mechanism for coordinating security activity.



**FIGURE 2.1** Information Security Management System Element

Figure 2.1 illustrates the key responsibilities at each level. As indicated, there is interaction among the three layers in the ongoing evolution of the information security management system (ISMS). In addition, three supplemental factors play roles. Internal security incident reports and global vulnerability reports from various sources help define the threat and level of risk that the organization faces in protecting its information assets. The numerous standards and best practices documents provide guidance on managing risk. User feedback comes from both internal users and external users who have access to the organization's information assets. This feedback helps improve the effectiveness of policies, procedures, and technical mechanisms. Depending on the organization and its cybersecurity approach, each of the three factors plays a role to a greater or lesser extent at each level.

This chapter is devoted to security governance. Chapter 3, "Information Risk Assessment," covers security management, and the succeeding chapters cover security implementation/operations.

## 2.2 Security Governance Principles and Desired Outcomes

Before getting into the details of security governance, an overview of principles and desired outcomes provides useful context.

### Principles

X.1054 provides concepts and guidance on principles and processes for information security governance, by which organizations evaluate, direct, and monitor the management of information security. X.1054 lays out as a key objective of information security governance the alignment of information security objectives and strategy with overall business objectives and strategy. X.1054 lists six principles for achieving this objective:

- **Establish organizationwide information security.** Information security, or cybersecurity, concerns should permeate the organization's structure and functions. Management at all levels should ensure that information security is integrated with **information technology (IT)** and other activities. Top-level management should ensure that information security serves overall business objectives and should establish responsibility and accountability throughout the organization.
- **Adopt a risk-based approach.** Security governance, including allocation of resources and budgets, should be based on the risk appetite of an organization, considering loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss.
- **Set the direction of investment decisions.** Information security investments are intended to support organizational objectives. Security governance entails ensuring that information security is integrated with existing organization processes for capital and operational expenditure, for legal and regulatory compliance, and for risk reporting.
- **Ensure conformance with internal and external requirements.** External requirements include mandatory legislation and regulations, standards leading to certification, and contractual requirements. Internal requirements comprise broader organizational goals and objectives. Independent security audits are the accepted means of determining and monitoring conformance.
- **Foster a security-positive environment for all stakeholders.** Security governance should be responsive to **stakeholder** expectations, keeping in mind that various stakeholders can have different values and needs. The governing body

#### information technology (IT)

Applied computer systems, both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. IT is often the name of the part of an enterprise that deals with all things electronic.

#### stakeholder

A person, a group, or an organization that has interest or concern in an organization. Stakeholders can affect or can be affected by the organization's actions, objectives, and policies. Some examples of stakeholders are creditors, directors, employees, government (and its agencies), owners (shareholders), suppliers, unions, and the community from which the business draws its resources.

should take the lead in promoting a positive information security culture, which includes requiring and supporting security education, training, and awareness programs.

- **Review performance in relation to business outcomes.** From a governance perspective, security performance encompasses not just effectiveness and efficiency but also impact on overall business goals and objectives. Governance executives should mandate reviews of a performance measurement program for monitoring, audit, and improvement that links information security performance to business performance.

Adherence to these principles is essential to the success of information security in the long term. How these principles are to be satisfied and who is responsible and accountable depend on the nature of the organization.

## **Desired Outcomes**

The IT Governance Institute defines five basic outcomes of information security governance that lead to successful integration of information security with the organization's mission [ITGI06]:

- **Strategic alignment:** The support of strategic organizational objectives requires that information security strategy and policy be aligned with business strategy.
- **Risk management:** The principal driving force for information security governance is risk management, which involves mitigating risks and reducing or preventing potential impact on information resources.
- **Resource management:** The resources expended on information security (e.g., personnel time and money) are somewhat open ended and a key goal of information security governance is to align information security budgets with overall enterprise requirements.
- **Value delivery:** Not only should resources expended on information security be constrained within overall enterprise resource objectives, but also information security investments need to be managed to achieve optimum value.
- **Performance measurement:** The enterprise needs metric against which to judge information security policy to ensure that organizational objectives are achieved.

It is worthwhile to keep these outcomes in mind throughout the discussion in the remainder of the chapter.

## 2.3 Security Governance Components

SP 800-100 lists the following key activities, or components that constitute effective security governances (refer to Figure 2.1):

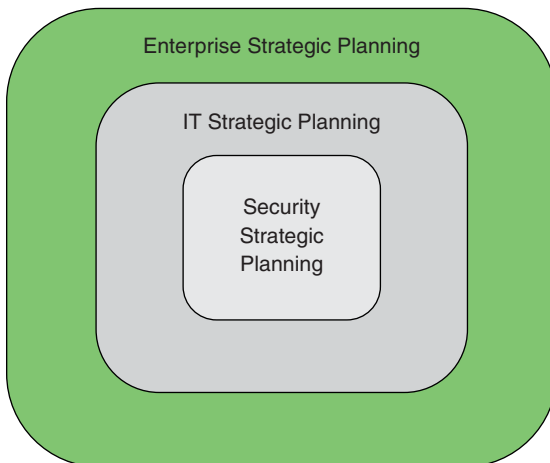
- Strategic planning
- Organizational structure
- Establishment of roles and responsibilities
- Integration with the enterprise architecture
- Documentation of security objectives in policies and guidance

The following sections examine each of these components in turn.

### Strategic Planning

It is useful for this discussion to define three hierarchically related aspects of strategic planning (see Figure 2.2):

- Enterprise strategic planning
- Information technology (IT) strategic planning
- Cybersecurity or information security strategic planning



**FIGURE 2.2** Strategic Planning

*Enterprise strategic planning* involves defining long-term goals and objectives for an organization (for example, business enterprise, government agency, or nonprofit

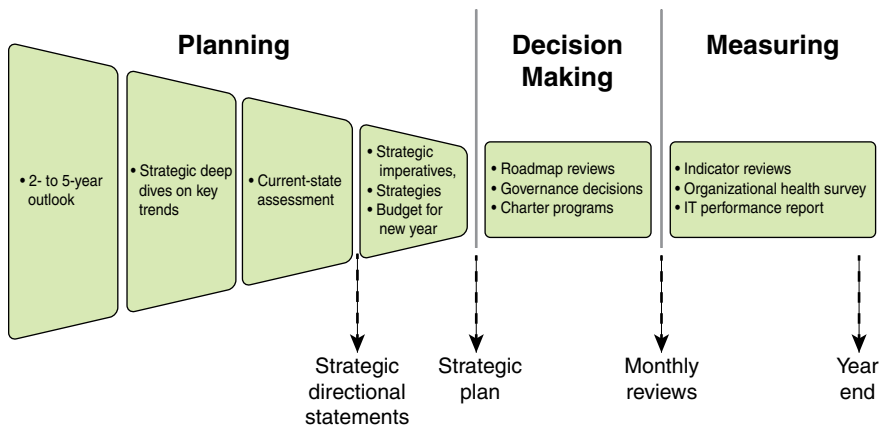
**strategic plan**

A document used to communicate, within the organization, the organization's goals, the actions needed to achieve those goals, and all the other critical elements developed during planning exercises.

organization) and the development of plans to achieve these goals and objectives. The management activity involved in enterprise strategic planning is described in the Strategic Management Group's *Strategic Planning Basics* [SMG17] as an activity used to set priorities, focus energy and resources, strengthen operations, ensure that employees and other stakeholders are working toward common goals, establish agreement around intended outcomes/results, and assess and adjust the organization's direction in response to a changing environment. It involves the development of a **strategic plan** and the ongoing oversight of the implementation of that plan.

*IT strategic planning* is the alignment of IT management and operation with enterprise strategic planning. The need to move beyond IT management and to ensure that the IT planning process is integrated with enterprise strategic planning follows from two strategic factors: mission necessity and enterprise maturity [JUIZ15]. With many actors exploiting IT to maximize effectiveness, an organization must engage in strategic planning to ensure that investments in IT produce business value and that the assessment of risks is aligned with enterprise goals and objectives. This is a necessity to support the overall enterprise mission. Further, as the IT infrastructure develops and matures, meeting enterprise strategic goals is likely to involve new arrangements with outside providers, such as cloud service providers, more use of mobile devices by employees and outside actors, and perhaps reliance on a variety of new hardware and software to develop Internet of Things (IoT) capability. These activities may create unintended barriers to flexibility and introduce new areas of risk. IT management must be guided by strategic planning to meet these challenges.

One of the best-documented examples of IT strategic planning is the process used at Intel [HAYD08a, HAYD08b, PETE12]. It is worth examining this model because it also serves as a model for security strategic planning. Intel's IT strategic planning process comprises six phases, as shown in Figure 2.3.



**FIGURE 2.3** Intel's IT Strategic Planning Process

The six phases are as follows:

1. **Two- to five-year business and technology outlook:** At the beginning of the year, the planning team takes as input an overall vision and mission statement developed at the enterprise level. During this phase, the team reviews the enterprise strategies, technology trends, employee trends, and so on to better understand the future environment that will shape the IT organization and its deliverables. IT subject matter experts from throughout the organization are recruited to help define the major trends that may be critical in shaping the organization and its decision making in the next few years.
2. **Strategic deep dive:** The team identifies a small number of high-impact areas that require more in-depth analysis to inform the overall strategic planning process. Depending on circumstances at a given point in time, these may include IoT, social media trends, and changing regulatory compliance rules.
3. **Current-state assessment:** The planning team analyzes the current state of all the IT-related systems and policies and compares these with the long-range outlook, paying special attention to the key drivers developed in the preceding phase. The result is a set of recommendations for adjustments to IT's focus areas and spending plans.
4. **Imperatives, roadmaps, and finances:** The next phase is the development of a strategic plan for IT. The plan includes a discussion of strategic objectives and a budget and investment plan. The plan reflects IT's highest-priority items and provides an outcome framework for defining success. Each item includes a roadmap that can influence budget and organization decisions in the upcoming year.
5. **Governance process and decision making:** Once the annual budget is approved, the information from the preceding phases is used to guide the governance process and the many decisions made across the organization to implement the strategic plan and one-year strategic objectives. These decisions include project chartering, supplier selection, sourcing, investment trade-off decisions, and so on.
6. **Regular reviews:** Monthly reviews based on a wide variety of input help ensure that the strategic plan and governance decisions are followed. This culminates in a year-end assessment. Reviews continue into the following year until a new strategic plan and new governance decisions provide input for modifying the review process.

This process can include a security strategic planning component, or planning can occur in a coordinated and parallel fashion in another team.



**Information security strategic planning** is alignment of information security management and operation with enterprise and IT strategic planning. The pervasive use and value of IT within organizations has resulted in an expanded notion of IT's delivery of value to the organization to include mitigation of the organization's risk [ZIA15]. Accordingly, IT security is a concern at all levels of an organization's governance and decision-making processes, and information security strategic planning is an essential component of strategic planning.

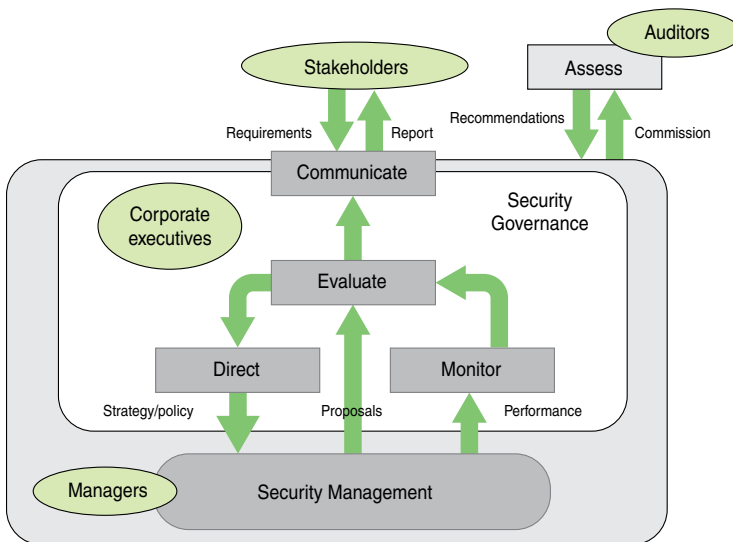
An information security strategic plan should be embodied in a document that is approved by the appropriate executives and committees and is regularly reviewed. Table 2.1 suggests an outline for such a document.

**TABLE 2.1** Elements of a Strategic Plan Document

Section	Description
<b>Definition</b>	
Mission, vision, and objectives	Defines the strategy for aligning the information security program with organizational goals and objectives, including the role of individual security projects in enabling specific strategic initiatives.
Priorities	Describes factors that determine strategy and the priorities of objectives.
Success criteria	Defines success criteria for the information security program. Includes risk management, resilience, and protection against adverse business impacts.
Integration	Strategy for integrating the security program with the organization's business and IT strategy.
Threat defense	Describes how the security program will help the organization defend against security threats.
<b>Execution</b>	
Operations plan	An annual plan to achieve agreed objectives that involves agreeing on budgets, resources, tools, policies, and initiatives. This plan (a) can be used for monitoring progress and communicating with stakeholders and (b) ensures that information security is included from the outset in each relevant project.
Monitoring plan	This plan involves planning and maintaining a stakeholder feedback loop, measuring progress against objectives, and ensuring that strategic objectives remain valid and in line with business needs.
Adjustment plan	This plan involves ensuring that strategic objectives remain valid and in line with business needs as well as procedures to communicate the value.
<b>Review</b>	
Review plan	This plan describes procedures and individuals/committees involved in regular review of the information security strategy.

## Organizational Structure

The organizational structure to deal with cybersecurity depends, in large part, on the size of the organization, its type (for example, government agency, business, nonprofit), and the organization's degree of dependence on IT. But the essential security governance functions to be performed are in essence the same across organizations. Figure 2.4, which is based on a figure in X.1054, illustrates these basic functions within a broader context.



**FIGURE 2.4** Framework for Security Governance

The basic security governance functions are as follows:

- **Direct:** Guiding security management from the point of view of enterprise strategies and risk management. This function involves developing an information security policy.
- **Monitor:** Monitoring the performance of security management with measurable indicators.
- **Evaluate:** Assessing and verifying the results of security performance monitoring in order to ensure that objectives are met and to determine future changes to the ISMS and its management.
- **Communicate:** Reporting enterprise security status to stakeholders and evaluating stakeholder requirements.

This framework includes the governing cycle to direct, monitor, and evaluate the ISMS. The evaluation incorporates both the results of the monitoring and proposals from security management to dictate changes and improvements. This cycle is in accordance with Requirement 4.4 in ISO 27001 that the organization shall establish, implement, maintain, and continually improve an ISMS.

The evaluate function triggers communication with stakeholders in the form of a report, which can be issued annually, more frequently, or based on a security incident. As indicated in the Information Security Governance Framework [OHKI09], reporting to stakeholders serves two purposes:

- **Accountability:** Reporting enables stakeholders to ensure that information security is being managed effectively, and it should include the following:
  - Information security policy
  - Risk evaluation
  - Risk measures and response
  - Management systems
- **Effect on corporate value:** Reporting should disclose the following:
  - Estimates of the costs and benefits of making an inventory of information assets. The information security risk assessment process includes making a complete inventory of information assets. This inventory may support improved strategic management of the information assets, apart from security concerns, which may enhance corporate value.
  - Estimates of the value of an inventory of information assets that is developed as a result of information security activities.
  - The extent to which information security activities increase the brand value as well as the trust of the customers and partners.
  - The economic value of protected information assets.
  - The amount by which the security implementation reduces the risk of damaging the information assets.

The following sidebar provides an example of an information security report outline, from the Information Security Governance Framework [OHKI09]. This report structure is based on a study of private companies by the Japanese Ministry of Economics, Trade and Industry. It gives an overall picture of the enterprise's information security governance. Section 5, in particular, involves providing a status update, which should be in sufficient detail for stakeholders to determine whether information security activities are being carried out as planned.

### **Information Security Report**

**(1) Basic Information**

Includes the purpose of issue of the report, cautions relating to usage, target periods and responsible departments.

**(2) Concept of Management Regarding Information Security**

Includes policy regarding information-security undertakings, target scope, ranking of stakeholders in the report and messages to stakeholders.

**(3) Information Security Governance**

Information security management system (e.g., placement of responsibility, organizational structure and compliance), risks relating to information security and information security strategy.

**(4) Information Security Measures Planning and Goals**

Includes action plan and target values.

**(5) Results and Evaluation of Information Security Measures**

Includes results, evaluation, information security quality improvement activities, management of overseas bases, outsourcing, social contribution activities relating to information security and accident reports.

**(6) Principle Focal Themes Relating to Information Security**

Includes internal controls and protection of personal information, undertakings to be particularly emphasized such as Business Continuity Plans, introduction to themes and newly devised points.

**(7) Third-Party Approval, Accreditation, etc. (if Required)**

Includes ISMS compliance evaluation system, information security audits, privacy mark systems, number of persons with information security qualifications, classification, and ranking.

X.1054 provides an example of information security status report structure that includes the following detailed contents:

- Introduction
  - Scope (strategy, policies, standards), perimeter (geographic/organizational units), period covered (month/quarter/six months/year)
- Overall status
  - Satisfactory/not yet satisfactory/unsatisfactory

- Updates (as appropriate and relevant)
  - Progress toward achieving the information security strategy
  - Elements completed/in-hand/planned
  - Changes in information security management system
  - ISMS policy revision, organizational structure to implement ISMS (including assignment of responsibilities)
  - Progress toward certification
  - ISMS (re)certification, certified information security audits
  - Budgeting/staffing/training
  - Financial situation, headcount adequacy, information security qualifications
  - Other information security activities
  - Business continuity management involvement, awareness campaigns, internal/external audit assistance
- Significant issues (if any)
  - Results of information security reviews
  - Recommendations, management responses, action plans, target dates
  - Progress in respect of major internal/external audit reports
  - Recommendations, management responses, action plans, target dates
  - Information security incidents
  - Estimated impact, action plans, target dates
  - Compliance (or noncompliance) with related legislation and regulations
  - Estimated impact, action plans, target dates
- Decision(s) required (if any)
  - Additional resources
  - To enable information security to support business initiative(s)

Such an outline is particularly useful for organizations that expect to enhance their reputation by emphasizing their security (for example, information and communications technology businesses). Transparency of the organization's approach to its security risk and appropriate disclosure is also effective at increasing trust. Common awareness can be shared among stakeholders through such activities. For example,

public cloud service providers share considerable detail about the information security program and even go the extent of allowing customers to conduct audits and vulnerability testing with prior arrangement. Other service providers and organizations with business customers traditionally did not provide this level of transparency.

Finally, the assess function depicted in Figure 2.4 is performed by independent third-party auditors, commissioned by enterprise top management.

## Roles and Responsibilities

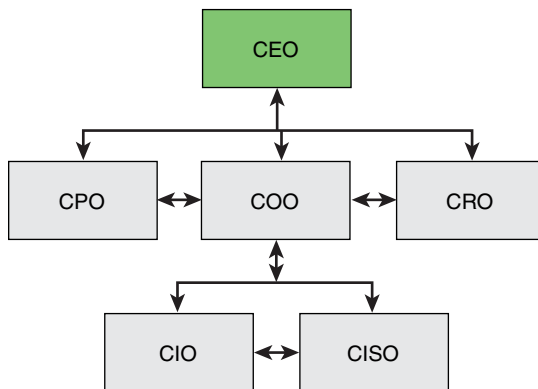
A key aspect of security governance is defining the roles and responsibilities of executives related to information security. Typically, these are **C-level** executives. Executive positions that play a role in security governance include the following:

- **Chief executive officer (CEO):** Responsible for the success or failure of the organization, overseeing the entire operation at a high level.
- **Chief operating officer (COO):** Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations.
- **Chief information officer (CIO):** In charge of IT strategy and the computer, network, and third-party (for example, cloud) systems required to support the enterprise's objectives and goals.
- **Chief security officer (CSO) or chief information security officer (CISO):** Tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security and a CISO in charge of digital security.
- **Chief risk officer (CRO):** Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings. This role does not exist in most enterprises. It is most often found in financial service organizations. In enterprises in which a CRO is not present, organizational risk decisions may be the responsibility of the CEO or board of directors.
- **Chief privacy officer (CPO):** Charged with developing and implementing policies designed to protect employee and customer data from unauthorized access.

### C-level

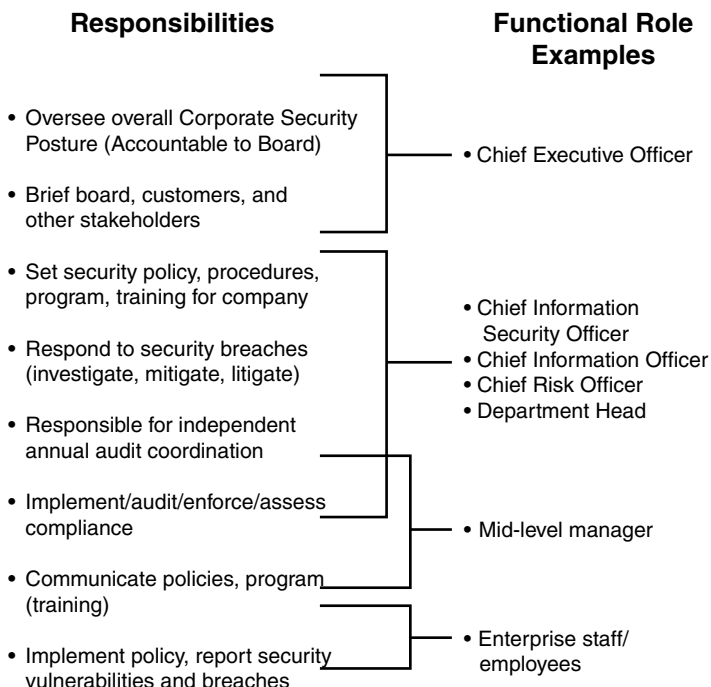
Chief level. Refers to high-ranking executives in an organization. Officers who hold C-level positions set the company's strategy, make high-stakes decisions, and ensure that the day-to-day operations align with fulfilling the company's strategic goals.

Figure 2.5 shows an example of reporting relationships among these roles for a large enterprise. In smaller organizations, a number of these roles may be assumed by a single individual.



**FIGURE 2.5** Possible Reporting Relationships for Security Governance

Two breakdowns of responsibility are useful in showing how to structure security-related roles in an organization. Figure 2.6, based on one in the Corporate Governance Task Force's *Information Security Governance: A Call to Action* [CGTF04], shows a recommended assignment of roles and responsibilities. This useful report also provides a more detailed discussion of these roles as well as a list of recommendations for implementing effective security governance.



**FIGURE 2.6** Security Governance Roles and Responsibilities Example

The Business Software Alliance's *Information Security Governance: Toward a Framework for Action* [BSA03] proposes a governance framework based on three categories (see Table 2.2):

- **Governance/business drivers:** What am I required to do? What should I do?
- **Roles and responsibilities:** How do I accomplish my objectives?
- **Metrics/audit:** How effectively do I achieve my objectives? What adjustments do I need to make?

**TABLE 2.2** Information Security Governance Responsibilities

Governance/ Business Drivers	Roles and Responsibilities	Metrics/Audit
<b>Corporate Executive</b>		
Legislation, ROI	<ul style="list-style-type: none"> <li>■ Provide oversight and coordination of policies</li> <li>■ Provide oversight of business unit compliance</li> <li>■ Ensure compliance reporting</li> <li>■ Monitor actions to enforce accountability</li> </ul>	Financial reporting, monetizing losses, conforming to policies
<b>Business Unit Head</b>		
Standards, policies, budgets	<ul style="list-style-type: none"> <li>■ Provide information security protection commensurate with the risk and business impact</li> <li>■ Provide security training</li> <li>■ Develop the controls environment and activities</li> <li>■ Report on effectiveness of policies, procedures, and practices</li> </ul>	Policy violations, misuse of assets, internal control violations
<b>Senior Manager</b>		
Standards, audit results	<ul style="list-style-type: none"> <li>■ Provide security for information and systems</li> <li>■ Periodic assessments of assets and their associated risks</li> <li>■ Determine level of security appropriate</li> <li>■ Implement policies and procedures to cost-effectively reduce risk to acceptable levels</li> <li>■ Perform periodic testing of security and controls</li> </ul>	Risk assessment and impact analysis, control environment activities, remedial actions, policy and procedure compliance, security and control test results



Governance/ Business Drivers	Roles and Responsibilities	Metrics/Audit
CIO/CISO		
Security policies, security operations, and resources	<ul style="list-style-type: none"><li>■ Develop, maintain, and ensure compliance with the program</li><li>■ Designate a security officer with primary duties and training</li><li>■ Develop required policies to support the security program and business-unit-specific needs</li><li>■ Assist senior managers with their security responsibilities</li><li>■ Conduct security awareness training</li></ul>	Security awareness effectiveness, incident response and impact analysis, security program effectiveness, information integrity, effects on information processing

**information security architecture**

An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans.

**architecture**

The way in which the component parts of an entity are arranged, organized, and managed.

Integration with Enterprise Architecture

A key element of security governance is the development of an **information security architecture**. This **architecture** provides information on how security capabilities (for example, identity and access management) are placed and used in the **enterprise architecture**. It allocates security requirements and controls to common services or infrastructures. It also provides a foundation for achieving risk-appropriate information system security, determining what circumstances and which security controls apply to information systems.

Over the past 20 years, a number of enterprise architecture models have been developed and adopted by various organizations. Two widely used governance resources for developing an information security architecture as part of an enterprise architecture are The Open Group Architecture Framework (TOGAF) [TOG11] and the Federal Enterprise Architecture Framework (FEAF) [OMB13]. The FEAF is the most comprehensive of all the enterprise architectures in use [SESS07], and this section provides an overview of it. Although developed for use by U.S. federal agencies, the FEAF is used effectively as a governance tool by other government organizations, private enterprises, nonprofit groups, and other organizations.

The FEAF provides the following:

- A perspective on how enterprise architectures are viewed in terms of sub-architecture domains
- Six reference models for describing different perspectives of the enterprise architecture
- A process for creating an enterprise architecture

- A transitional process for migrating from a pre-enterprise architecture to a post-enterprise architecture paradigm
- A taxonomy for cataloging assets that fall within the purview of the enterprise architecture
- An approach to measuring the success of using the enterprise architecture to drive business value

The sub-architecture domains represent specific areas of the overall framework. The domains provided a standardized language and framework for describing and analyzing investments and operations.

Each domain is defined in terms of a set of artifacts, which are essentially items of documentation that describe part or all of an architecture. [EAPA17] describes three levels of artifacts:

- **High-level artifacts:** These document strategic plans and objectives, typically in the form of policy statements and diagrams.
- **Mid-level artifacts:** These document organizational procedures and operations, such as services, supply chain elements, information flows, and IT and network architecture. Typical artifacts at this level are narrative description, flowcharts, spreadsheets, and diagrams.
- **Low-level EA artifacts:** These document the specific resources, such as applications, interfaces, data dictionaries, hardware, and security controls. Typical artifacts at this level are detailed technical specifications and diagrams.

The FEAF describes six domains:

- Strategy
- Business
- Data and information
- Enabling applications
- Host and infrastructure
- Security

Corresponding to the six domains are six reference models that describe the artifacts in the corresponding domains (see Table 2.3).

### **enterprise architecture**

The systems, infrastructure, operations, and management of all information technology throughout an enterprise. The architecture is typically organized as high-level internally compatible representations of organizational business models, data, applications, and information technology infrastructure.

**TABLE 2.3** Enterprise Architecture Reference Models

Reference Model	Elements	Goals/Benefits
Performance reference model	Goals, measurement areas, measurement categories	Improved organizational performance and governance, cost benefits
Business reference model	Mission sectors, functions, services	Organization transformation, analysis, design, and reengineering
Data reference model	Domain, subject, topic	Data quality/reuse, information sharing, Agile development
Application reference model	System, component, interface	Application portfolio management, cost benefits
Infrastructure reference model	Platform, facility, network	Asset management standardization, cost benefits
Security reference model	Purpose, risk, control	Secure business/IT environment

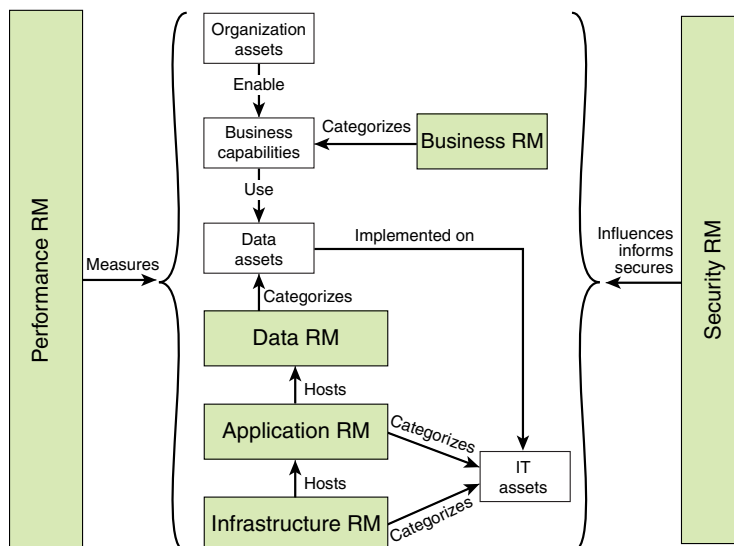
The following description provides further detail of the reference models (RMs):

- **Performance reference model (PRM):** Defines standard ways of describing the value delivered by enterprise architectures, linked to the strategy domain. An example of a PRM artifact for this domain is a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis report that presents the strengths, weaknesses/limitations, opportunities, and threats involved in a project or in a business venture, including risks and impacts.
- **Business reference model (BRM):** Describes an organization through a taxonomy of common mission and support service areas. The BRM provides guidance in defining functions and services in various mission sectors of the enterprise and is linked to the business services domain. An example of a BRM artifact for this domain is a use-case narrative and diagram that describes a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal.
- **Data reference model (DRM):** Facilitates discovery of existing data holdings residing in silos and enables understanding the meaning of the data, how to access it, and how to leverage it to support performance results. The DRM is linked to the data and information domain. An example of a DRM artifact for this domain is a data dictionary, which is a centralized repository of information about data such as name, type, range of values, source, and authorization for access for each data element in the organization's files and databases.
- **Application reference model (ARM):** Categorizes the system- and application-related standards and technologies that support the delivery of service capabilities. The ARM provides guidance in developing a uniform scheme for documenting system, components, and interfaces and for managing

application portfolios. It is linked to the enabling applications domain. An example of an ARM artifact for this domain is a system/application evolution diagram. This artifact documents the planned incremental steps toward migrating a suite of systems and/or applications to a more efficient suite, or toward evolving a current system or application to a future implementation.

- **Infrastructure reference model (IRM):** Categorizes the network- or cloud-related standards and technologies to support and enable the delivery of voice, data, video, and mobile service components and capabilities. The ARM provides guidance in developing a uniform scheme for documenting platform, facility, and network elements and managing assets. It is linked to the host infrastructure domain. An example of an IRM artifact for this domain is a hosting concept of operations, which presents the high-level functional architecture, organization, roles, responsibilities, processes, metrics, and strategic plan for hosting and use of hosting services. Other artifacts provide detailed documentation of infrastructure elements.
- **Security reference model (SRM):** Provides a common language and methodology for discussing security and privacy in the context of the organization's business and performance goals. The SRM provides guidance in risk-adjusted security/privacy protection and in the design and implementation of security controls. It is linked to the security domain. An example of an SRM artifact for this domain is a continuous monitoring plan, which describes the organization's process of monitoring and analyzing the security controls and reporting on their effectiveness.

Figure 2.7 illustrates the interactions among the reference models.

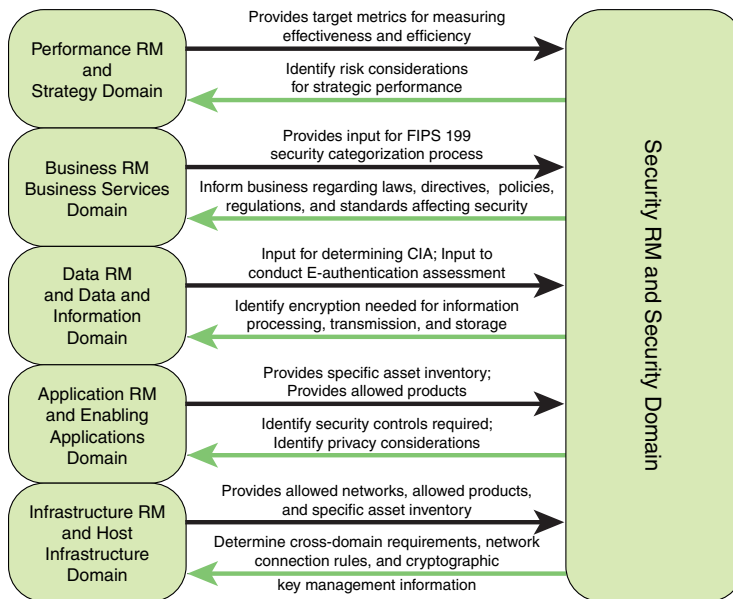


**FIGURE 2.7** Relationships Between RM Components

These reference models operate on four categories of assets:

- **Organization assets:** These assets include investments, programs, processes, applications, infrastructures, and individuals.
- **Business capabilities:** A business capability represents the ability of an organization to perform an activity that results in an outcome of value. A business capability can be viewed as an assembly of organization assets for a specific purpose.
- **Data assets:** Data assets include databases, files, and other data resources available to the organization.
- **IT assets:** IT assets include devices, peripherals, systems, applications, and IT capital investments.

Figure 2.8 shows in more detail the interaction between the security reference model and the other reference models.



**FIGURE 2.8** Interactions Between the Security Reference Model and Other Reference Models

An enterprise architecture is a powerful methodology for enabling enterprise and security governance, and it should be viewed as an essential element of governance.

## Policies and Guidance

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, defines an information security policy as an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. It is an essential component of security governance, providing a concrete expression of the security goals and objectives of the organization. The policies, together with guidance documents on the implementation of the policies, are put into practice through the appropriate selection of controls to mitigate identified risks. The policies and guidance need to cover information security roles and responsibilities, a baseline of required security controls, and guidelines for rules of behavior for all users of data and IT assets.

## 2.4 Security Governance Approach

Effective security governance requires the development and clear documentation of a framework, which is a structured approach for overseeing and managing risk for an enterprise. The implementation and ongoing use of the governance framework enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management.

### Security Governance Framework

The definition, monitoring, and maintenance of a security governance framework entails a number of tasks:

- Appoint a single executive to be ultimately responsible for security governance, whose duties including implementing the framework and developing and monitoring an information security strategy and security assurance program. The framework needs to encompass all of the elements discussed in Section 2.3.
- Decide and communicate to top executives the objectives of the security governance framework, including ensuring alignment with overall organization policies and goals, enhancing business value, and adequately managing risk.
- Ensure integration of the security architecture with the enterprise architecture, as discussed in Section 2.3.
- Include a process that enables the governing body to evaluate the operation of the information security strategy to ensure that it aligns with business needs the organization's current risk appetite.
- Regularly review the organization's risk appetite to ensure that it is appropriate for the current environment in which the organization operates.
- Formally approve the information security strategy, policy, and architecture.

## Security Direction

A governing body is responsible for ensuring that there is effective security direction. Typically, the governing body consists of those individuals ultimately responsible for what the organization does. In a publicly held company, for example, this is the board of directors, supplemented by executive managers who have operational responsibility for various business units.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) recommends that effective security direction be provided by a combination of a single individual responsible for information security supported by a governing body. The single individual is a CISO or equivalent executive. This individual's responsibilities include implementing the organization's overall approach and ensuring that a security mind-set permeates the organization. This latter requirement entails coordination and collaboration with executives, managers, and operations personnel.

The SGP also recommends that the governing body include the CISO and have a mission to support the CISO as well as review the activities that are under the CISO's direction. Other members of the governing body could include the CIO, key department heads, and heads of business support functions such as human resources. The governing body assists in the coordination of security activities and ensuring that the CISO has the resources and authority required to effect needed changes. In addition, the governing body reports security status and plans to the stakeholders.

COBIT 5 provides a more elaborate governing body structure than the SGP suggests, and it is worthwhile for larger organizations. COBIT 5 distinguishes five distinct roles/structures:

- **Chief information security officer (CISO):** The CISO has overall responsibility for the enterprise information security program. The CISO is the liaison between executive management and the information security program. The CISO should also work with key business stakeholders to address information protection needs. The CISO is responsible for:
  - Establishing and maintaining an ISMS
  - Defining and managing an information security risk treatment plan
  - Monitoring and reviewing the ISMS
- **Information security steering (ISS) committee:** This committee ensures, through monitoring and review, that good practices in information security are applied effectively and consistently throughout the enterprise. The ISS committee is responsible for enterprisewide information security decision making in support of strategic decisions made by the enterprise risk management committee.

- **Information security manager (ISM):** The ISM has overall responsibility for the management of information security efforts, including application security, infrastructure security, access management, threat and incident management, risk management, awareness program, metrics, and vendor assessments.
- **Enterprise risk management (ERM) committee:** This committee is responsible for the decision making of the enterprise to assess, control, optimize, finance, and monitor risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.
- **Information custodians/business owners:** These individuals serve as liaisons between the business and information security functions. They are associated with types of information, specific applications, or business units in an enterprise. They serve as trusted advisors and monitoring agents regarding information within the business.

COBIT 5 makes a distinction between the CISO and the ISM, with the CISO being a C-level position with oversight of an ISM, who has operational management responsibilities [ISAC08]. Other organizations combine the roles of CISO and ISM and may dispense with the CISO title.

Also, many organizations have a single security governing body, but COBIT 5 recommends a split into two committees for larger organizations. The ISS committee focuses on ensuring that security policies and practices are effectively implemented and monitored, and the ERM committee focuses on risk assessment. The suggested composition of the ISS committee is as follows:

- **CISO:** Serves as ISS committee chair and liaison to the ERM committee.
- **ISM:** Communicates design, implementation, and monitoring of practices.
- **Information custodians/business owners:** Are in charge of certain processes or business applications; responsible for communicating business initiatives that may impact information security and information security practices that may impact the user community.
- **IT manager:** Reports on the status of IT-related information security initiatives.
- **Representatives of specialist functions:** May include, permanently or as needed, representatives from internal audit, human resources, and legal departments.

The suggested composition of the ERM committee is as follows:

- **CISO:** Provides the committee with advice on specific information risks.
- **CEO, COO, CFO, etc.:** One or more representatives of senior executive management.



- **Information custodians/business owner:** Are in charge of certain processes or business applications; responsible for communicating business initiatives that may impact information security and information security practices that may impact the user community.
- **Audit/compliance representative:** Advises committee on compliance risk.
- **Legal representative:** Provides legal input.
- **CRO:** Advises on risk from strategic, financial, operational, reputational, and compliance perspectives.

## Responsible, Accountable, Consulted, and Informed (RACI) Charts

COBIT addresses the responsibility of all roles played by employees involved in IT governance actions. The COBIT responsibility model is formalized through a RACI chart matrix attached to all 34 COBIT processes. RACI explains what the responsibilities of all employees are regarding the key activities performance:

- **Responsible:** A person doing an activity and expected to deliver or submit the assigned work portion within the given deadlines. For example, in the case of software development project, developers are responsible.
- **Accountable:** A person with decision-making authority and who is expected to ensure the successful completion of project work. For example, a team leader or a project coordinator is accountable.
- **Consulted:** A stakeholder who should be included in any decision making or work activity by being consulted prior to the decision or action. This may a person whose area of responsibility would be affected by the activity, such as a business unit manager, or a person whose expertise should be consulted, such as a technical professional.
- **Informed:** A person who needs to know of decision making or actions after they occur. Such a person may have a direct concern in the outcome and progress of the work.

RACI charting helps avoid the following problems:

- Unclear accountability between individuals or departments
- Redundancies or work not being accomplished
- Delayed or incomplete work
- Inadequate communication and/or coordination
- Unclear approval/decision-making processes

Table 2.4 shows a portion of the RACI chart for security governance. The table indicates which entity is accountable for each activity, and which entity or entities are responsible for that activity.

**TABLE 2.4** Partial COBIT 5 RACI Chart for Organizational Structures

Activity	CISO	ISS	ISM	ERM	IC/BO
Identify and communicate information security threats, desirable behaviors, and changes needed to address these points.	A		R		
Ensure that environmental and facilities management adheres to information security requirements.	A		R		
Provide ways to improve efficiency and effectiveness of the information security function (for example, through training of information security staff; documentation of processes, technology, and applications; and standardization and automation of the process).	A		R		
Define and communicate an information security strategy that is in line with the business strategy.	R	A			
Research, define, and document information security requirements.	R	A			
Validate information security requirements with stakeholders, business sponsors, and technical implementation personnel.	R	A			
Develop information security policies and procedures.	R	A			
Define and implement risk evaluation and response strategies and cooperate with the risk office to manage the information risk.	R			A	
Ensure that the potential impact of changes is assessed.	R	A			
Collect and analyze performance and compliance data related to information security and information risk management.	R		R		
Raise the profile of the information security function within the enterprise and potentially outside the enterprise.		R			R

A = accountable

R = responsible

IC/BO = Information custodians/ business owners

## 2.5 Security Governance Evaluation

An ancient Roman saying asks “Who will guard the guards themselves?” Those who are responsible for enterprise governance and information security governance need to be open to evaluation of their efforts at governance. In a publicly held corporation, the board performs or commissions such evaluation, and in any organization, the auditing function illustrated in Figure 2.7 encompasses an assessment of the governance function.

Johnston and Hale’s article “Improved Security Through Information Security Governance” reports a useful set of metrics for evaluating security governance [JOHN09] (see Table 2.5).

**TABLE 2.5** Indicators of Information Security Governance Effectiveness

Indicator Category	Indicators
Executive management support	Executive management understands the relevance of information security to the organization Executives promote effective information security governance Executives actively support the information security program Executives comply with all aspects of the information security program Executive management understands their responsibility for information security Executives understand the liability associated with not executing information security responsibilities
Business and information security relationship	Security investments are optimized to support business objectives Business process owners actively support the information security program Business process owners view security as an enabler Business process owners are involved in evaluating security alternatives Business process owners actively support the development of a security culture Business process owners accept responsibility for information security Business process owners are accountable for information security
Information protection	All information in use within the organization is identified Information is classified according to criticality Information is classified according to sensitivity Information classifications are enforced Information classifications are applied to information received from outside entities Information classifications are applied to information provided to an outside entity Ownership responsibilities for all information are assigned Applications that process sensitive information are identified Applications that support critical business processes are identified Data retention standards are defined and enforced

The metrics fall into three categories:

- **Executive management support:** This is a critical component for cybersecurity program success. If top executives exhibit an understanding of security issues and take an active role in promoting security, this influence is felt throughout the firm. Strong executive management security awareness and support promotes a culture of secure practices.
- **Business and information security relationship:** An effective security governance program conveys a strong relationship between business goals and objectives and information security. When information security is incorporated into the enterprise planning process, employees tend to feel a greater responsibility for the security of their assets and view security not as an impediment but as an enabler.
- **Information protection:** These indicators of security governance effectiveness deal with the pervasiveness and strength of information security mechanisms. These indicators reflect the degree of awareness of information security issues and the level of preparedness, enterprisewide, to deal with attacks.

The SGP mandates that an organization adopt a consistent and structured approach to information risk management to provide assurance that information risk is adequately addressed. A key element is that a structured technique be used at the governing body level, such as the ISF Business Impact Reference Table (BIRT), discussed in Chapter 3. The BIRT is used to document the maximum level of risk or harm that the organization is prepared to accept in any given situation and is used to inform any decisions about information risk throughout the organization.

Based on the risk appetite, the security strategy, security controls, and security assessment measures are developed.

## 2.6 Security Governance Best Practices

The ISF SGP breaks down the best practices in the security governance category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Security governance approach:** This area provides guidance for establishing, maintaining, and monitoring an information security governance framework, which enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management.

- **Security governance framework:** This topic provides a checklist of actions for establishing a security governance framework and ensuring that the organization's overall approach to information security supports high standards of governance.
- **Security direction:** This topic outlines a recommended top-down management structure and mechanism for coordinating security activity (for example, an information security program) and supporting the information security governance approach. It includes discussion of a CISO, a working group, and the tasks of each.
- **Security governance components:** This area provides guidance for supporting the information security governance framework by creating an information security strategy and implementing an information security assurance program that are aligned with the organization's strategic objectives.
  - **Information security strategy:** Provides a checklist for developing an information security strategy.
  - **Stakeholder value delivery:** Focuses on how the organization should implement processes to measure the value delivered by information security initiatives and report the results to all stakeholders.
  - **Information security assurance:** Discusses actions to assure that information risk is being adequately addressed.

## 2.7 Key Terms and Review Questions

### Key Terms

After completing this chapter, you should be able to define the following terms:

architecture	Federal Enterprise Architecture
C-level	Framework (FEAF)
chief executive officer (CEO)	governance
chief information officer (CIO)	information security architecture
chief information security officer (CISO)	information security governance
chief operating officer (COO)	information security implementation/operations
chief privacy officer (CPO)	information security steering (ISS)
chief risk officer (CRO)	committee
chief security officer (CSO)	information security management
enterprise architecture	information security strategic planning
enterprise risk management (ERM)	information technology (IT)
committee	IT strategic planning

RACI chart  
security governance  
security implementation/  
operations

security management  
security program  
stakeholder  
strategic plan

## Review Questions

Answers to the Review Questions can be found online in Appendix C, “Answers to Review Questions.” Go to [informit.com/title/9780134772806](http://informit.com/title/9780134772806).

1. Briefly differentiate between information security governance and information security management.
2. Explain how the three supplemental factors in Figure 2.1—internal incident and global vulnerability reports, standards and best practices, and user feedback—play interconnected roles in designing a security program.
3. Differentiate between internal and external stakeholders from an information security point of view.
4. What are the two key pillars on which IT strategy planning should ideally be based?
5. What are the three categories of metrics for evaluating an organization’s security governance?
6. What are the five roles within a security governing body structure defined in COBIT 5?
7. Explain the acronym RACI from context of information security policy.

## 2.8 References

- BSA03:** Business Software Alliance, *Information Security Governance: Toward a Framework for Action*. 2003. <https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf>
- CGTF04:** Corporate Governance Task Force, *Information Security Governance: A Call to Action*. U.S. Department of Homeland Security, 2004.
- EAPA17:** The EA Pad. *Basic Elements of Federal Enterprise Architecture*. <https://eapad.dk.gov/us/common-approach/basic-elements-of-federal-enterprise-architecture/>
- HAYD08a:** Haydamack, C., “Strategic Planning Processes for Information Technology,” *BPTrends*, September 2008.

- HAYD08b:** Haydamack, C., & Johnson, S., *Aligning IT with Business Goals Through Strategic Planning*. Intel Information Technology White Paper, December 2008.
- ISAC08:** ISACA, *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*. 2008. [www.isaca.org](http://www.isaca.org)
- ITGI06:** IT Governance Institute, *Information Security Governance Guidance for Boards of Directors and Executive Management*. 2006. <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx>
- JOHN09:** Johnston, A., & Hale, R., “Improved Security Through Information Security Governance.” *Communications of the ACM*, January 2009.
- JUIZ15:** Juiz, C., & Toomey, M., “To Govern IT, or Not to Govern IT?” *Communications of the ACM*, February 2015.
- OHKI09:** Ohki, E., et al., “Information Security Governance Framework.” *First ACM Workshop on Information Security Governance (WISG)*, November 2009.
- OMB13:** Office of Management and Budget, *Federal Enterprise Architecture Framework*. 2013.
- PETE12:** Peters, C., & Schuman, B., *Achieving Intel’s Strategic Goals with IT*. Intel Information Technology White Paper, February 2012.
- SESS07:** Sessions, R., “A Comparison of the Top Four Enterprise-Architecture Methodologies.” *Microsoft Developer Network*, May 2007. <http://www3.cis.gsu.edu/dtruex/courses/CIS8090/2013Articles/A%20Comparison%20of%20the%20Top%20Four%20Enterprise-Architecture%20Methodologies.html>
- SGM17:** Strategic Management Group, *Strategic Planning Basics*. [http://www.strategymanage.com/strategic-planning-basics/retrieved April 6, 2017](http://www.strategymanage.com/strategic-planning-basics/retrieved%20April%206%202017).
- TOG11:** The Open Group, *The Open Group Architecture Framework (TOGAF)*. 2011. <http://www.opengroup.org/subjectareas/enterprise/togaf>
- ZIA15:** Zia, T., “Organisations Capability and Aptitude Towards IT Security Governance.” *2015 5th International Conference on IT Convergence and Security (ICITCS)*, August 2015.

## Numbers

---

***10 Key Facts Businesses Need to Note About the GDPR, 193***

***2017 Data Breach Investigations Report (Verizon), 294***

## A

---

**AAL (Authentication Assurance Levels), biometric authentication, 341–347**

**ABAC (Attribute-Based Access Control), 349, 353–355**

attribute metadata, 355–357

resources, 357–358

**access (system)**

access control, 305, 347

ABAC, 349, 353–355

ABAC, attribute metadata, 355–357

ABAC, resources, 357–358

access rights, 348–349

ACL, 350–351

DAC, 349–351

discretionary access control, 312

MAC, 349

metrics, 358–360

objects, 348

RBAC, 349, 351–353

subjects, 348

authorization, 305, 306–307

best practices, 362–363

customer access

arrangements, 360

connections, 361

contracts, 361

data security, 361

defined, 360

functions of, 305

user authentication, 304, 307

authenticators, 311

biometric authentication, 330–331

biometric authentication, AAL, 341–347

biometric authentication, accuracy of, 333, 335–336

biometric authentication, artifact detection, 340

biometric authentication, biometric spoofing, 339

biometric authentication, costs of, 333

biometric authentication, criteria for, 331

biometric authentication, cryptographic devices, 345

biometric authentication, FMR, 335–336

biometric authentication, FNMR, 335–336

biometric authentication, liveness detection, 340

biometric authentication, lookup secrets, 345

biometric authentication, memorized secrets, 345

biometric authentication, operating characteristic curves, 336

biometric authentication, operation of, 333–335



- biometric authentication, OTP devices, 345
- biometric authentication, PAD, 339–340
- biometric authentication, physical
  - characteristics used in, 332–333
- biometric authentication, presentation
  - attacks, 339–340
- biometric authentication, risk assessment, 341–347
- biometric authentication, security controls, 339–341
- biometric authentication, threats to, 337–339
- factors of, 310–311
- hardware tokens, 322
- hardware tokens, eID cards, 325–327
- hardware tokens, memory cards, 322–323
- hardware tokens, OTP devices, 328–329
- hardware tokens, security controls, 330
- hardware tokens, smart cards, 323–325
- hardware tokens, threats to, 329–330
- inherence factor, 310
- knowledge factor, 310
- multifactor authentication, 311–312
- passwords, 312
- passwords, blacklists, 321
- passwords, cracking, 317–319
- passwords, file access control, 319–320
- passwords, hashed passwords, 315–316
- passwords, OTP devices, 328–329
- passwords, PACE, 327
- passwords, regulating password
  - selection, 321
- passwords, shadow password files, 319
- passwords, system-selected passwords, 321–322
- passwords, UNIX password schemes, 315–316
- passwords, user-selected passwords, 320
- passwords, vulnerabilities, 313–315
- possession factor, 310

## **accessibility**

- increased accessibility, privacy threats, 191
- remote access security, ICS, 230

- accidental behavior (culture of security), 169**

- account attacks (specific), 313**

- accountability, 5**

- accounting management, 393, 395–396**

## **accreditation**

- C&A, 266, 270

- Security Accreditation Packages, 269

- security accreditation. *See* authorization

- ACL (Access Control Lists), 350–351**

- acquisition phase (HAM), 214**

- active monitoring, 511–512**

- actuators, ICS, 224**

- address books, office equipment threats/vulnerabilities, 218**

- administration, port administration, VoIP networks, 443**

- adware, 91, 487**

- aggregation, privacy threats, 190**

- AI (Artificial Intelligence), non-malware attacks, 577**

- algorithms (cryptographic), 518**

- ALM (Application Life Cycle Management), 257–259, 281–283**

- AM (Application Management), 280–281**

- ALM, 281–283

- APFM, 283

- defined, 283

- matrix, dimensions of, 283–284

- portfolio management practices, 284–285

- reengineering, 284

- APM, 285–286

- defined, 286

- steps of, 286–287

- application security, 287

- business application registers, 287–288

- external application security, 289

- internal application security, 288–289

- web applications, 293

- web applications, policies, 294–295

- web applications, risks, 289–291

- web applications, WAF, 291–293

- best practices, 300–301

- defined, 281
- EUDA, 295–296, 301
  - benefits of, 296
  - risks of, 296–297
  - security framework, 297–300
- TCO, 281–283
- anomaly detection (intrusion detection), 504–505**
- antivirus software**
  - cyber attack kill chains, 574
  - real-time antivirus software, VoIP networks, 443
- AP (Access Points)**
  - NAP, physical network management, 423
  - rogue AP, wireless network security, 427
  - WAP
    - network management, 416
    - SSID, 426
- APFM (Application Portfolio Management), 283**
  - defined, 283
  - matrix, dimensions of, 283–284
  - portfolio management practices, 284–285
  - reengineering, 284
- APM (Application Performance Management), 285–286**
  - defined, 286
  - steps of, 286–287
- app stores, 236**
- application whitelisting**
  - defined, 164
  - ICS, 229
- application-layer firewalls, VoIP networks, 443**
- application-level gateways (stateful inspection firewalls), 413**
- applications**
  - backups, 641–642
  - cloud-based applications, security, 232
  - EUDA, 295–296, 301
    - benefits of, 296
    - risks of, 296–297
    - security framework, 297–300
  - security, 287
    - business application registers, 287–288
    - external application security, 289
    - internal application security, 288–289
    - web applications, 293
    - web applications, policies, 294–295
    - web applications, risks, 289–291
    - web applications, WAF, 291–293
  - technology stacks, 234
  - unknown authorship of, 237
  - vetting process, 240–241
  - web applications
    - Open Web Application Security Project, 290–291
    - security, 293
    - security, policies, 294–295
    - security, risks, 289–291
    - security, WAF, 291–293
- appropriation, privacy threats, 191**
- APT (Advanced Persistent Threats), 566**
- architectures**
  - defined, 58
  - enterprise architectures, 59
    - FEAF, 58–59
    - RM, 59–62
    - security governance integration, 58
  - information security architectures, 58
- ARM (Application Reference Models), 60–61**
- arrangements (customer), access control, 360**
- artifact detection, biometric authentication, 340**
- assets**
  - asset register, 87–88
  - business assets, defined, 87
  - defined, 4, 75–77
  - hardware assets, defined, 85
  - identifying, 84–85
  - information assets, defined, 86–87
  - physical asset management, 210–211
    - CMDB, 212
    - HAM, 211–212

- HAM, acquisition phase, 214
- HAM, average life cycle duration of common hardware, 216
- HAM, deployment phase, 214–215
- HAM, disposition phase, 216
- HAM, management phase, 215–216
- HAM, planning phase, 213–214
- ICS, defined, 223
- ICS, elements of, 224–225
- ICS, IT systems versus, 225–228
- ICS, security, 227–228, 229–231
- ICS, threats/vulnerabilities, 228–229
- mobile devices, ecosystem of, 234–236
- mobile devices, security, 231–233
- mobile devices, technology stacks, 233–234
- office equipment, 217
- office equipment, cryptographic erasure, 222–223
- office equipment, disposal of, 222–223
- office equipment, OS security, 219
- office equipment, physical security, 219
- office equipment, security controls, 219–222
- office equipment, threats/vulnerabilities, 217–219
- risk assessment, determining future problems, 79
- RM assets, 62
- software assets, defined, 85
- ATE (Awareness, Training, Education), 172**
- attack surfaces**
  - defined, 230
  - reducing, ICS, 230
- attacks**
  - brute-force attacks, 532
  - cyber attacks, defined, 570
  - DDoS attacks
    - cyber attack kill chains, 575
    - defined, 575
  - DoS attacks, servers, 368
  - exploits, defined, 566
  - man-in-the-middle attacks, VoIP, 443
  - non-malware attacks, 576–577
  - offline dictionary attacks, 313

- password guessing, 313
- phishing, defined, 565
- popular password attacks, 313
- presentation attacks, 339–340
- side-channel attacks, 242
- social engineering attacks, defined, 571
- source routing attacks, 411
- spear phishing, defined, 571
- specific account attacks, 313
- tiny fragment attacks, 411

## **audits**

- business continuity readiness, 653–654
- ERM committees, 66
- security audits
  - controls, 673–677
  - data collection, 668–672
  - defined, 666–667
  - elements of, 668
  - external audits, 672–673
  - internal audits, 672
  - logs, 671–672
  - objectives of, 667
  - security audit trails, 667, 671–672

## **AUP (Acceptable Use Policies), 146, 152–153**

- email, 434–435
- IM, 436–437
- SANS Institute AUP template, 152–153

## **authentication**

- DANE, 433
- device authentication, VoIP networks, 443
- digital authentication, 308
- DMARC, 433
- managing, ICS, 230
- MFA, 230
- possession-based authentication. *See* hardware tokens
- user authentication, 304, 307
  - authenticators, 311
  - biometric authentication, 330–331
  - biometric authentication, AAL, 341–347
  - biometric authentication, accuracy of, 333, 335–336

- biometric authentication, artifact detection, 340
- biometric authentication, biometric spoofing, 339
- biometric authentication, costs of, 333
- biometric authentication, criteria for, 331
- biometric authentication, cryptographic devices, 345
- biometric authentication, FMR, 335–336
- biometric authentication, FNMR, 335–336
- biometric authentication, liveness detection, 340
- biometric authentication, lookup secrets, 345
- biometric authentication, memorized secrets, 345
- biometric authentication, operating characteristic curves, 336
- biometric authentication, operation of, 333–335
- biometric authentication, OTP devices, 345
- biometric authentication, PAD, 339–340
- biometric authentication, physical characteristics used in, 332–333
- biometric authentication, presentation attacks, 339–340
- biometric authentication, risk assessment, 341–347
- biometric authentication, security controls, 339–341
- biometric authentication, SP 800-63B guidelines, 340–341
- biometric authentication, threats to, 337–339
- cryptography and, 518
- factors of, 310–311
- hardware tokens, 322
- hardware tokens, eID cards, 325–327
- hardware tokens, memory cards, 322–323
- hardware tokens, OTP devices, 328–329
- hardware tokens, security controls, 330
- hardware tokens, smart cards, 323–325
- hardware tokens, threats to, 329–330
- inherence factor, 310
- knowledge factor, 310
- multifactor authentication, 311–312

- NIST SP 800-63 Digital Identity Model, 307–310
- passwords, 312
- passwords, blacklists, 321
- passwords, cracking, 317–319
- passwords, file access control, 319–320
- passwords, hashed passwords, 315–316
- passwords, OTP devices, 328–329
- passwords, PACE, 327
- passwords, regulating password selection, 321
- passwords, shadow password files, 319
- passwords, system-selected passwords, 321–322
- passwords, UNIX password schemes, 315–316
- passwords, user-selected passwords, 320
- passwords, vulnerabilities, 313–315
- possession factor, 310
- VoIP networks, 443

## **authenticity, 5**

## **authorization, 305, 306–307**

- operations/maintenance phase (NIST SDLC), 272
- security, 269, 270

## **automation, passwords, 314**

## **auto-rooters, 91, 488**

## **availability, 5**

## **avoidance controls, 100**

# **B**

---

## **backdoors (trapdoors), 91, 488**

## **background checks/screening, 162–163**

## **backups**

- application backups, 641–642
- cold site backups, 385
- data restoration from backups, cyber attack kill chains, 574
- hot site backups, 386
- systems management, 384–386
- warm site backups, 386

## **BCM (Business Continuity Management), 623, 625**

- application backups, 641–642
- BCMS, 625
- BCP, 625, 642
  - components of, 642–644
  - crisis management plans, 645–646
  - emergency response plans, 644–645
  - governance, 630–631
  - overview of, 643–644
  - recovery/restoration plans, 646–647
- best practices, 660
- BIA, 631–632
- business continuity readiness
  - awareness, 637–638
  - BCP, 642–647
  - control selection, 640–642
  - exercising/testing, 647–650
  - performance evaluations, 650–654
  - resilience, 639–640
  - training, 638–639
- business continuity strategies
  - cost balancing, 634–635
  - determination/selection, 635–636
  - protection/mitigation, 637
  - resource requirements, 636–637
- business resilience, 639–640
- components of, 630
- COOP, defined, 630
- crisis management plans, 656–657
- effectiveness of, 628–629
- elements of, 623
- emergency response plans, 655–656
- ICT supply chains, 630
- incident response process, 659
- objectives of, 629
- process of, 655
- recovery/restoration plans, 657–659
- resources, 622–623
- risk assessment, 632–634
- threats
  - cyber attacks, 627
  - human-caused physical threats, 627–628
  - natural disasters, 626
  - system problems, 627

## **BCMS (Business Continuity Management Systems), 625**

### **BCP (Business Continuity Plan), 625, 642**

- components of, 642–644
- crisis management plans, 645–646
- emergency response plans, 644–645
- governance, 630–631
- overview of, 643–644
- recovery/restoration plans, 646–647

### **behaviors (culture of security)**

- accidental behavior, 169
- malicious behavior, 168–169
- negligent behavior, 168

### **best practices**

- AM, 300–301
- BCM, 660
- cloud computing, 476–477
- communications, 444–445
- cryptography, 542
- DRM, 515–517, 542
- IAM, 501–502, 542
- IDS, 508–509
- incident management, 597–598
- information management, 205–206
- intrusion detection, 508–509, 542
- local environment security, 619
- malware, 541
- network management, 444–445
- people management, 175–176
- physical asset management, 244–245
- physical security, 619
- PKI, 542
- risk assessment, 131–132
- SCM, 478–479
- SCRM, 463–466
- security governance, 69–70
- security incident management frameworks, 597–598
- security management, 154
- security monitoring, 691–692
- SEM, 561–563
- system access, 362–363
- system development, 278

systems management, 389–390

technical security management, 541–542

## **best practices and standards documents, 6–7, 36–37**

CIS CSC, 27–28

COBIT 5 for information security, 29–30

ISO/IEC 27000 suite of information security standards, 12–13

ISMS, 13–15

ISO 27001, 14, 15–16

ISO 27002, 14, 17–18

ISO 27005, 15

ISO 27014, 15

ISO 27036, 15

mapping to ISF SGP, 18–21

ITU-T security documents, 32–34

NIST cybersecurity framework and security documents, 21–22, 25–26

components of, 22–25

FIPS 200, 26

FIPS 800-27, 26

SP 800-12, 26

SP 800-55, 26

SP 800-100, 26

SP 800-144, 26

SP 1800, 26

PCI-DSS, 30–32

Standard of Good Practice for Information Security (SGP), 7–10

areas of, 10–12

categories of, 10–12

mapping ISO 27000 suite to ISF SGP, 18–21

## **BIA (Business Impact Analysis), 631–632**

### **biometric authentication, 330–331**

AAL, 341–347

accuracy of, 333, 335–336

artifact detection, 340

biometric spoofing, 339

costs of, 333

criteria for, 331

cryptographic devices, 345

FMR, 335–336

FNMR, 335–336

liveness detection, 340

lookup secrets, 345

memorized secrets, 345

operating characteristic curves, 336

operation of, 333–335

OTP devices, 345

PAD, 339–340

physical characteristics used in, 332–333

presentation attacks, 339–340

risk assessment, 341–347

security controls, 339–341

SP 800-63B guidelines, 340–341

threats to, 337–339

### **biometric spoofing, 339**

### **BIRT (Business Impact Reference Tables), 126–127**

### **blacklists, 321**

### **blackmail, privacy threats, 191**

### **blockchains, 95**

### **bots (zombies), 91, 489**

### **breach of confidentiality, privacy threats, 190**

### **BRM (Business Reference Models), 60**

### **brute-force attacks, 532**

### **business application management. See AM (Application Management)**

### **business application registers, 287–288**

### **business assets, 87**

### **Business Continuity Management (BCM), 623, 625**

application backups, 641–642

BCMS, 625

BCP, 625, 642

components of, 642–644

crisis management plans, 645–646

emergency response plans, 644–645

governance, 630–631

overview of, 643–644

recovery/restoration plans, 646–647

best practices, 660

BIA, 631–632

business continuity readiness

awareness, 637–638

BCP, 642–647

control selection, 640–642

- exercising/testing, 647–650
- performance evaluations, 650–654
- resilience, 639–640
- training, 638–639
- business continuity strategies
  - cost balancing, 634–635
  - determination/selection, 635–636
  - protection/mitigation, 637
  - resource requirements, 636–637
- business resilience, 639–640
- components of, 630
- COOP, defined, 630
- crisis management plans, 656–657
- effectiveness of, 628–629
- elements of, 623
- emergency response plans, 655–656
- ICT supply chains, 630
- incident response process, 659
- objectives of, 629
- process of, 655
- recovery/restoration plans, 657–659
- resources, 622–623
- risk assessment, 632–634
- threats
  - cyber attacks, 627
  - human-caused physical threats, 627–628
  - natural disasters, 626
  - system problems, 627
- business resource threats, 89**
- BYOD (Bring Your Own Device) policies, 173**

## C

- C&A (Certification and Accreditation), 266, 270**
- C-level roles/responsibilities, 55**
- CA (Certification Authorities), 539–540**
- cables, telecommunication cables, physical network management, 423**
- capacity management, 383–384**
- capacity planning, 138**
- capital planning, security planning**

- information security costs, 144–145
- investment lifecycle, 142–145
- CCB (Change Control Boards)**
  - defined, 271
  - NIST SDLC security
    - disposal phase, 273
    - operations/maintenance phase, 272
- CEO (Chief Executive Officers)**
  - ERM committees, 65
  - security governance, 55
- CERT (Computer Emergency Response Teams), vulnerability management, 548–549**
- certificates (public key), 536–538**
- certifications**
  - C&A, 266, 270
  - CISM, 175
  - CISSP, 175
  - defined, 15
  - GSEC, 174
  - SANS computer security training and certification, 175
  - security awareness/education, 174–175
  - SSCP, 175
- CFO (Chief Financial Officers), ERM committees, 65**
- change control**
  - CCB
    - defined, 271
    - NIST SDLC security, disposal phase, 273
    - NIST SDLC security, operations/maintenance phase, 272
  - defined, 271
- change management, 169, 386–389**
- characteristic curves, biometric authentication, 336**
- Chase Bank online privacy policy, 190**
- CIO (Chief Information Officers), security governance, 55**
- circuit-level gateways (stateful inspection firewalls), 413–414**
- CIS (Center of Internet Security), CIS CSC, 27–28**
- Cisco Annual Cybersecurity Reports, 98**



**CISM (Certified Information Security Manager), 175****CISO (Chief Information Security Officers)**

- COBIT 5, 64
- ERM committees, 65
- ISS committees, 65
- security governance, 55
- security management, 137
- security management, role in, 138–140

**CISSP, 175****classifying**

- information, 179
  - labeling information, 185
  - NIST risk management framework, 179–183
  - RFID tags, 185
  - security classification process, 183–185
- threats, 89–90

**clickless malware, 490****cloud computing**

- applications, security, 232
- best practices, 476–477
- cloud auditors, 471, 472
- cloud brokers, 471–472
- cloud carriers, 471, 472
- cloud consumers, 471–472
- cloud service providers, 382–383
- community clouds, 468
- context of, 468–469
- CP, 471–472
- defined, 466
- deployment models, 468–470
- elements of, 466–467
- hybrid clouds, 468
- IaaS, 468, 472
- PaaS, 468, 472
- private clouds, 468–469
- public clouds, 468, 469–470
- reference architecture, 470–472
- risk assessment, 475–476
- SaaS, 467–468
- security, 473
  - risk assessment, 475–476
  - threats, 474–475

service agreements, 477–478

service models, 467–468

threats, 474–475

**CMDB (Configuration Management Database), 212****COBIT 5 (Control Objectives for Business and Related Technology 5)**

- change management, 386
- information security, 29–30
  - CISO, 64
  - ERM committees, 65
  - information custodians, 65
  - ISM, 65
  - ISS committees, 64
  - RACI charts, 66–67
  - security governance, 64–66
- sensitive information management, 204–205

**code injection, 92****coding, mobile codes, 91****cold site backups, 385****collecting information, threats to privacy, 189****communications, 430**

- best practices, 444–445
- email, 430–431
  - AUP, 434–435
  - DANE, 433
  - DKIM, 433
  - DMARC, 433
  - MDA, 432
  - MS, 432
  - MSA, 432
  - MTA, 432
  - MUA, 431–432
  - S/MIME, 433
  - SPF, 433
  - STARTTLS, 433
  - trustworthy email standards, 432–434
- IM, 436
  - AUP, 436–437
  - security policies, 437–438
- IP telephony/conferencing, 444



- VoIP networks, 438
  - context, 440–442
  - processing, 439–440
  - security, 443
  - signaling, 439
  - threats, 442–443
- community clouds, 468**
- compliance monitoring, security performance, 690–691**
- conferencing/IP telephony, 444**
- confidentiality, 5, 190**
- configuration management, 393, 396–397**
  - defined, 139
  - ICS, 230
  - security management and, 139
- connection reviews. See ORR**
- connections (customer), access control, 361**
- container virtualization, 85, 374**
- contingency planning and security management, 139**
- contingency training, 267–269**
- contracts (customer), access control, 361**
- control gates, NIST SDLC security, 260**
  - development/acquisition phase, 266
  - implementation/assessment phase, 270
  - initiation phase, 263
  - operations/maintenance phase, 272
- controllers, ICS, 225**
- controls**
  - avoidance controls, 100
  - checklist of controls, 101–102
  - deterrent controls, 100–101
  - identifying, 98–99
  - online catalog of security controls, 99–100
  - responsive controls, 101
  - vulnerability controls, 101
- COO (Chief Operating Officers)**
  - ERM committees, 65
  - security governance, 55
- COOP (Continuity of Operations), 630**
- COPPA (Children's Online Privacy Protection Act), 195**
- copy/scan logs, office equipment threats/vulnerabilities, 218**
- costs**
  - balancing, business continuity strategies, 634–635
  - cybersecurity, 6
  - risk assessment, 108
- COTS (Commercial-Off-The-Shelf) software, 288**
- countermeasures, 26**
- CP (Cloud Providers), 471–472**
- CPO (Chief Privacy Officers), security governance, 55**
- crackers (hackers), 92**
- cracking passwords, 317–319**
- credentials**
  - CSP, 308
  - defined, 309
- crisis management plans, 645–646, 656–657**
- critical information, 171**
- Critical Security Controls for Effective Cyber Defense (CSC), 27–28**
- CRO (Chief Risk Officers)**
  - ERM committees, 66
  - security governance, 55
- cryptanalysis, 532**
- cryptographic devices, biometric authentication, 345**
- cryptographic erasure, 222–223**
- cryptography**
  - algorithms, 518, 525
  - best practices, 542
  - data encryption, 517–518
  - data integrity, 518
  - digital signatures, 518, 524–525
  - implementation considerations, 526–528
  - key management
    - cryptoperiods, 532–533
    - cryptosystems, 528
    - group keys, 530
    - key life cycles, 534–536
    - resources, 529–530
    - types of keys, 530–531

- public key encryption, 520–521
- secure hash functions, 522–524
- symmetric encryption, 518–520
- user authentication, 518
- uses of, 517–518
- cryptoperiods, 532–533**
- CSC (Critical Security Controls for Effective Cyber Defense), 27–28**
- CSIRT (Computer Security Incident Response Teams), 381–382**
- CSO (Chief Security Officers), security governance, 55**
- CSP (Credential Service Providers), 308**
- CTI (Cyber Threat Intelligence). *See* threat intelligence**
- culture of security, 168**
- customer access**
  - arrangements, 360
  - connections, 361
  - contracts, 361
  - data security, 361
  - defined, 360
- CVSS metrics, NVD, 105–107**
- cyber attack kill chains, 570**
  - actions phase, 573, 575
  - command-and-control phase, 573, 575
  - delivery phase, 572, 573–574
  - exploit phase, 572, 574
  - installation phase, 572, 574–575
  - non-malware attacks, 576–577
  - reconnaissance phase, 570–571, 573
  - weaponization phase, 571, 573
- cyber attacks**
  - BCM, 627
  - defined, 570
- cybersecurity**
  - accountability, 5
  - authenticity, 5
  - availability, 5
  - benefits of, 6
  - confidentiality, 5
  - costs of, 6
  - defined, 3

- essentials program, 173
- information security, 4, 68–69
  - COBIT 5, 29–30, 64–66
  - information security architectures, 58
  - information security governance, defined, 42–43
  - information security reports, 53–55
  - information security standards, 12–21
  - information security strategic planning, 50
  - Standard of Good Practice for Information Security (SGP), 9–12
- integrity, 5
- learning continuum, phases of, 167
- management process, 34–37
- network security, 4
- nonrepudiation, 5
- objectives of, 4–5
- user needs versus security implementation, 6
- cyberspace**
  - complexity of, 5
  - defined, 3
  - scale of, 5

## D

---

- DAC (Discretionary Access Control), 349–351**
- DANE (DNS-based Authentication of Named Entities), 433**
- DAS (Direct Access Storage), 377**
- data at rest (DLP), 510–511**
- data breaches, 294**
- data encryption, 517–518**
- data in motion (or transit), DLP, 510, 511–512**
- data in use (DLP), 510, 512**
- data integrity, 518**
- data restoration from backups, cyber attack kill chains, 574**
- data tampering, 89**
- databases, fingerprinting, 509**
- DBIR (Data Breach Investigations Reports), 93–94**
- DDoS (Distributed Denial-of-Service) attacks**
  - cyber attack kill chains, 575
  - defined, 92, 575

- de-perimeterization, mobile devices, 232
- decisional interference, privacy threats, 191
- defense in depth strategies (physical security), 610–612
- deployment phase (HAM), 214–215
- deployment reviews. *See* ORR
- deterrent controls, 100–101
- development/acquisition phase (NIST SDLC), 250–251, 264–266
- device authentication, VoIP networks, 443
- DevOps, 254–256**
  - ALM, 257–259
  - defined, 254
  - reference architecture, 255–257
- diagnostics (remote), ICS, 225**
- dictionary attacks (offline), 313**
- digital authentication, 308**
- digital signatures, 518, 524–525**
- directory servers, 164**
- disclosure, privacy threats, 190**
- disclosure of information, office equipment threats/vulnerabilities, 218**
- discretionary access control, 312**
- disposal phase (NIST SDLC), 252, 272–273**
- disposing of office equipment, 222–223**
- disposition phase (HAM), 216**
- disseminating information, threats to privacy, 190–191**
- distortion, privacy threats, 191**
- distributed network management systems, 401–402**
- DKIM (DomainKeys Identified Mail), 433**
- DLP (Data Loss Prevention), 186, 509**
  - classifying data, 509–510
  - data at rest, 510–511
  - data in motion (or transit), 510, 511–512
  - data in use, 510, 512
  - database fingerprinting, 509
  - exact file matching/hash values, 510
  - partial document matching, 510
  - rule-based recognition, 509
- DMARC (Domain-based Message Authentication, Reporting and Conformance), 433**

**DMZ (Demilitarized Zones), 508****DMZ networks and firewalls, 414–416****DNS attacks, 92****documents, 140–141**

- AUP, 146, 152–153
- awareness program communication materials, 170–172
- BCP, 642
  - components of, 642–644
  - crisis management plans, 645–646
  - emergency response plans, 644–645
  - overview of, 643–644
  - recovery/restoration plans, 646–647
- best practices and standards documents, 6–7, 8–12
- change request documents, 388
- crisis management plans, 645–646
- emergency response plans, 644–645
- employment agreements, 163
- information security reports, 53–55
- information security strategic planning, 146
- managing, 198–202
- network documentation, physical network management, 423
- partial document matching, 510
- RACI charts, security governance, 66–67
- recovery/restoration plans, 646–647
- risk assessment reports, 92–93
  - Cisco Annual Cybersecurity Reports, 98
  - ENISA Threat Landscape Reports, 95–96
  - Fortinet Threat Landscape Reports, 98
  - Threat Horizon Reports, 94–95
  - Trustwave Global Security Reports, 97
  - Verizon DBIR, 93–94
- Router and Switch Security Policy (SANS Institute), 148–150
- security planning, 146
  - AUP, 146, 152–153
  - information security strategic planning, 146
  - Router and Switch Security Policy (SANS Institute), 148–150
  - security policies, 146
  - security policies, templates, 147–150

- simple risk analysis worksheet, 113–114
- templates
  - Router and Switch Security Policy (SANS Institute), 148–150
  - security planning, 147–150
  - security policy templates, 147–150

### **DoS (Denial-of-Service) attacks, 90**

- defined, 92
- office equipment, 218–219
- servers, 368

### **downloaders, 91, 488**

### **DRM (Data Reference Models), 60**

### **DRM (Data Rights Management), 512**

- architecture of, 514–515
- best practices, 515–517, 542
- components of, 513–514

### **droppers, 91, 488**

### **dual operator policies, human resource security, 165**

### **duties, separation of, human resource security, 165**

## **E**

---

### **eavesdropping**

- VoIP, 443
- wireless network security, 427

### **eID (Electronic Identification) cards, 325–327**

### **Electronic Communications Privacy Act, The, 195**

### **element management layer (network management systems), 403**

### **elevation of privileges, 90**

### **email, 430–431**

- AUP, 434–435
- DANE, 433
- DKIM, 433
- DMARC, 433
- MDA, 432
- MS, 432
- MSA, 432
- MTA, 432
- MUA, 431–432
- S/MIME, 433

- SPF, 433

- STARTTLS, 433

- trustworthy email standards, 432–434

### **emergencies (security incident), handling, 590–592**

### **emergency response plans, 644–645, 655–656**

### **EMI (Electromagnetic Interference), 609**

### **EMM systems, mobile devices, 242–243**

### **employees, security**

- awareness/education, 166, 168
  - awareness program communication materials, 170–172
  - awareness program evaluation, 172
  - certification, 174–175
  - culture of security, 168
  - cybersecurity essentials program, 173
  - cybersecurity learning continuum, phases of, 167
  - NIST ATE, 172
  - processes of, 169–170
  - role-based training, 173–174
  - SP 800-16, 166
  - SP 800-50, 166
- current employees, 164–165
- dual operator policies, 165
- limited reliance on key employees, 165
- privileges, 165
- remote working, 176
- separation of duties, 165
- termination of employment, 165–166
- vacations, 165

### **employment agreements, 163**

### **encryption**

- cryptographic erasure, 222–223
- data encryption, 517–518
- public key encryption, 520–521
- symmetric encryption, 518–520
- VoIP networks, 443

### **end-user testing, 265**

### **ENISA Threat Landscape Reports, 95–96, 294**

### **enterprise architectures, 59**

- FEAF, 58–59
- RM, 59–60

- ARM, 60–61
- assets of, 62
- BRM, 60
- DRM, 60
- IRM, 61
- PRM, 60
- relationships between components, 61
- SRM, 61–62
- security governance integration, 58
- enterprise infrastructures, mobile devices, 242–243**
- enterprise strategic planning, 47**
- environment security, 275–277**
- environmental threats**
  - BCM, 626
  - defined, 89
  - local environment security, 607–608, 612–614
- equipment disposal, 222–223**
- erasing data, cryptographic erasure, 222–223**
- ERM (Enterprise Risk Management) committees**
  - COBIT 5, 65
  - ERM committees, 65–66
- EUDA (End-User-Developed Applications), 295–296, 301**
  - benefits of, 296
  - risks of, 296–297
  - security framework, 297–300
- evaluating, risk, 76**
- events**
  - defined, 75
  - threat event frequency, estimating, 118–119
- exact file matching/hash values, 510**
- exclusion, privacy threats, 190**
- exfiltration, 457**
- exploit kits, 91**
- exploits, 488**
  - defined, 91, 566
  - website exploits, defined, 92
- exposure**
  - privacy threats, 190
  - RoE, 76

- external network connections, managing, 427–428**

- external requirements function, security management, 140**

## F

- FACTA (Fair and Accurate Credit Transaction Act of 2003), 195**

- FAIR (Factor Analysis of Information Risk), 114**

- impact assessment, 122–123

- BIRT, 126–127

- loss estimation, 123–126

- likelihood assessments, 116–118

- loss estimation, 123–126

- loss event frequency, 121–122

- Open Group security standards, 114–115

- risk assessment, 115–116

- risk assessment matrices, 120–121

- false negatives (intrusion detection), 504–505**

- false positives (intrusion detection), 504–505**

- fault management, 393, 394–395**

- fax logs, office equipment threats/vulnerabilities, 218**

- FEAF (Federal Enterprise Architecture Framework), 58–59**

- Federal Policy for the Protection of Human Subjects, 195**

- federated identity management, 498–500**

- FERPA (Family Educational Rights and Privacy Act of 1974), 195**

- file access control and passwords, 319–320**

- fileless malware, 490**

- fingerprinting (database), 509**

- firewalls, 404**

- application-layer firewalls, VoIP networks, 443

- characteristics of, 404–405

- cyber attack kill chains, 574, 575

- DMZ networks, 414–416

- limitations of, 406

- network-based firewalls, 292

- next-generation firewalls, 414

- packet filtering firewalls, 406–411
- planning, 428–429
- policies, 428
- stateful inspection firewalls, 411–413
  - application-level gateways, 413
  - circuit-level gateways, 413–414
- VPN (firewall-based), 420
- WAF, 291–293, 574

### **firmware, technology stacks, 234**

### **flooders, 91, 488**

### **flows (ICT supply chains), 450–451**

### **FMR (False Match Rates), biometric authentication, 335–336**

### **FNMR (False Nonmatch Rates), biometric authentication, 335–336**

### **forensics, 592–593**

- analysis phase, 595–596
- collection phase, 594–595
- identification phase, 594
- incident management, 584
- preparation phase, 593–594
- preservation phase, 595
- reporting phase, 596

### **Fortinet Threat Landscape Reports, 98**

### **functional testing, 265**

## **G**

---

### **gateways, stateful inspection firewalls**

- application-level gateways, 413
- circuit-level gateways, 413–414

### **GDPR (General Data Protection Regulation), 193–195**

### **GIAC (Global Information Assurance Certification), GSEC, 174**

### **GLBA (Gramm-Leach-Bliley Act of 1999), 195**

### **golden records, ICS, 231**

### **Google privacy policy, 190**

### **governance (security)**

- BCP, 630–631
- best practices, 69–70
- CEO, 55
- CIO, 55

### **CISO, 55**

- components of, 47

### **COO, 55**

### **CPO, 55**

### **CRO, 55**

### **CSO, 55**

- defined, 43

- desired outcomes, 46

- effectiveness of, 68–69

- enterprise architecture integration, 58

- evaluating, 68–69

- framework of, 63

- information security architectures, 58

- governance, defined, 42–43

- ISMS, 44

- principles of, 45–46

- reporting relationships for, 56

- roles/responsibilities of, 55, 57–58

- security direction

- COBIT 5, 64–66

- ISF SGP, 64

- RACI charts, 66–67

- security management and, 138

- security programs, defined, 43

- stakeholders, defined, 45–46

- strategic planning, 47

- defined, 48

- enterprise strategic planning, 47

- framework of, 51–52

- information security strategic planning, 50

- IT strategic planning, 48–49

### **GPS (location services), security, 237**

### **group key cryptography, 530**

### **GSEC (Global Security Essentials), 174**

### **guessing passwords, 313**

### **guest OS (VM), 371**

## **H**

---

### **hackers (crackers)**

- defined, 92

- wireless network security, 427

**HAM (Hardware Asset Management), 211–212**

- acquisition phase, 214
- average life cycle duration of common hardware, 216
- deployment phase, 214–215
- disposition phase, 216
- management phase, 215–216
- planning phase, 213–214

**hard drives, SED, 222****hardware assets**

- CMDB, 212
- defined, 85
- HAM, 211–212
  - acquisition phase, 214
  - average life cycle duration of common hardware, 216
  - deployment phase, 214–215
  - disposition phase, 216
  - management phase, 215–216
  - planning phase, 213–214

**hardware, technology stacks, 233–234****hardware tokens, 322**

- eID cards, 325–327
- memory cards, 322–323
- OTP devices, 328–329
- security controls, 330
- smart cards, 323–325
- threats to, 329–330

**hash functions (secure), 522–524****hash values/exact file matching, 510****hashed passwords, 315–316****HIDS (Host-based Intrusion Detection Systems), 503, 505–506, 574****hijacking workstations, 313****HIPAA (Health Insurance Portability and Accountability Act of 1996), 195****hiring process, security, 162**

- background checks/screening, 162–163
- directory servers, 164
- employment agreements, 163
- job descriptions, 164

**hosted (nested) virtualization, 372****hosted virtualization security, 377****hostile actors, threat identification, 89****hot site backups, 386****human resource security, 160–162**

- current employees, 164–165
- dual operator policies, 165
- hiring process, 162
  - background checks/screening, 162–163
  - directory servers, 164
  - employment agreements, 163
  - job descriptions, 164
- limited reliance on key employees, 165
- privileges, 165
- remote working, 176
- separation of duties, 165
- termination of employment, 165–166
- vacations, 165

**human-caused physical threats**

- BCM, 627–628
- local environment security, 609, 615

**human-machine interface, ICS, 225****hybrid clouds, 468****hypervisors, 371**

- functions of, 371
- security, 376
- types of, 371–374

**I****IaaS (Infrastructure as a Service), 468, 472****IAM (Identity and Access Management), 496**

- architecture of, 497–498
- best practices, 501–502, 542
- defined, 496
- federated identity management, 498–500
- planning, 500–501
- SSO, 497

**ICS (Industrial Control Systems)**

- actuators, 224
- application whitelisting, 229
- attack surfaces, reducing, 230
- authentication management, 230

- configuration management, 230
- controllers, 225
- defined, 223
- elements of, 224–225
- golden records, 231
- human-machine interface, 225
- IT systems versus, 225–228
- maintenance, 225
- monitoring security, 231
- patch management, 230
- remote access security, 230
- remote diagnostics, 225
- security, 227–228, 229–231
- sensors, 224
- threats/vulnerabilities, 228–229

### **ICT supply chains**

- BCM, 630
- defined, 449
- flows, 450–451
- SCRM, 453–456
  - security controls, 460–463
  - threats, 456–459
  - vulnerabilities, 459–460

### **identification, 307–310, 321**

- eID cards, 325–327
- privacy threats, 190

### **identifying risk, 76**

### **identity**

- federated identity management, 498–500
- IAM, 496
  - architecture of, 497–498
  - best practices, 501–502, 542
  - defined, 496
  - federated identity management, 498–500
  - planning, 500–501
  - SSO, 497
- proofing, 308
- spoofing, 89

### **IDS (Intrusion Detection Systems), 502–503**

- best practices, 508–509
- HIDS, cyber attack kill chains, 574
- NIDS, cyber attack kill chains, 575

### **IEC (International Electrotechnical Commission), ISO/IEC 27000 suite of information security standards, 12–13**

- ISMS, 13–15
- ISO 27001, 14, 15–16
- ISO 27002, 14, 17–18
- ISO 27005, 15
- ISO 27014, 15
- ISO 27036, 15
- mapping to ISF SGP, 18–21

### **IM (Instant Messaging), 436**

- AUP, 436–437
- security policies, 437–438

### **impact (risk management)**

- defined, 75
- determining risk, 77
- impact assessment, 122–123
  - BIRT, 126–127
  - loss estimation, 123–126

### **implementation/assessment phase (NIST SDLC), 251–252, 266–270**

### **incident handling checklist, 589**

### **incident management, 577–578**

- best practices, 597–598
- emergencies, handling, 590–592
- forensics, 592–593
  - collection phase, 594–595
  - identification phase, 594
  - preparation phase, 593–594, 595–596
  - preservation phase, 595
  - reporting phase, 596
- gathering information, 583
- incident handling checklist, 589
- incident response process, 584–585
  - containment/eradication/recovery phase, 587–588
  - detection/analysis phase, 586–587
  - incident handling checklist, 589
  - post-incident activity phase, 588–589
  - preparation phase, 585
- ISMS and, 579–580
- objectives of, 579



- policies, 580–581
- resources, 578–579
- roles/responsibilities of, 581–582
- tools, 583–584

### **incident response**

- BCM, 659
- security management and, 139

### **increased accessibility, privacy threats, 191**

### **information**

- assets, defined, 86–87
- collecting, threats to privacy, 189
  - disclosure, 90, 218
- disseminating, threats to privacy, 190–191
  - flows (supply chains), 450–451
- invasions, threats to privacy, 190–191
- labeling, 185
  - leakage. *See* DLP (Data Loss Prevention)
- processing, threats to privacy, 189–190

### **information custodians**

- COBIT 5, 65
- ERM committees, 66
- ISS committees, 65

### **information management, 178–179**

- best practices, 205–206
- classifying information, 179
  - labeling information, 185
- NIST risk management framework, 179–183
- RFID tags, 185
  - security classification process, 183–185
- document/records management, 198–199
  - differences between documents and records management, 199–200
  - document management, 200–202
  - records management, 202–204
- handling information, 186
- privacy, 186–188
  - Chase Bank online privacy policy, 190
  - collecting information, 189
  - disseminating information, 190–191
  - Google privacy policy, 190
  - invasions, 190–191
  - principles/policies, 191–198

- privacy controls, 196–198
- processing information, 189–190
- security's relationship to privacy, 188
- threats to privacy, 189–191
  - U.S. privacy laws/regulations, 195
- sensitive information, 204–205

### **information protection champions, 605–606**

### **information security, 4, 68–69**

- architectures, 58
- COBIT 5
  - CISO, 64
  - COBIT 5 for information security, 29–30
- coordinators, 604–605
- governance, defined, 42–43
- ISMS, 44
- ISO/IEC 27000 suite of information security standards, 12–13
  - ISMS, 13–15
  - ISO 27001, 14, 15–16
  - ISO 27002, 14, 17–18
  - ISO 27005, 15
  - ISO 27014, 15
  - ISO 27036, 15
- mapping to ISF SGP, 18–21
- management, defined, 43
- reports, 53–55
- Standard of Good Practice for Information Security (SGP), 9–12, 18–21
- strategic planning, 50, 146

### **information system resilience, 639**

### **inherence factor (user authentication), 310**

### **initiation phase (NIST SDLC), 249–250, 260–263**

### **injection flaws, 92**

### **insecurity, privacy threats, 190**

### **integration testing, 251**

### **integrity, 5, 518**

### **interrogation, privacy threats, 189**

### **intrusion, privacy threats, 191**

### **intrusion detection, 502, 504**

- anomaly detection, 504–505
- best practices, 508–509, 542

- false negatives, 504–505
- false positives, 504–505
- HIDS, 503, 505–506
- IDS, 502–503, 508–509
- misuse detection, 504
- NIDS, 503, 506
  - deploying, 507–508
  - function of, 506
  - principles of, 503–504
  - true negatives, 505
  - true positives, 505
- invasions of privacy, information management, 190–191**
- investment lifecycles, capital planning, security planning, 142–145**
- IP address spoofing, 411**
- IP telephony/conferencing, 443–444**
- IPR (Intellectual Property Rights), 455**
- IPS (Intrusion Protection Systems), cyber attack kill chains, 574**
- IPSec (IP Security), 418–420**
- IRM (Infrastructure Reference Models), 61**
- ISACA, CISM, 175**
- ISC (Internet Storm Center)**
  - CISSP, 175
  - SSCP, 175
  - vulnerability management, 549
- ISF (Information Security Forum)**
  - SGP, security governance, 64
  - Standard of Good Practice for Information Security (SGP), 7–10
    - areas of, 10–12
    - categories of, 10–12
    - mapping ISO 27000 suite to ISF SGP, 18–21
  - Threat Horizon Reports, 94–95
- ISM (Information Security Managers)**
  - COBIT 5 for information security, 65
  - ISS committees, 65
  - security management, 137–138
- ISMS (Information Security Management Systems), 44**
  - incident management and, 579–580
  - ISO/IEC 27000 suite of information security standards, 12–15

## **ISO (International Organization for Standardization)**

- ISO 7498–4, Open Systems Interconnection-Basic Reference Model-Part 4: Management Framework, 393
- ISO 22301, BCM methodology, 623
- ISO 27002, Code of Practice for Information Security Controls, 162, 386
- ISO 27005, information security risk management, 81–84

## **ISO 29100, 192**

- ISO/IEC 27000 suite of information security standards, 12–13
  - ISMS, 13–15
  - ISO 27001, 14, 15–16
  - ISO 27002, 14, 17–18
  - ISO 27005, 15
  - ISO 27014, 15
  - ISO 27036, 15
- mapping to ISF SGP, 18–21

## **ISS (Information Security Steering) committees**

- COBIT 5, 64
- ISS committees, 65

## **IT (Information Technology), 45**

## **IT managers, ISS committees, 65**

## **IT strategic planning, 48**

## **IT systems, ICS versus, 225–228**

## **ITSM (IT Service Management), SLA, 379**

## **ITU (International Telecommunication Union), ITU-T security documents, 32–34, 45, 393**

# **J - K**

## **job descriptions, hiring process security, 164**

## **key life cycle, 534–536**

## **keyloggers, 91, 488**

## **kill chains**

- defined, 96
- phases of, 96–97

## **kits (virus generators), 91, 488**

## **knowledge factor (user authentication), 310**

## **KPI (Key Performance Indicators), 455**

## L

---

**labeling, information, 185**

**leakage of information. See DLP (Data Loss Prevention)**

**least privilege**

defined, 230

human resource security, 165

**level of risk, 76–77**

**likelihood (risk assessment)**

defined, 76

determining risk, 77

**likelihood assessments, 116–118**

**limited reliance on key employees, human resource security, 165**

**liveness detection, biometric authentication, 340**

**local environment security**

best practices, 619

coordinating, 604–606

defined, 602–603

information protection champions, 605–606

information security coordinators, 604–605

physical security

best practices, 619

controls, 615–616

controls, assessments, 618–619

controls, baselines, 617–618

defense in depth strategies, 610–612

defined, 606

PSO, 609–610

security maps, depth of security, 611–612

threats, 606

threats, environmental threats, 607–608, 612–614

threats, human-caused physical threats, 609, 615

threats, preventing/mitigating, 612–615

threats, technical threats, 608–609, 614–615

profiles, 603–604

security champions, 605–606

**local storage. See DAS**

**location services, security, 237**

**logic bombs, 90, 488**

**logs**

defined, 556

log management policy, 558–559

network device logs, 557

office equipment threats/vulnerabilities, 218

OS logs, 557

security audits, 671–672

security event logs, 554–556

determining what to log, 557

log management policy, 558–559

objective of, 556

potential log sources, 556–557

securing data, 557–558

vulnerability logs, 551

web server logs, 557

**lookup secrets, biometric authentication, 345**

**loss event frequency, 121–122**

## M

---

**MaaS (Malware as a Service), 488**

**MAC (Mandatory Access Control), 349**

**machine learning, non-malware attacks, 577**

**machine-human interface, ICS, 225**

**mailboxes (MFD), office equipment threats/vulnerabilities, 218**

**maintenance**

ICS, 225

remote network maintenance, 429–430

**malicious behavior (culture of security), 168–169**

**malware**

adware, 487

auto-rooters, 488

backdoors (trapdoors), 488

best practices, 541

bots (zombies), 489

clickless malware, 490

defined, 90, 487

downloaders, 488

droppers, 488

- exploits, 488
- fileless malware, 490
- flooders, 488
- keyloggers, 488
- kits (virus generators), 488
- logic bombs, 488
- MaaS, 488
- malware protection software
  - capabilities of, 494–495
  - managing, 495–496
- mobile codes, 488
- nature of, 490
- non-malware attacks, 576–577
- polymorphic droppers, 488
- practical malware protection, 490–494
- PUP, 488, 490
- ransomware, 489
- RAT, 489
- rootkits, 489
- scrapers, 489
- spammer programs, 489
- spyware, 489
- Trojan horses, 489
- types of, 487–489
- virus generators (kits), 488
- viruses, 489
- web drive-bys, 489
- worms, 489
- zombies (bots), 489
- management phase (HAM), 215–216**
- management protocols, office equipment, 217**
- managing**
  - applications. *See* AM
  - authentication management, ICS, 230
  - capacity, 383–384
  - change, 169, 386–389
  - CMDB, 212
  - configurations
    - defined, 139
    - ICS, 230
    - security management and, 139
  - cybersecurity, 34–37
  - documents, 198–202
  - information, 178–179
    - best practices, 205–206
    - classifying information, 179–185
    - document/records management, 198–204
    - handling information, 186
    - privacy, 186–198
    - security, 43–44
    - sensitive information, 204–205
  - log management policy, 558–559
  - malware protection software, 495–496
  - passwords, automated password managers, 314
  - patches, 230, 551–554
  - people
    - best practices, 175–176
    - human resource security, 160–166
    - security awareness/education, 166–175
  - performance, 383–384
  - physical assets, 210–211
    - best practices, 244–245
    - CMDB, 212
    - HAM, 211–212
    - HAM, acquisition phase, 214
    - HAM, average life cycle duration of common hardware, 216
    - HAM, deployment phase, 214–215
    - HAM, disposition phase, 216
    - HAM, management phase, 215–216
    - HAM, planning phase, 213–214
    - mobile devices, EMM systems, 242–243
    - mobile devices, enterprise infrastructures, 242–243
    - mobile devices, network protocols/services, 241–242
    - mobile devices, physical access, 242
    - mobile devices, security, 238–239, 243
    - mobile devices, technology stacks, 239–240
    - mobile devices, threats/vulnerabilities, 236–237
    - mobile devices, vetting applications, 240–241
    - office equipment, 217

- office equipment, threats/vulnerabilities, 217–219
- resources, 243
- PKI, 540–541
- records/documents, 198–200, 202–204
- risk, 80
  - defined, 76
  - ISO 27005 information security risk management, 81–84
  - NIST risk management framework, 179–183
  - security management and, 139
  - X.1055 risk management process, 80–81
- security, 137
  - awareness/training, 138
  - best practices, 154
  - capacity planning, 138
  - CISO, role in, 137, 138–140
  - configuration management, 139
  - consistency in security, 139
  - contingency planning, 139
  - external requirements function, 140
  - governance, 138
  - incident response, 139
  - ISM, role in, 137–138
  - monitor function, 140
  - performance measures, 139
  - planning, 138
  - policies, 151
  - products/services acquisition, 138
  - projects function, 140
  - risk management and, 139
  - support function, 139
  - system development life cycle, 138
- sensitive information, 204–205
- system development, 273–274
  - environments, 275–277
  - methodologies, 274–275
  - QA, 277
- mandatory vacations, human resource security, 165**
- man-in-the-middle attacks, VoIP, 443**
- MDA (Mail Delivery Agents), 432**
- memorized secrets, biometric authentication, 345**
- memory cards, user authentication, 322–323**
- methodologies of system development, 274–275**
- MFA (Multifactor Authentication), 230**
- MFD (Multifunction Devices). See also office equipment, 217**
  - address books, threats/vulnerabilities, 218
  - cryptographic erasure, 222–223
  - equipment disposal, 222–223
  - logs, threats/vulnerabilities, 218
  - mailboxes, threats/vulnerabilities, 218
  - management protocols, 217
  - OS security, 219
  - physical security, 219
  - security controls, 219–222
  - SED, 222
  - services protocols, 217–218
  - threats/vulnerabilities, 217
    - DoS attacks, 218–219
    - information disclosure, 218
    - network services, 217–218
- mirroring ports, 511**
- misuse detection (intrusion detection), 504**
- mobile codes, 91, 488**
- mobile devices**
  - applications, vetting, 240–241
  - cloud-based applications, 232
  - de-perimeterization, 232
  - ecosystem of, 234–236
  - EMM systems, 242–243
  - enterprise infrastructures, 242–243
  - network management, 416
  - network protocols/services, 241–242
  - physical access, 242
  - resources, 243
  - screen locks, 242
  - security, 231–233, 243
  - security strategies, 238–239
  - technology stacks, 233–234, 239–240
  - threats/vulnerabilities, 236–237

**ModSecurity WAF (Web Application Firewall), 293****money flows (supply chains), 451****monitoring**

- active monitoring, 511–512
- ICS security, 231
- passive monitoring, 511–512
- password use, 314

**monitoring security**

- best practices, 691–692
- security audit trails
  - application-level audit trails, 671
  - defined, 667
  - network-level audit trails, 671
  - physical access audit trails, 671–672
  - system-level audit trails, 671
  - user-level audit trails, 671
- security audits
  - controls, 673–677
  - data collection, 668–672
  - defined, 666–667
  - elements of, 668
  - external audits, 672–673
  - internal audits, 672
  - logs, 671–672
  - objectives of, 667
- security management, 140
- security performance, 678
  - compliance monitoring, 690–691
  - metrics, 678–679
  - metrics, defined, 682–683
  - metrics, development process, 683–685
  - metrics, examples of, 680–681
  - metrics, monitoring/reporting, 686–688
  - metrics, risk reporting, 688–689
  - metrics, sources of, 679–680
  - metrics, values of, 682
  - monitoring/reporting, 686–688
  - risk reporting, 688–689
- security policies, 151–152

**MS (Message Stores), 432****MSA (Mail Submission Agents), 432****MSP (Managed Service Providers), SLA, 379****MTA (Message Transfer Agents), 432****MTD (Maximum Tolerable Downtime), 632****MUA (Message User Agents), 431–432****multifactor authentication, 311–312****multiple password use, exploiting, 314**

---

**N****NAP (Network Access Points), physical network management, 423****NAS (Network Attached Storage), 378–379****National Science Foundation, 210****native virtualization, 371–372, 373****natural disasters**

- BCM, 626
- local environment security, 607–608, 612–614

**negligent behavior (culture of security), 168****nested (hosted) virtualization, 372****network management, 393**

- accounting management, 393, 395–396
- best practices, 444–445
- configuration management, 393, 396–397
- device logs, 557
- DMZ, defined, 508
- DMZ networks, 414–416
- documentation, physical network management, 423
- external network connections, 427–428
- fault management, 393, 394–395
- firewalls, 292, 404
  - characteristics of, 404–405
  - DMZ networks, 414–416
  - limitations of, 406
  - next-generation firewalls, 414
  - packet filtering firewalls, 406–411
  - planning, 428–429
  - policies, 428
  - stateful inspection firewalls, 411–413
  - stateful inspection firewalls, application-level gateways, 413
  - stateful inspection firewalls, circuit-level

- gateways, 413–414
- VPN (firewall-based), 420
- IPSec, 418–420
- mobile devices, 416
- network management systems
  - architecture of, 402–404
  - components of, 399–401
  - distributed network management systems, 401–402
  - element management layer, 403
  - NME, 400–401
  - NML, 403–404
  - service management layer, 404
- performance management, 393, 397–398
- physical network management, 423–426
  - NAP, 423
  - network documentation, 423
  - telecommunication cables, 423
  - providers, SLA, 379–381
- remote network maintenance, 429–430
- SDN, defined, 85
- security, 4
  - device configuration, 421–423
  - managing, 393, 398–399
- services, office equipment threats/vulnerabilities, 217–218
- storage, 377
  - DAS, 377
  - NAS, 378–379
  - SAN, 377–379
- VoIP networks, 438
  - context, 440–442
  - processing, 439–440
  - security, 443
  - signaling, 439
  - threats, 442–443
- VPN, 417–418, 426–427
  - defined, 241
  - external network connections, 428
  - firewall-based VPN, 420
  - VoIP networks, 443
- WAP, 416
- wireless network management, 416–417
- wireless network security, 426–427
- next-generation firewalls, 414**
- NFV (Network Function Virtualization), 85**
- NIDS (Network-based Intrusion Detection Systems), 503, 506**
  - cyber attack kill chains, 575
  - deploying, 507–508
  - function of, 506
- NIST (National Institute of Standards and Technology), 188**
  - ATE, 172
  - cybersecurity framework and security documents, 21–22, 25–26
    - components of, 22–25
    - FIPS 200, 26
    - FIPS 800-27, 26
    - SP 800-12, 26
    - SP 800-55, 26
    - SP 800-100, 26
    - SP 800-144, 26
    - SP 1800, 26
  - NVD, 103–104
    - CVSS metrics, 105–107
    - scoring example, 104–105
  - risk management framework, 179–183
  - SDLC, 248–249
    - development/acquisition phase, 250–251, 264–266
    - disposal phase, 252, 272–273
    - implementation/assessment phase, 251–252, 266–270
    - incorporating security, 259–260
    - incorporating security, development/acquisition phase, 264–266
    - incorporating security, disposal phase, 272–273
    - incorporating security, implementation/assessment phase, 266–270
    - incorporating security, initiation phase, 260–263
    - incorporating security, operations/maintenance phase, 270–272

initiation phase, 249–250

initiation phase, security, 260–263

operations/maintenance phase, 252, 270–272

SP 800-12, 26

SP 800-16, 166

SP 800-18, 140–141

SP 800-37, 261, 267–269

SP 800-41, 428

SP 800-45, 434

SP 800-50, 166

SP 800-53, 63, 196–198

SP 800-53A, 267–269

SP 800-55, 26

SP 800-63, 307–310

SP 800-63B, 321, 340–341

SP 800-88, 272

SP 800-90A, 321

SP 800-100, 26

SP 800-122, 198

SP 800-125, 374–376

SP 800-125A, 374–375

SP 800-144, 26

SP 800-162, 357–358

SP 800-177, 433

SP 800-178, 358

SP 1800, 26

SP 1800-3, 358

**NISTIR 7874, 358–360**

**NISTIR 8112, 358**

**NME (Network Management Entities), 400–401**

**NML (Network Management Layer), network management systems, 403–404**

**noise (EMI), 609**

**non-malware attacks, 576–577**

**nonrepudiation, 5**

**NTP (Network Time Protocol), 594**

**number generators (pseudorandom), 535**

**NVD (National Vulnerability Database), 103–104**

CVSS metrics, 105–107

scoring example, 104–105

## O

**objects (system access), 348**

**office equipment, security. *See also* MFD, 217**

address books, threats/vulnerabilities, 218

cryptographic erasure, 222–223

equipment disposal, 222–223

logs, threats/vulnerabilities, 218

mailboxes, threats/vulnerabilities, 218

management protocols, 217

OS security, 219

physical security, 219

security controls, 219–222

SED, 222

services protocols, 217–218

threats/vulnerabilities, 217

DoS attacks, 218–219

information disclosure, 218

network services, 217–218

**offline dictionary attacks, 313**

**Open Group security standards, 114–115**

**Open Web Application Security Project, application security risks, 290–291**

**operating characteristic curves, biometric authentication, 336**

**operations/maintenance phase (NIST SDLC), 252, 270–272**

**organizational information/decision work flows, cybersecurity management process, 36–37**

**ORR (Operational Readiness Reviews), 270**

**OS (Operating Systems)**

logs, 557

mobile OS, 234

security, office equipment, 219

**OTP (One-Time Password) devices, 328–329, 345**

**outages (power), 608**

**overvoltage, 609**

**OWASP (Open Web Application Security Project)**

Risk Rating Methodology, 294

Testing Guide, 295

**ownership, total cost of (TCO), 281–283**



## P

**PaaS (Platform as a Service), 468, 472**

**PACE (Password Authentication Connection Establishment), 327**

**packet filtering firewalls, 406–411**

**Packet Storm, vulnerability management, 549**

**PAD (Presentation Attack Detection), 339–340**

**parallel runs, implementation/assessment phase (NIST SDLC), 252**

**partial document matching, 510**

**passive monitoring, 511–512**

**passwords, 312**

- automated password managers, 314

- blacklists, 321

- cracking, 317–319

- discretionary access control, 312

- file access control, 319–320

- guessing, 313

- hashed passwords, 315–316

- monitoring, 314

- multiple password use, exploiting, 314

- offline dictionary attacks, 313

- OTP devices, 328–329, 345

- PACE, 327

- password attacks

- defined, 92

- popular password attacks, 313

- regulating password selection, 321

- shadow password files, 319

- specific account attacks, 313

- system-selected passwords, 321–322

- UNIX password schemes, 315–316

- user-selected passwords, 320

- vulnerabilities, 313–315

- workstation hijacking, 313

**patches**

- cyber attack kill chains, 574

- ICS

- patch management, 230

- patch vulnerability, 228–229

- managing, 551–554

- virtual patching, ModSecurity WAF, 293

**PCI (Payment Card Industry), PCI-DSS, 30–32**

**penetration testing, 265**

**people management**

- best practices, 175–176

- human resource security, 160–162

- current employees, 164–165

- dual operator policies, 165

- hiring process, 162

- hiring process, background checks/screening, 162–163

- hiring process, directory servers, 164

- hiring process, employment agreements, 163

- hiring process, job descriptions, 164

- limited reliance on key employees, 165

- privileges, 165

- remote working, 176

- separation of employee duties, 165

- termination of employment, 165–166

- vacations, 165

- security awareness/education, 166, 168

- awareness program communication materials, 170–172

- awareness program evaluation, 172

- certification, 174–175

- culture of security, 168

- cybersecurity essentials program, 173

- cybersecurity learning continuum, phases of, 167

- NIST ATE, 172

- processes of, 169–170

- role-based training, 173–174

- SP 800-16, 166

- SP 800-50, 166

**performance, 393, 397–398**

- APM, 285–286

- business continuity readiness, evaluating performance, 650–653

- internal audits, 653–654

- management reviews, 654

- managing, 383–384

- performance measures and security management, 139

- security performance, 678

- compliance monitoring, 690–691
- metrics, 678–679
- metrics, defined, 682–683
- metrics, development process, 683–685
- metrics, examples of, 680–681
- metrics, monitoring/reporting, 686–688
- metrics, risk reporting, 688–689
- metrics, sources of, 679–680
- metrics, values of, 682
- monitoring/reporting, 686–688
- risk reporting, 688–689

### **phishing**

- defined, 92, 565
- spear phishing, defined, 571

### **physical asset management, 210–211**

- best practices, 244–245
- CMDB, 212
- HAM, 211–212
  - acquisition phase, 214
  - average life cycle duration of common hardware, 216
  - deployment phase, 214–215
  - disposition phase, 216
  - management phase, 215–216
  - planning phase, 213–214

### **ICS**

- defined, 223
- elements of, 224–225
- IT systems versus, 225–228
- security, 227–228, 229–231
- threats/vulnerabilities, 228–229

### **mobile devices**

- ecosystem of, 234–236
- EMM systems, 242–243
- enterprise infrastructures, 242–243
- network protocols/services, 241–242
- physical access, 242
- resources, 243
- security, 231–233, 243
- security strategies, 238–239
- technology stacks, 233–234, 239–240
- threats/vulnerabilities, 236–237
- vetting applications, 240–241

- office equipment, 217
  - cryptographic erasure, 222–223
  - equipment disposal, 222–223
  - OS security, 219
  - physical security, 219
  - security controls, 219–222
  - threats/vulnerabilities, 217–219

### **physical network management, 423**

- NAP, 423
- network documentation, 423
- telecommunication cables, 423
- TIA-492, 423–426

### **physical security**

- best practices, 619
- controls, 615–616
  - assessments, 618–619
  - baselines, 617–618
- defense in depth strategies, 610–612
- defined, 606
- PSO, 609–610
- security maps, depth of security, 611–612
- threats, 606
  - environmental threats, 607–608, 612–614
  - human-caused physical threats, 609, 615
  - preventing/mitigating, 612–615
  - technical threats, 608–609, 614–615

### **PII (Personally Identifiable Information), 112, 261–262**

### **pilot runs, implementation/assessment phase (NIST SDLC), 252**

### **PKI (Public Key Infrastructure), 536**

- architecture of, 538–540
- best practices, 542
- CA, 539–540
- managing, 540–541
- public key certificates, 536–538
- RA, 539
- relying parties, 539–540
- repositories, 539

### **planning**

- capacity planning, 138
- capital planning, security planning, 142–145
- changes, change management, 387

- contingency planning and security management, 139
- firewall implementations, 428–429
- security planning, 138
  - capital planning, 142–145
  - defined, 140
  - example of, 141–142
  - process of, 141–142
  - requirements, 142
  - security policies, 145
  - security policies, AUP, 146, 152–153
  - security policies, categories of, 146–147
  - security policies, information security strategic planning, 146
  - security policies, managing, 151
  - security policies, monitoring, 151–152
  - security policies, Router and Switch Security Policy (SANS Institute), 148–150
  - security policies, security-related documents, 145–146
  - security policies, templates, 147–150
  - SP 800-18, 140–141
- strategic planning, 47
  - defined, 47
  - enterprise strategic planning, 47
  - framework of, 51–52
  - information security strategic planning, 50
  - IT strategic planning, 48
- planning phase (HAM), 213–214**
- POA&M (Plans of Action and Milestones), 269, 272**
- policies**
  - AUP, 146, 152–153
    - email, 434–435
    - IM, 436–437
  - SANS Institute AUP template, 152–153
- BYOD policies, 173
- dual operator policies, human resource security, 165
- firewall policies, 428
- incident management policies, 580–581
- log management policy, 558–559
- privacy policies
  - COPPA, 195
  - Electronic Communications Privacy Act, The, 195
  - FACTA, 195
  - Federal Policy for the Protection of Human Subjects, 195
  - FERPA, 195
  - GDPR, 193–195
  - GLBA, 195
  - HIPAA, 195
  - ISO 29100, 192
  - Privacy Act of 1974, The, 195
- Router and Switch Security Policy (SANS Institute), 148–150
- security policies, 145
  - AUP, 146, 152–153
  - categories of, 146–147
  - defined, 9
  - IM, 437–438
  - information security strategic planning, 146
  - managing, 151
  - monitoring, 151–152
  - NIST SP 800-53, 63
  - security-related documents, 145–146
  - templates, 147–150
- polymorphic droppers, 488**
- popular password attacks, 313**
- port administration, VoIP networks, 443**
- port mirroring, 511**
- portfolio management practices (APFM), 284–285**
- possession factor (user authentication), 310**
- possession-based authentication. See hardware tokens**
- power outages (undervoltage), 608**
- PowerShell, 576**
- presentation attacks, 339–340**
- print logs, office equipment threats/vulnerabilities, 218**
- privacy**
  - information management, 186–188
    - Chase Bank online privacy policy, 190
    - collecting information, 189

- disseminating information, 190–191
- Google privacy policy, 190
- invasions, 190–191
- principles/policies, 191–198
- privacy controls, 196–198
- processing information, 189–190
- security's relationship to privacy, 188
- threats to privacy, 189–191
- U.S. privacy laws/regulations, 195
- principles/policies
  - COPPA, 195
  - Electronic Communications Privacy Act, The, 195
  - FACTA, 195
  - Federal Policy for the Protection of Human Subjects, 195
  - FERPA, 195
  - GDPR, 193–195
  - GLBA, 195
  - HIPAA, 195
  - ISO 29100, 192
  - Privacy Act of 1974, The, 195
- Privacy Act of 1974, The, 195
- threats to privacy
  - aggregation, 190
  - appropriation, 191
  - blackmail, 191
  - breach of confidentiality, 190
  - decisional interference, 191
  - disclosure, 190
  - distortion, 191
  - exclusion, 190
  - exposure, 190
  - identification, 190
  - increased accessibility, 191
  - insecurity, 190
  - interrogation, 189
  - intrusion, 191
  - secondary use, 190
  - surveillance, 189
- private clouds, 468–469**
- privileges**
  - elevation of privileges, 90
  - human resource security, 165
  - least privilege, 230

- PRM (Performance Reference Models), 60**
- processing information, threats to privacy, 189–190**
- product/service flows (supply chains), 450**
- projects function, security management, 140**
- pseudorandom number generators, 535**
- PSO (Physical Security Officers), 609–610**
- public clouds, 468, 469–470**
- public key encryption, 520–521**
- PUP (Potentially Unwanted Programs), 488, 490**

## Q

- QA (Quality Assurance), system development, 277**
- qualitative risk assessment, 108–110, 111–112**
- quantitative risk assessment, 107–108, 109–110**

## R

- RA (Registration Authorities), 539**
- RACI charts, security governance, 66–67**
- ransomware, 90, 489**
- RAT (Remote Access Trojans), 489**
- RBAC (Role-Based Access Control), 349, 351–353**
- real-time antivirus software, VoIP networks, 443**
- records management, 198–200, 202–204**
- recovery/restoration plans, 646–647, 657–659**
- reengineering, APFM, 284**
- reliance on key employees, human resource security, 165**
- relying parties (PKI), 539–540**
- remote access attacks, 92**
- remote access security, ICS, 230**
- remote diagnostics, ICS, 225**
- remote network maintenance, 429–430**

**remote working, 176****reports**

- risk assessment reports, 92–93
  - Cisco Annual Cybersecurity Reports, 98
  - ENISA Threat Landscape Reports, 95–96
  - Fortinet Threat Landscape Reports, 98
  - Threat Horizon Reports, 94–95
  - Trustwave Global Security Reports, 97
  - Verizon DBIR, 93–94
- risk reporting (security performance), 688–689
- vulnerability reports, 551

**repositories (PKI), 539****repudiation threats, 89****requirements, security planning, 142****residual risk, 76****responsive controls, 101****reverse proxy servers**

- defined, 293
- ModSecurity WAF, 293

**RFID (Radio Frequency Identification) tags, 185****risk**

- avoidance, 130–131
- criteria, defined, 76
- CRO, security governance, 55
- defined, 4, 76
- determination, 128
- ERM committees, 65
- evaluating, 76, 128–129
- identifying, 76
- level of risk, defined, 76–77
- managing, 76, 80
  - ISO 27005 information security risk management, 81–84
- NIST risk management framework, 179–183
- SCRM, 453–456
- security management and, 139
- X.1055 risk management process, 80–81
- reducing, 130
- reporting (security performance), 688–689
- retention/acceptance, 130
- transferring, 131
- treatments, defined, 76

**risk analysis**

- defined, 76
- events, threat event frequency, estimating, 118–119
- FAIR, 114, 115–116
  - BIRT, 126–127
  - impact assessment, 122–123
  - likelihood assessments, 116–118
  - loss estimation, 123–126
  - loss event frequency, 121–122
  - Open Group security standards, 114–115
  - risk assessment matrices, 120–121
- risk avoidance, 130–131
- risk determination, 128
- risk evaluation, 128–129
- risk retention/acceptance, 130
- risk transfer, 131
- risk treatment, 129–130
- simple risk analysis worksheet, 113–114

**risk assessment, 74–75, 78, 80**

- assets
  - asset register, 87–88
  - business assets, 87
  - defined, 75, 77
  - determining future problems, 79
  - hardware assets, 85
  - identifying, 84–85
  - information assets, 86–87
  - software assets, 85
- BCM, 632–634
- best practices, 131–132
- biometric authentication, 340–341
- cloud computing, 475–476
- container virtualization, defined, 85
- control identification, 98–99
  - avoidance controls, 100
  - checklist of controls, 101–102
  - deterrent controls, 100–101
  - online catalog of security controls, 99–100
  - responsive controls, 101
  - vulnerability controls, 101
- costs of, 160
- defined, 76

- EUDA, 296–297
- events
  - defined, 75
  - threat event frequency, estimating, 118–119
- FAIR, 114, 115–116
  - BIRT, 126–127
  - impact assessment, 122–123
  - likelihood assessments, 116–118
  - loss estimation, 123–126
  - loss event frequency, 121–122
  - Open Group security standards, 114–115
  - risk assessment matrices, 120–121
- impact
  - defined, 75
  - determining risk, 77
- level of risk, defined, 76–77
- likelihood
  - defined, 76
  - determining risk, 77
- likelihood assessments, 116–118
- NFV, 85
- OWASP Risk Rating Methodology, 294
- PII, 112
- qualitative risk assessment, 108–110, 111–112
- quantitative risk assessment, 107–108, 109–110
- reports, 92–93
  - Cisco Annual Cybersecurity Reports, 98
  - ENISA Threat Landscape Reports, 95–96
  - Fortinet Threat Landscape Reports, 98
  - Threat Horizon Reports, 94–95
  - Trustwave Global Security Reports, 97
  - Verizon DBIR, 93–94
- residual risk, defined, 76
- RoE, 76
- SDN, defined, 85
- security categories, 110–111
- security control, defined, 76
- security incidents, defined, 76
- terminology of, 75–76
- threat actions, defined, 75
- threat agents, defined, 75
- threats, 89
  - adware, 91
  - auto-rooters, 91
  - backdoors (trapdoors), 91
  - business resource threats, 89
  - classifying, 89–90
  - code injection, 92
  - data tampering, 89
  - DDoS attacks, 92
  - defined, 75, 76
  - determining future problems, 79
  - determining risk, 77
  - DNS attacks, 92
  - DoS attacks, 90, 92
  - downloaders, 91
  - droppers, 91
  - elevation of privileges, 90
  - environmental threats, 89
  - exploit kits, 91
  - exploits, 91
  - flooders, 91
  - hackers (crackers), 92
  - hostile actors, 89
  - identifying, 89
  - information disclosure, 90
  - injection flaws, 92
  - keyloggers, 91
  - logic bombs, 90
  - malware, 90
  - mobile codes, 91
  - password attacks, 92
  - phishing, 92
  - ransomware, 90
  - remote access attacks, 92
  - repudiation threats, 89
  - rootkits, 91
  - social engineering, 92
  - spam, 90
  - spammer programs, 91
  - spoofing identity, 89
  - spyware, 91
  - STRIDE threat model, 89–90
  - threat event frequency, estimating, 118–119

- Trojan horses, 91
- virus generators (kits), 91
- viruses, 90
- website exploits, 92
- worms, 90
- zombies (bots), 91
- value proposition, defined, 123
- VM, defined, 84
- vulnerabilities
  - categories of, 103
  - defined, 76
  - determining future problems, 80
  - determining risk, 78
  - estimating, 119–120
  - identifying, 102
  - NVD, 103–104

## **RM (Reference Models)**

- ARM, 60–61
- assets of, 62
- BRM, 60
- DRM, 60
- enterprise architecture RM, 59–62
- IRM, 61
- PRM, 60
- relationships between components, 61
- SRM, 61–62

## **RoE (Risk of Exposure), 76**

## **rogue AP (Access Points), wireless network security, 427**

## **role-based training, security awareness/education, 173–174**

## **rootkits, 91, 489**

## **Router and Switch Security Policy (SANS Institute), 148–150**

## **RPO (Recovery Point Objectives), 632**

## **RTO (Recovery Time Objectives), 632**

## **rule-based recognition (DLP), 509**

# **S**

## **S/MIME, 433**

## **SaaS (Software as a Service), 467–468**

## **SABSA (Sherwood Applied Business Security Architecture), 483–487**

## **SAN (Storage Area Networks), 377–379**

## **SANS Institute**

- AUP template, 152–153
- computer security training and certification, 175
- Router and Switch Security Policy, 148–150

## **scanning for vulnerabilities, 549–551**

## **SCM (Supply Chain Management), 449**

- best practices, 478–479
- elements of, 451–452
- flows, 450–451
- ICT supply chains
  - defined, 449
  - flows, 450–451
  - SCRM, 453–456
  - SCRM, threats, 456–459

- SCRM, 453–456
  - best practices, 463–466
  - exfiltration, 457
  - IPR, 455
  - KPI, 455
  - security controls, 460–463
  - threats, 456–459
  - vulnerabilities, 459–460
- security controls, 460–463
- supply chains, defined, 449
- threats, 456–459
- vulnerabilities, 459–460

## **scrapers, 489**

## **screen locks (mobile devices), 242**

## **screening employees/background checks, 162–163**

## **SCRM (Supply Chain Risk Management), 453–456**

- best practices, 463–466
- exfiltration, defined, 457
- IPR, 455
- KPI, 455
- security controls, 460–463
- threats, 456–459
- vulnerabilities, 459–460

## **SDLC (System Development Life Cycle), 248–249**

### **NIST SDLC**

- development/acquisition phase, 250–251
- development/acquisition phase, security, 264–266
- disposal phase, 252
- disposal phase, security, 272–273
- implementation/assessment phase, 251–252
- implementation/assessment phase, security, 266–270
- incorporating security, 259–260
- incorporating security, development/acquisition phase, 264–266
- incorporating security, disposal phase, 272–273
- incorporating security, implementation/assessment phase, 266–270
- incorporating security, initiation phase, 260–263
- incorporating security, operations/maintenance phase, 270–272
- initiation phase, 249–250
- initiation phase, security, 260–263
- operations/maintenance phase, 252
- operations/maintenance phase, security, 270–272

### **SGP SDLC, 253–254**

## **SDN (Software-Defined Networking), 85**

### **secondary use, privacy threats, 190**

### **secrets, biometric authentication, 345**

### **secure hash functions, 522–524**

### **security**

- accreditation. *See* authorization
- applications, 237, 287
  - business application registers, 287–288
  - external application security, 289
  - internal application security, 288–289
  - web applications, 293
  - web applications, policies, 294–295
  - web applications, risks, 289–291
  - web applications, WAF, 291–293
- authorization, 270

### implementation/assessment phase (NIST SDLC), 269

### operations/maintenance phase (NIST SDLC), 272

- awareness/education, 166, 168
  - awareness program communication materials, 170–172
  - awareness program evaluation, 172
- certification, 174–175
- culture of security, 168
- cybersecurity essentials program, 173
- cybersecurity learning continuum, phases of, 167
- NIST ATE, 172
- processes of, 169–170
- role-based training, 173–174
- SP 800-16, 166
- SP 800-50, 166
- categories of, 110–111
- classification process, information management, 183–185
- cloud computing, 473
  - cloud-based applications, 232
  - risk assessment, 475–476
  - threats, 474–475
- contingency training, 267–269
- controls
  - defined, 15, 76
  - office equipment, 219–222
  - SCRM, 460–463
- customer data, 361
- EUDA security framework, 297–300
- event logs, 554–556
  - determining what to log, 557
  - log management policy, 558–559
  - objective of, 556
  - potential log sources, 556–557
  - securing data, 557–558
- firewalls, 404
  - application-layer firewalls, VoIP networks, 443
  - characteristics of, 404–405



- cyber attack kill chains, 574
- limitations of, 406
- network-based firewalls, 292
- planning, 428–429
- policies, 428
- WAF, 291–293, 574
- governance, 138
  - best practices, 69–70
  - CEO, 55
  - CIO, 55
  - CISO, 55
  - components of, 47
  - COO, 55
  - CPO, 55
  - CRO, 55
  - CSO, 55
  - defined, 43
  - desired outcomes, 46
  - effectiveness of, 68–69
  - enterprise architecture integration, 58
  - evaluating, 68–69
  - framework of, 63
  - information security architectures, 58
  - information security governance, defined, 42–43
  - ISMS, 44
  - principles of, 45–46
  - reporting relationships for, 56
  - roles/responsibilities of, 55, 57–58
  - security direction, 64–67
  - security management and, 138
  - security programs, defined, 43
  - stakeholders, defined, 45–46
  - strategic planning, 47, 48–50, 51–52
- GPS (location services), 237
- human resource security, 160–162
  - current employees, 164–165
  - dual operator policies, 165
  - hiring process, 162
  - hiring process, background checks/screening, 162–163
  - hiring process, directory servers, 164
  - hiring process, employment agreements, 163
  - hiring process, job descriptions, 164
  - limited reliance on key employees, 165
  - privileges, 165
  - remote working, 176
  - separation of employee duties, 165
  - termination of employment, 165–166
  - vacations, 165
- hypervisors, 376
- IM security policy, 437–438
- incidents, defined, 76
- information security, 4, 68–69
  - COBIT 5, 29–30, 64–66
  - information security architectures, 58
  - information security governance, defined, 42–43
  - information security management, defined, 43
  - information security reports, 53–55
  - information security strategic planning, 50
  - ISMS, 44
  - ISO/IEC 27000 suite of information security standards, 12–21
  - Standard of Good Practice for Information Security (SGP), 9–12
- location services, 237
- managing, 137, 393, 398–399
  - awareness/training, 138
  - best practices, 154
  - capacity planning, defined, 138
  - CISO, role in, 137, 138–140
  - configuration management, 139
  - consistency in security, 139
  - contingency planning, 139
  - external requirements function, 140
  - incident response, 139
  - ISM, role in, 137–138
  - monitor function, 140
  - performance measures, 139
  - projects function, 140
  - risk management and, 139
  - security governance, 138

- security planning, defined, 138
- security products/services acquisition, 138
- support function, 139
- system development life cycle, 138
- maps, depth of security, 611–612
- mobile devices, 231–233, 238–239
- network management, device configuration, 421–423
- network security, 4
- NIST SDLC, 259–260
  - development/acquisition phase, 264–266
  - disposal phase, 272–273
  - implementation/assessment phase, 266–270
  - initiation phase, 260–263
  - operations/maintenance phase, 270–272
- planning
  - capital planning, 142–145
  - defined, 138, 140
  - example of, 141–142
  - process of, 141–142
  - requirements, 142
  - security policies, 145–150, 151–153
  - SP 800-18, 140–141
- policies. *See* policies
- privacy's relationship to security, 188
- programs, defined, 43
- servers, requirements, 368–370
- technical security management, security architectures, 483–487
- virtualization
  - hypervisors, 376
  - issues with security, 374–375
- VoIP networks, 443
- wireless network security
  - hackers (crackers), 427
  - VPN, 426–427
- Security Accreditation Packages, 269**
- security champions, 605–606**
- security incident management frameworks, 577–578**
  - best practices, 597–598
  - emergencies, handling, 590–592
- forensics, 592–593
  - collection phase, 594–595
  - identification phase, 594
  - preparation phase, 593–594, 595–596
  - preservation phase, 595
  - reporting phase, 596
- gathering information, 583
- incident handling checklist, 589
- incident response process, 584–585
  - containment/eradication/recovery phase, 587–588
  - detection/analysis phase, 586–587
  - incident handling checklist, 589
  - post-incident activity phase, 588–589
  - preparation phase, 585
- ISMS and, 579–580
- objectives of, 579
- policies, 580–581
- resources, 578–579
- roles/responsibilities of, 581–582
- tools, 583–584
- security monitoring**
  - best practices, 691–692
  - security audit trails
    - application-level audit trails, 671
    - defined, 667
    - network-level audit trails, 671
    - physical access audit trails, 671–672
    - system-level audit trails, 671
    - user-level audit trails, 671
  - security audits
    - controls, 673–677
    - data collection, 668–672
    - defined, 666–667
    - elements of, 668
    - external audits, 672–673
    - internal audits, 672
    - logs, 671–672
    - objectives of, 667
  - security performance, 678
    - compliance monitoring, 690–691
    - metrics, 678–679

- metrics, defined, 682–683
- metrics, development process, 683–685
- metrics, examples of, 680–681
- metrics, monitoring/reporting, 686–688
- metrics, risk reporting, 688–689
- metrics, sources of, 679–680
- metrics, values of, 682
- monitoring/reporting, 686–688
- risk reporting, 688–689
- SecurityFocus, vulnerability management, 549**
- SED (Self-Encrypting Drives), 222**
- SEM (Security Event Management), 559–560**
  - assessing security, 562–563
  - best practices, 561–563
  - deploying, 563
  - functions of, 560–561
  - planning, 561–562
  - simplifying security, 563
- sensitive information**
  - defined, 171–172
  - managing, 204–205
- sensors, ICS, 224**
- separation of duties, human resource security, 165**
- servers. *See also* virtualization**
  - directory servers, defined, 164
  - DoS attacks, 368
  - reverse proxy servers
    - defined, 293
    - ModSecurity WAF, 293
  - security, requirements, 368–370
  - threats to, 368
  - web server logs, 557
- service management layer (network management systems), 404**
- services protocols, office equipment, 217–218**
- SGP (Standard of Good Practice for Information Security), 7–10**
  - areas of, 10–12
  - categories of, 10–12
  - environment security, 277
  - ISF SGP, security governance, 64
  - mapping ISO 27000 suite to ISF SGP, 18–21
  - SDLC, 253–254
- shadow password files, 319**
- side-channel attacks, 242**
- SIEM (Security Information and Event Management), 569**
- signatures (digital), 518, 524–525**
- simple risk analysis worksheet, 113–114**
- single version of truth. *See* golden records**
- SLA (Service-Level Agreements), 379–381**
  - cloud service providers, 382–383
  - CSIRT, 381–382
  - ITSM, 379
  - MSP, 379
- smart cards, user authentication, 323–325**
- SOC (Security Operations Centers), 97**
- social engineering**
  - defined, 92
  - social engineering attacks, defined, 571
- software**
  - antivirus software, cyber attack kill chains, 574
  - assets, defined, 85
  - COTS software, 288
  - real-time antivirus software, VoIP networks, 443
  - SDN, defined, 85
- source code repositories, 263**
- source routing attacks, 411**
- SP 800-12, 26**
- SP 800-16, 166**
- SP 800-18, 140–141**
- SP 800-37, 261, 267–269**
- SP 800-41, 428**
- SP 800-45, 434**
- SP 800-50, 166**
- SP 800-53, 63, 196–198**
- SP 800-53A, 267–269**
- SP 800-55, 26**
- SP 800-63, 307–310**
- SP 800-63B, 321, 340–341**
- SP 800-88, 272**
- SP 800-90A, 321, 534**

- SP 800-90B, 534**
- SP 800-90C, 534**
- SP 800-100, 26**
- SP 800-122, 198**
- SP 800-125, 374–376**
- SP 800-125A, 374–375**
- SP 800-144, 26**
- SP 800-162, 357–358**
- SP 800-177, 433**
- SP 800-178, 358**
- SP 1800, 26**
- SP 1800-3, 358**
- spam, 90**
- spammer programs, 91, 489**
- spear phishing, 571**
- specific account attacks, 313**
- SPF (Sender Policy Framework), 433**
- SPIT (Spam over Internet Telephone), 443**
- spoofing**
  - biometric spoofing, 339
  - identity spoofing, 89
- spyware, 91, 489**
- SRM (Security Reference Models), 61–62**
- SSCP (Systems Security Certified Practitioner), 175**
- SSID (Secure Set Identifiers), WAP, 426**
- SSO (Single Sign-On), 497**
- stakeholders, 45–46**
- Standard of Good Practice for Information Security (SGP), 7–10**
  - areas of, 10–12
  - categories of, 10–12
  - mapping ISO 27000 suite to ISF SGP, 18–21
- standards and best practices documents, 6–7, 36–37**
  - CIS CSC, 27–28
  - COBIT 5 for information security, 29–30
  - ISO/IEC 27000 suite of information security standards, 12–13
    - ISMS, 13–15
    - ISO 27001, 14, 15–16
    - ISO 27002, 14, 17–18
    - ISO 27005, 15
    - ISO 27014, 15
    - ISO 27036, 15
    - mapping to ISF SGP, 18–21
  - ITU-T security documents, 32–34
  - NIST cybersecurity framework and security documents, 21–22, 25–26
    - components of, 22–25
  - FIPS 200, 26
  - FIPS 800-27, 26
  - SP 800-12, 26
  - SP 800-55, 26
  - SP 800-100, 26
  - SP 800-144, 26
  - SP 1800, 26
- PCI-DSS, 30–32**
- Standard of Good Practice for Information Security (SGP), 7–10**
  - areas of, 10–12
  - categories of, 10–12
  - mapping ISO 27000 suite to ISF SGP, 18–21
- STARTTLS, 433**
- stateful inspection firewalls, 411–413**
  - application-level gateways, 413
  - circuit-level gateways, 413–414
- storage**
  - DAS, 377
  - local storage. *See* DAS
  - NAS, 378–379
  - network storage, 377
    - DAS, 377
    - NAS, 378–379
    - SAN, 377–379
  - SAN, 377–379
- strategic planning, 47**
  - defined, 47
  - enterprise strategic planning, 47
  - framework of, 51–52
  - information security strategic planning, 50
  - IT strategic planning, 48
- STRIDE threat model, 89–90**
- subjects (system access), 348**
- supply chains. *See* SCM (Supply Chain Management)**

**support, security management, 139**

**surveillance, privacy threats, 189**

**switches, Router and Switch Security Policy (SANS Institute), 148–150**

**symmetric encryption, 518–520**

## **system access**

access control, 305, 347

ABAC, 349, 353–355

ABAC, attribute metadata, 355–357

ABAC, resources, 357–358

access rights, 348–349

ACL, 350–351

DAC, 349–351

discretionary access control, 312

MAC, 349

metrics, 358–360

objects, 348

RBAC, 349, 351–353

subjects, 348

authorization, 305, 306–307

best practices, 362–363

customer access

arrangements, 360

connections, 361

contracts, 361

data security, 361

defined, 360

defined, 305–306

functions of, 305

user authentication. *See* user authentication

## **system development**

best practices, 278

environments, 275–277

managing, 273–274

environments, 275–277

methodologies, 274–275

QA, 277

methodologies, 274–275

NIST SDLC. *See* SDLC

QA, 277

security, contingency training, 267–269

SGP SDLC, 253–254

waterfall development, 249

## **system owners, 261**

## **systems management**

backups, 384–386

best practices, 389–390

capacity management, 383–384

change management, 386–389

cloud service providers, 382–383

CSIRT, 381–382

defined, 366–367

elements of, 366–367

network storage, 377

DAS, 377

NAS, 378–379

SAN, 377–379

performance management, 383–384

servers. *See also* virtualization

security requirements, 368–370

threats to, 368

SLA, 379–381

cloud service providers, 382–383

CSIRT, 381–382

ITSM, 379

MSP, 379

trust relationships, 369

virtualization. *See also* servers

container virtualization, 374

hosted (nested) virtualization, 372

hosted virtualization security, 377

hypervisors, 371

hypervisors, functions of, 371

hypervisors, security, 376

hypervisors, types of, 371–374

infrastructure security, 376

native virtualization, 371–372, 373

security, hosted virtualization security, 377

security, infrastructure security, 376

security, issues with, 374–375

VM, 370

## **system-selected passwords, 321–322**

## T

---

**tampering with data, 89**

**tar pits, cyber attack kill chains, 575**

**TCO (Total Cost of Ownership), 281–283**

**technical security management**

best practices, 541–542

cryptography. *See* cryptography

defined, 482–483

DLP, 509

classifying data, 509–510

data at rest, 510–511

data in motion (or transit), 510, 511–512

data in use, 510, 512

database fingerprinting, 509

exact file matching/hash values, 510

partial document matching, 510

rule-based recognition, 509

DRM, 512

architecture of, 514–515

best practices, 515–517, 542

components of, 513–514

IAM, 496

architecture of, 497–498

best practices, 501–502, 542

defined, 496

federated identity management, 498–500

planning, 500–501

SSO, 497

intrusion detection, 502, 504

anomaly detection, 504–505

best practices, 508–509, 542

false negatives, 504–505

false positives, 504–505

HIDS, 503, 505–506

IDS, 502–503, 508–509

misuse detection, 504

NIDS, 503, 506–508

principles of, 503–504

true negatives, 505

true positives, 505

malware

best practices, 541

defined, 487

malware protection software, 494–496

nature of, 490

practical malware protection, 490–494

types of, 487–489

PKI, 536

architecture of, 538–540

best practices, 542

CA, 539–540

managing, 540–541

public key certificates, 536–538

RA, 539

relying parties, 539–540

repositories, 539

SABSA, 483–487

security architectures, 483–487

technical controls, defined, 482–483

**technical threats**

BCM, 627

local environment security, 608–609,  
614–615

**technical vulnerability management. *See*  
vulnerabilities**

**technology stacks**

applications, 234

firmware, 234

mobile devices, 239–240

mobile OS, 234

**telecommunication cables, physical network  
management, 423**

**telephony (IP)/conferencing, 443–444**

**templates (AUP), 152–153**

**termination of employment, human resource  
security, 165–166**

**tests**

business continuity readiness, 647–648,  
649–650

end-user testing, defined, 265

functional testing, defined, 265

integration testing, 251

OWASP Testing Guide, 295

penetration testing, defined, 265

UAT, 251

user testing, defined, 265

**theft of service, VoIP, 443**

**threat actions, 75**

**threat agents, 75**

**Threat Horizon Reports, 94–95**

**Threat Landscape Reports, 95–96**

**threats, 89**

- adware, defined, 91
- analyzing, 569–570
- APT, defined, 566
- auto-rooters, defined, 91
- backdoors (trapdoors), defined, 91
- BCM
  - environmental threats, 627
  - human-caused physical threats, 627–628
  - natural disasters, 626
  - system problems, 627
- business resource threats, defined, 89
- classifying, 89–90
- code injection, defined, 92
- data tampering, 89
- DDoS attacks, defined, 92
- defined, 5, 75–76
- determining risk, 77
- DNS attacks, defined, 92
- DoS attacks, 90, 92
- downloaders, defined, 91
- droppers, defined, 91
- elevation of privileges, 90
- environmental threats
  - defined, 89
  - local environment security, 607–608, 612–614
- event frequency, estimating, 118–119
- exploit kits, defined, 91
- exploits, defined, 91, 566
- flooders, defined, 91
- hackers (crackers), defined, 92
- hostile actors, 89
- human-caused physical threats, local environment security, 609, 615
- ICS, 228–229
- identifying, 89
- information disclosure, 90
- injection flaws, defined, 92
- intelligence, 563
  - analyzing threats, 569–570
  - benefits of, 566–568
  - gathering, 568–569
  - importance of, 566–568
  - SIEM, defined, 569
  - sources of threats, 564
  - types of threats, 564–565
- keyloggers, defined, 91
- local environment security
  - environmental threats, 607–608, 612–614
  - human-caused physical threats, 609, 615
  - technical threats, 608–609, 614–615
- logic bombs, defined, 90
- malware, defined, 90
- mobile codes, defined, 91
- mobile devices, 236–237
- office equipment, 217
  - DoS attacks, 218–219
  - information disclosure, 218
  - network services, 217–218
- password attacks, defined, 92
- phishing, defined, 92
- physical security
  - environmental threats, 607–608, 612–614
  - human-caused physical threats, 609, 615
  - technical threats, 608–609, 614–615
- privacy threats, 189–191
- ransomware, defined, 90
- remote access attacks, defined, 92
- repudiation threats, 89
- risk assessment, determining future problems, 79
- rootkits, defined, 91
- social engineering, defined, 92
- sources of, 564
- spam, defined, 90
- spammer programs, defined, 91
- spoofing identity, 89
- spyware, defined, 91

STRIDE threat model, 89–90  
 technical threats, local environment security, 608–609, 614–615  
 Trojan horses, defined, 91  
 types of, 564–565  
 virus generators (kits), defined, 91  
 viruses, defined, 90  
 website exploits, defined, 92  
 worms, defined, 90  
 zero-day threats, defined, 567  
 zombies (bots), defined, 91  
**TIA-492, 423–426**  
**tiny fragment attacks, 411**  
**traffic analysis/eavesdropping, wireless network security, 427**  
**training, role-based training, security awareness/education, 173–174**  
**trapdoors (backdoors), 91, 488**  
**Trojan horses, 91, 489**  
**true negatives (intrusion detection), 505**  
**true positives (intrusion detection), 505**  
**trust relationships, 369**  
**Trustwave Global Security Reports, 97**  
**truth, single version of. See golden records**

## U

---

**U.S. privacy laws/regulations, 195**  
**UAT (User Acceptance Testing), 251**  
**undervoltage (power outages), 608**  
**UNIX, password schemes, 315–316**  
**user authentication, 304, 307**

authenticators, 311  
 biometric authentication, 330–331  
   AAL, 341–347  
   accuracy of, 333, 335–336  
   artifact detection, 340  
   biometric spoofing, 339  
   costs of, 333  
   cryptographic devices, 345  
   FMR, 335–336  
   FNMR, 335–336  
   liveness detection, 340

lookup secrets, 345  
 memorized secrets, 345  
 operating characteristic curves, 336  
 operation of, 333–335  
 OTP devices, 345  
 PAD, 339–340  
 physical characteristics used in, 332–333  
 presentation attacks, 339–340  
 risk assessment, 341–347  
 security controls, 339–341  
 SP 800-63B guidelines, 340–341  
 threats to, 337–339  
 cryptography and, 518  
 factors of, 310–311  
 hardware tokens, 322, 325–327  
   memory cards, 322–323  
   OTP devices, 328–329  
   security controls, 330  
   smart cards, 323–325  
   threats to, 329–330  
 inherence factor, 310  
 knowledge factor, 310  
 multifactor authentication, 311–312  
 NIST SP 800-63 Digital Identity Model, 307–310  
 passwords. *See* passwords  
 possession factor, 310  
 VoIP networks, 443

## users

mistakes, exploiting, 314  
 passwords, 320  
 testing, defined, 265  
 user needs versus security implementation, 6

## V

---

**vacations, human resource security, 165**  
**value proposition, 123**  
**Verizon, Data Breach Investigations Reports, 93–94, 294**  
**vetting applications, 240–241**  
**virtual patching, ModSecurity WAF, 293**



**virtualization. See also servers**

- container virtualization, 85, 374
- hosted (nested) virtualization, 372, 377
- hypervisors, 371
  - functions of, 371
  - security, 376
  - types of, 371–374
- infrastructure security, 376
- native virtualization, 371–372, 373
- NFV, 85
- security
  - hosted virtualization security, 377
  - hypervisors, 376
  - infrastructure security, 376
  - issues with, 374–375
- VM, 370, 371

**virus generators (kits), 91, 488****viruses, 489**

- antivirus software, cyber attack kill chains, 574
- defined, 90
- real-time antivirus software, VoIP networks, 443

**VM (Virtual Machines), 370**

- defined, 84
- guest OS, 371

**VoIP (Voice over Internet Protocol) networks, 438**

- context, 440–442
- processing, 439–440
- security, 443
- signaling, 439
- threats, 442–443

**VPN (Virtual Private Networks), 417–418**

- defined, 241
- external network connections, 428
- firewall-based VPN, 420
- VoIP networks, 443
- wireless network security, 426–427

**vulnerabilities, 547**

- categories of, 103
- CERT teams, 548
- controls, 101

- defined, 5, 76
- determining risk, 78
- discovering known vulnerabilities, 548–549
- estimating, 119–120
- ICS, 228–229
- identifying, 102
- ISC, 549
- logs/reports, 551
- mobile devices, 236–237
- NVD, 103–104
  - CVSS metrics, 105–107
  - scoring example, 104–105
- office equipment, 217
  - DoS attacks, 218–219
  - information disclosure, 218
  - network services, 217–218
- Packet Storm, 549
  - patch management, 551–554
  - planning, 547–548
  - remediating vulnerabilities, 551–554
- risk assessment, determining future problems, 80
- scanning for vulnerabilities, 549–551
- SecurityFocus, 549

**W****WAF (Web Application Firewalls), 291–293, 574****WAP (Wireless Access Points)**

- network management, 416
- SSID, 426

**warm site backups, 386****waterfall development, 249****web analytics, 573****web applications**

- Open Web Application Security Project, 290–291
- security, 293
  - policies, 294–295
  - risks, 289–291
  - WAF, 291–293

**web drive-bys, 489**

**web server logs, 557**

**websites, exploits, 92**

**whitelisting**

application whitelisting, 164, 229

defined, 164

**wireless networks**

managing, 416–417

security

hackers (crackers), 427

network management, 426–427

VPN, 426–427

WAP, SSID, 426

**WMI (Windows Management  
Instrumentation), 576**

**work flows (organizational information/  
decision), cybersecurity management  
process, 36–37**

**workstation hijacking, 313**

**worms, 90, 489**

## **X - Y - Z**

---

**X.816 security audit and alarms framework.**

**See security monitoring, security  
audits**

**X.1055 risk management process,  
80–81**

**zero-day threats, 567**

**zombies (bots), 91, 489**