

FOURTH EDITION



# DEVELOPING CYBERSECURITY PROGRAMS AND POLICIES IN AN AI-DRIVEN WORLD

OMAR SANTOS

FREE SAMPLE CHAPTER



# **Developing Cybersecurity Programs and Policies in an AI-Driven World**

**Fourth Edition**

Omar Santos

**PEARSON**

Hoboken, New Jersey

# Developing Cybersecurity Programs and Policies in an AI-Driven World

Fourth Edition

Copyright © 2025 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced. 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.pearson.com/permissions](http://www.pearson.com/permissions).

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

ISBN-13: 978-0-13-807410-4

ISBN-10: 0-13-807410-0

*Library of Congress Cataloging-in-Publication Data: 2024909456*

\$PrintCode

## Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

## Special Sales

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).

**GM K12, Early Career and Professional Learning**  
Soo Kang

**Director, ITP Product Management**  
Brett Bartow

**Executive Editor**  
James Manly

**Development Editor**  
Christopher Cleveland

**Managing Editor**  
Sandra Schroeder

**Senior Project Editor**  
Mandie Frank

**Copy Editor**  
Kitty Wilson

**Indexer**  
Timothy Wright

**Proofreader**  
Donna E. Mulder

**Technical Editor**  
John Stuppi

**Publishing Coordinator**  
Cindy Teeters

**Designer**  
Chuti Prasertsith

**Compositor**  
codeMantra

## Contents at a Glance

Introduction .....	xviii
1        Understanding Cybersecurity Policy and Governance .....	2
2        Cybersecurity Policy Organization, Format, and Styles.....	46
3        Cybersecurity Frameworks .....	80
4        Cloud Security.....	132
5        Governance and Risk Management .....	176
6        Asset Management and Data Loss Prevention .....	220
7        Human Resources Security and Education .....	256
8        Physical and Environmental Security .....	290
9        Cybersecurity Operations (CyberOps), Incident Response, Digital Forensics, and Threat Hunting .....	320
10       Access Control Management.....	384
11       Supply Chain Security, Information Systems Acquisition, Development, and Maintenance .....	434
12       Business Continuity Management.....	474
13       Regulatory Compliance for Financial Institutions.....	514
14       Regulatory Compliance for the Health-care Sector.....	556
15       PCI Compliance for Merchants .....	600
16       Privacy in an AI-Driven Landscape .....	634
17       Artificial Intelligence Governance and Regulations .....	652
Appendix A: Answers to the Multiple Choice Questions .....	696
Index.....	716

# Table of Contents

<b>Introduction</b>	<b>xviii</b>
<b>Chapter 1: Understanding Cybersecurity Policy and Governance</b>	<b>2</b>
Information Security vs. Cybersecurity Policies . . . . .	6
Looking at Policy Through the Ages . . . . .	6
Policy in Ancient Times. . . . .	7
The U.S. Constitution as a Policy Revolution . . . . .	7
Policy Today . . . . .	8
Cybersecurity Policy . . . . .	10
What Are Assets? . . . . .	11
Characteristics of Successful Policy . . . . .	13
What Is the Role of Government? . . . . .	19
The Challenges of Global Policies . . . . .	28
Cybersecurity Policy Life Cycle . . . . .	28
Policy Development . . . . .	29
Policy Publication . . . . .	30
Policy Adoption . . . . .	32
Policy Review . . . . .	33
Summary . . . . .	34
<b>Chapter 2: Cybersecurity Policy Organization, Format, and Styles</b>	<b>46</b>
Policy Hierarchy . . . . .	47
Standards . . . . .	47
Baselines . . . . .	48
Guidelines . . . . .	49
Procedures . . . . .	49
Plans and Programs . . . . .	50
Writing Style and Technique . . . . .	51
Using Plain Language . . . . .	51

The Plain Language Movement . . . . .	52
Plain Language Techniques for Policy Writing . . . . .	53
Policy Format . . . . .	56
Understand Your Audience . . . . .	56
Policy Format Types . . . . .	57
Policy Components . . . . .	58
Summary . . . . .	69
<b>Chapter 3: Cybersecurity Frameworks</b>	<b>80</b>
Confidentiality, Integrity, and Availability (CIA) . . . . .	81
What Is Confidentiality? . . . . .	82
What Is Integrity? . . . . .	88
What Is Availability? . . . . .	89
Who Is Responsible for CIA? . . . . .	93
What Is a Cybersecurity Framework? . . . . .	94
What Is NIST's Function? . . . . .	94
So, What About ISO? . . . . .	95
The Importance of ISO Standards for Cybersecurity . . . . .	96
NIST Cybersecurity Framework . . . . .	110
The Objective of the NIST Cybersecurity Framework . . . . .	111
The Scope of the CSF . . . . .	112
The NIST Framework Core Components . . . . .	112
Implementation Examples and Informative References . . . . .	114
The NIST Cybersecurity Framework and the NIST Privacy Framework . . . . .	116
Summary . . . . .	118
<b>Chapter 4: Cloud Security</b>	<b>132</b>
Why Cloud Computing? . . . . .	133
Scalability vs. Elasticity . . . . .	134
Cost-Benefit Analysis of Cloud Computing . . . . .	135

Cloud Computing Models. . . . .	139
Software as a Service (SaaS). . . . .	139
Infrastructure as a Service (IaaS). . . . .	140
Platform as a Service (PaaS). . . . .	140
Function as a Service (FaaS). . . . .	140
The Cloud Shared Responsibility Model. . . . .	141
Cloud Governance . . . . .	141
Centralized Control and Coordination. . . . .	142
Standardization and Compliance. . . . .	142
Preventing Shadow IT. . . . .	146
The Role of Cloud Governance . . . . .	147
Transferring Regulatory Responsibility and Costs to the Cloud . . . . .	148
Multitenancy . . . . .	150
Core Components of the Cloud Computing Reference Architecture . . . . .	151
Key Concepts and Functional Layers of Cloud Computing . . . . .	152
The Importance of the Reference Architecture. . . . .	153
Understanding Top Cybersecurity Risks in Cloud Computing . . . . .	153
Data Breaches and Loss . . . . .	154
Inadequate Identity and Access Management (IAM). . . . .	155
Leveraging Identity Federation . . . . .	156
Automating the IAM Processes and Mitigating Associated Risks . . . . .	157
Misconfiguration and Inadequate Change Control . . . . .	161
Lack of Visibility and Control Over Data . . . . .	163
Insider Threats. . . . .	164
Advanced Persistent Threats (APTs) and Sophisticated Malware Against Cloud-Based Solutions . . . . .	165
AI and the Cloud: Revolutionizing the Future of Computing . . . . .	166
Summary . . . . .	168

<b>Chapter 5: Governance and Risk Management</b>	<b>176</b>
Understanding Cybersecurity Policies . . . . .	177
What Is Governance? . . . . .	177
What Is Meant by Strategic Alignment? . . . . .	177
Regulatory Requirements . . . . .	179
User-Level Cybersecurity Policies . . . . .	180
Vendor Cybersecurity Policies . . . . .	180
Cybersecurity Vulnerability Disclosure Policies . . . . .	180
Client Synopsis of Cybersecurity Policies . . . . .	181
Who Authorizes Cybersecurity Policy? . . . . .	183
What Is a Distributed Governance Model? . . . . .	184
Evaluating Cybersecurity Policies . . . . .	187
Revising Cybersecurity Policies: Change Drivers . . . . .	190
NIST Cybersecurity Framework Governance Subcategories and Informative References . . . . .	191
Regulatory Requirements . . . . .	193
The European Union Cyber Resilience Act . . . . .	195
Cybersecurity Risk . . . . .	197
Is Risk Bad? . . . . .	198
Understanding Risk Management . . . . .	199
Risk Appetite and Tolerance . . . . .	201
What Is a Risk Assessment? . . . . .	202
Risk Assessment Methodologies . . . . .	204
Summary . . . . .	207
<b>Chapter 6: Asset Management and Data Loss Prevention</b>	<b>220</b>
Information Assets and Systems . . . . .	221
Who Is Responsible for Information Assets? . . . . .	222
Information Classification . . . . .	224
How Does the Federal Government Classify Data? . . . . .	226
Why Is National Security Information Classified Differently? . . . . .	228



Who Decides How National Security Data Is Classified? . . . . .	230
How Does the Private Sector Classify Data? . . . . .	230
Can Information Be Reclassified or Even Declassified? . . . . .	232
Labeling and Handling Standards . . . . .	233
Why Label? . . . . .	233
Why Handling Standards? . . . . .	233
Information Systems Inventory . . . . .	236
Why an Inventory Is Necessary and What Should Be Inventoried . . .	236
Understanding Data Loss Prevention Technologies . . . . .	242
Summary . . . . .	245
<b>Chapter 7: Human Resources Security and Education</b>	<b>256</b>
The Employee Life Cycle . . . . .	257
What Does Recruitment Have to Do with Security? . . . . .	259
What Happens in the Onboarding Phase? . . . . .	265
What Is User Provisioning? . . . . .	266
What Should an Employee Learn During Orientation? . . . . .	267
Why Is Termination Considered the Most Dangerous Phase? . . . . .	268
The Importance of Employee Agreements . . . . .	269
What Are Confidentiality, or Nondisclosure, Agreements? . . . . .	269
What Is an Acceptable Use Agreement? . . . . .	270
The Importance of Security Education and Training . . . . .	272
NICE Work Roles and Categories . . . . .	273
NICE Insider Threat Analysis . . . . .	274
Influencing Behavior with Security Awareness . . . . .	276
Teaching a Skill with Security Training . . . . .	276
Security Education Is Knowledge Driven . . . . .	276
Summary . . . . .	278

<b>Chapter 8: Physical and Environmental Security</b>	<b>290</b>
Understanding the Secure Facility Layered Defense Model . . . . .	292
How Do We Secure the Site? . . . . .	293
How Is Physical Access Controlled? . . . . .	295
Protecting Equipment . . . . .	299
The Importance of Power to Processing . . . . .	299
How Dangerous Is Fire? . . . . .	301
What About Disposal of Devices Containing Data? . . . . .	303
Stop, Thief! . . . . .	306
Environmental Sustainability. . . . .	308
Summary . . . . .	310
<b>Chapter 9: Cybersecurity Operations (CyberOps), Incident Response, Digital Forensics, and Threat Hunting</b>	<b>320</b>
Incident Response. . . . .	321
What Is an Incident? . . . . .	322
How Are Incidents Reported? . . . . .	328
What Is an Incident Response Program? . . . . .	330
The Incident Response Process . . . . .	332
Tabletop Exercises and Playbooks . . . . .	335
Information Sharing and Coordination . . . . .	336
Operationalizing Threat Intelligence . . . . .	336
Computer Security Incident Response Teams (CSIRTs) . . . . .	339
Product Security Incident Response Teams (PSIRTs) . . . . .	341
Incident Response Training and Exercises . . . . .	348
What Happened? Investigation and Evidence Handling . . . . .	349
Documenting Incidents. . . . .	350
Working with Law Enforcement . . . . .	350
Understanding Threat Hunting . . . . .	351
Objectives of Threat Hunting . . . . .	351

The Threat Hunting Process . . . . .	351
Best Practices for Threat Hunting . . . . .	354
Using SIGMA for Incident Response and Threat Hunting . . . . .	356
Understanding Digital Forensic Analysis . . . . .	357
Data Breach Notification Requirements . . . . .	360
Is There a Federal Breach Notification Law? . . . . .	361
Does Notification Work? . . . . .	365
Summary . . . . .	368
<b>Chapter 10: Access Control Management</b>	<b>384</b>
Access Control Fundamentals . . . . .	385
What Is a Security Posture? . . . . .	386
How Is Identity Verified? . . . . .	388
What Is Authorization? . . . . .	393
Accounting. . . . .	398
Infrastructure Access Controls . . . . .	399
Why Segment a Network? . . . . .	400
What Is Layered Border Security? . . . . .	403
Remote Access Security . . . . .	409
User Access Controls . . . . .	416
Why Manage User Access? . . . . .	417
What Types of Access Should Be Monitored? . . . . .	419
Summary . . . . .	422
<b>Chapter 11: Supply Chain Security, Information Systems Acquisition, Development, and Maintenance</b>	<b>434</b>
Strengthening the Links: A Deep Dive into Supply Chain Security . . . . .	435
Emerging Threats to Supply Chains . . . . .	436
Strategies for Enhancing Supply Chain Security . . . . .	437
The Critical Role of SBOMs in Enhancing Supply Chain Security . . .	437
Artificial Intelligence Bill of Materials (AI BOM). . . . .	440

System Security Requirements . . . . .	441
What Is SDLC? . . . . .	441
NIST's Secure Software Development Framework (SSDF) . . . . .	444
What About Commercially Available or Open Source Software? . . . . .	445
The Testing Environment . . . . .	446
Protecting Test Data . . . . .	447
Secure Code . . . . .	448
The Open Worldwide Application Security Project (OWASP) . . . . .	449
Cryptography . . . . .	453
Why Encrypt? . . . . .	455
Regulatory Requirements . . . . .	455
What Is a Key? . . . . .	455
What Is PKI? . . . . .	456
Why Protect Cryptographic Keys? . . . . .	457
Digital Certificate Compromise . . . . .	458
Post-Quantum Cryptography: Securing the Future of Digital Security . . . . .	460
Summary . . . . .	462
<b>Chapter 12: Business Continuity Management</b>	<b>474</b>
Emergency Preparedness . . . . .	475
What Is a Resilient Organization? . . . . .	476
Regulatory Requirements . . . . .	477
Business Continuity Risk Management . . . . .	479
What Is a Business Continuity Threat Assessment? . . . . .	479
What Is a Business Continuity Risk Assessment? . . . . .	480
What Is a Business Impact Assessment? . . . . .	482
The Business Continuity Plan . . . . .	485
Roles and Responsibilities . . . . .	485
Disaster Response Plans . . . . .	488

Business Continuity and Disaster Recovery in Cloud Services. . . . .	493
Key Components of BC/DR in Cloud Computing . . . . .	493
Best Practices for BC/DR in Cloud Services . . . . .	493
Business Continuity and Disaster Recovery Strategies in Cloud Computing vs. Traditional Data Centers . . . . .	494
Operational Contingency Plans . . . . .	495
The Disaster Recovery Phase . . . . .	497
The Resumption Phase . . . . .	499
Plan Testing and Maintenance . . . . .	500
Why Is Testing Important? . . . . .	500
Plan Maintenance . . . . .	502
Summary . . . . .	504
<b>Chapter 13: Regulatory Compliance for Financial Institutions</b>	<b>514</b>
The Gramm-Leach-Bliley Act . . . . .	515
What Is a Financial Institution? . . . . .	516
Regulatory Oversight . . . . .	518
What Are the Interagency Guidelines? . . . . .	520
New York's Department of Financial Services Cybersecurity Regulation. . . . .	533
What Is a Regulatory Examination? . . . . .	535
Examination Process . . . . .	535
Examination Ratings . . . . .	536
Personal and Corporate Identity Theft. . . . .	537
What Is Required by the Interagency Guidelines Supplement A? . . .	537
Authentication in an Internet Banking Environment. . . . .	538
Regulation of Fintech, Digital Assets, and Cryptocurrencies . . . . .	540
The Rise of Fintech and Digital Assets . . . . .	540
Regulatory Responses . . . . .	541
Summary . . . . .	542

<b>Chapter 14: Regulatory Compliance for the Health-care Sector</b>	<b>556</b>
The HIPAA Security Rule	558
What Is the Objective of the HIPAA Security Rule?	559
How Is the HIPAA Security Rule Organized?	560
What Are the Administrative Safeguards?	562
What Are the Physical Safeguards?	571
What Are the Technical Safeguards?	574
What Are the Organizational Requirements?	578
What Are the Policies and Procedures Standards?	580
Mapping the HIPAA Security Rule to the NIST Cybersecurity Framework	581
The HITECH Act and the Omnibus Rule	581
What Changed for Business Associates?	582
What Are the Breach Notification Requirements?	584
Understanding the HIPAA Compliance Enforcement Process	586
Summary	588
<b>Chapter 15: PCI Compliance for Merchants</b>	<b>600</b>
Protecting Cardholder Data	601
What Is the PAN?	602
The Luhn Algorithm.	603
What Is the PCI DDS Framework?	604
Business-as-Usual Approach	605
What Are the PCI Requirements?	606
PCI Compliance.	616
Who Is Required to Comply with PCI DSS?	616
What Is a Data Security Compliance Assessment?	617
What Is the PCI DSS Self-Assessment Questionnaire (SAQ)?	619
Are There Penalties for Noncompliance?	621
Summary	623

<b>Chapter 16: Privacy in an AI-Driven Landscape</b>	<b>634</b>
Defining Privacy in the Digital Context . . . . .	635
The Interplay Between AI and Privacy . . . . .	636
AI as a Privacy Protector and Challenger . . . . .	636
Privacy Concerns in AI Applications . . . . .	636
Privacy-Preserving Techniques in AI . . . . .	637
General Data Protection Regulation (GDPR) . . . . .	637
GDPR Key Principles . . . . .	637
Impact on Businesses . . . . .	638
Rights for Individuals . . . . .	639
California Consumer Privacy Act (CCPA) . . . . .	640
Key Provisions and Compliance Requirements of CCPA . . . . .	640
CCPA vs. GDPR . . . . .	641
Personal Information Protection and Electronic Documents Act (PIPEDA) . . . . .	641
Data Protection Act 2018 in the United Kingdom . . . . .	643
Comparing GDPR, CCPA, PIPEDA, and DPA 2018 . . . . .	644
Leveraging AI to Enhance Privacy Protections . . . . .	645
Summary . . . . .	647
<b>Chapter 17: Artificial Intelligence Governance and Regulations</b>	<b>652</b>
The AI Double-Edged Sword . . . . .	653
Generative AI, LLMs, and Traditional Machine Learning Implementations . . . . .	653
Introduction to AI Governance . . . . .	654
The U.S. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence . . . . .	655
The Blueprint for an AI Bill of Rights . . . . .	655
The Foundation of AI Governance: Guiding Principles from the Executive Order . . . . .	656
NIST's AI Risk Management Framework . . . . .	657
Implementing the AI RMF . . . . .	658

The Importance of High Accuracy and Precision in AI Systems . . . . .	661
Explainable AI (XAI): Building Trust and Understanding . . . . .	663
Tools for XAI . . . . .	664
Government and Society-wide Approaches to AI Governance . . . . .	665
The U.S. National AI Advisory Committee . . . . .	666
The European Artificial Intelligence Board . . . . .	666
A Society-wide Approach to AI Governance . . . . .	667
The EU AI Act . . . . .	667
Comparing U.S. Executive Order 14110 and the EU AI Act . . . . .	669
Guidelines for Secure AI System Development . . . . .	670
Key Guidelines from CISA and NCSC . . . . .	670
Provider and User Responsibility . . . . .	671
AI Supply Chain Security . . . . .	672
OWASP Top 10 Risks for LLM . . . . .	674
Prompt Injection Attacks . . . . .	674
Insecure Output Handling . . . . .	678
Training Data Poisoning . . . . .	678
Model Denial of Service . . . . .	678
Supply Chain Vulnerabilities . . . . .	679
Sensitive Information Disclosure . . . . .	680
Insecure Plugin Design . . . . .	680
Excessive Agency . . . . .	681
Overreliance . . . . .	681
Model Theft . . . . .	682
Model Inversion and Extraction . . . . .	682
Backdoor Attacks . . . . .	682
MITRE ATLAS Framework . . . . .	683
Summary . . . . .	684
<b>Appendix A: Answers to the Multiple Choice Questions</b>	<b>696</b>
<b>Index</b>	<b>716</b>



## About the Author

**Omar Santos** is a Distinguished Engineer at Cisco, focusing on artificial intelligence (AI) security, cybersecurity research, incident response, and vulnerability disclosure. He is a board member of the OASIS Open standards organization and the founder of OpenEoX. Omar's collaborative efforts extend to numerous organizations, including the Forum of Incident Response and Security Teams (FIRST) and the Industry Consortium for Advancement of Security on the Internet (ICASI). Omar is the co-chair of the FIRST PSIRT Special Interest Group (SIG). Omar is the co-founder of the DEF CON Red Team Village and the chair of the Common Security Advisory Framework (CSAF) technical committee.

Omar is the author of more than 25 books, 21 video courses, and more than 50 academic research papers. He is a renowned expert in ethical hacking, vulnerability research, incident response, and AI security. He employs his deep understanding of these disciplines to help organizations stay ahead of emerging threats. His dedication to cybersecurity has made a significant impact on technology standards, businesses, academic institutions, government agencies, and other entities striving to improve their cybersecurity programs. Prior to working for Cisco, Omar served in the U.S. Marines, focusing on the deployment, testing, and maintenance of Command, Control, Communications, Computer and Intelligence (C4I) systems. **You can find Omar at:**

X: @santosomar

LinkedIn: <https://www.linkedin.com/in/santosomar>

## Dedication

*I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.*

*I also dedicate this book to the memory of my father, Jose, and my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.*

## Acknowledgments

This book is a result of concerted efforts of various individuals. Without their help, this book would have not become a reality. I would like to thank the technical reviewer and my friend, John Stuppi, for his contributions and expert guidance.

I would also like to express my gratitude to Chris Cleveland, development editor, and James Manly, executive editor, for their help and continuous support during the development of this book.

## About the Technical Reviewer

**John Stuppi**, CCIE No. 11154, is an Engineering Program Manager in the Security & Trust Organization (S&TO) at Cisco where he works with Cisco customers to investigate suspected compromises in their network environment and to protect their networks against existing and emerging cybersecurity threats, risks, and vulnerabilities. Current projects include working with newly acquired entities to integrate them into Cisco's PSIRT Vulnerability Management processes and advising some of Cisco's most strategic customers on vulnerability management and risk assessment. John has presented multiple times on various network security topics at Cisco Live, Black Hat, as well as other customer-facing cybersecurity conferences. John is also the co-author of the *Official Certification Guide for CCNA Security 210-260* published by Cisco Press. Additionally, John has contributed to the Cisco Security Portal through the publication of white papers, Security Blog posts, and Cyber Risk Report articles. Prior to joining Cisco, John worked as a network engineer for JPMorgan and then as a network security engineer at Time, Inc., with both positions based in New York City. John is also a CISSP (#25525) and holds AWS Cloud Practitioner and Information Systems Security (INFOSEC) Professional Certifications. In addition, John has a BSEE from Lehigh University and an MBA from Rutgers University. John splits his time between Eatontown, New Jersey, and Clemson, South Carolina, with his wife, son, and daughter.

## We Want to Hear from You!

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

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

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

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

Email: [community@informit.com](mailto:community@informit.com)

## Reader Services

Register your copy of *Developing Cybersecurity Programs and Policies in an AI-Driven World* for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to [www.pearsonitcertification.com/register](http://www.pearsonitcertification.com/register) and log in or create an account\*. Enter the product ISBN 9780138074104 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

\*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

## Introduction

The number of cyber attacks continues to rise. Demand for safe and secure data and other concerns mean that companies need professionals to keep their information safe. Cybersecurity risk includes not only the risk of a data breach but the risk of an entire organization being undermined via business activities that rely on digitization and accessibility. As a result, learning how to develop an adequate cybersecurity program is crucial for any organization. Cybersecurity can no longer be something that you delegate to the information technology (IT) team. Everyone needs to be involved, including the board of directors.

This book focuses on industry-leading practices and standards, such as the International Organization for Standardization (ISO) standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Special Publications. This book is meticulously crafted for cybersecurity professionals, policymakers, and organizational leaders aiming to fortify their defenses in a world increasingly dominated by sophisticated threats, including emerging technologies such as artificial intelligence (AI).

This book begins with a foundational overview of cybersecurity policy and governance to set the stage for the need for balance between policy and practicality in cybersecurity programs. It then goes into detail on cybersecurity policy organization, format, and styles, providing insights into crafting effective and adaptable policies.

As the book progresses, it covers topics such as cloud security, governance and risk management, and asset management and data loss prevention, which are just some of the multifaceted challenges organizations face in securing their assets. Cloud security is paramount in today's environments because of the need to protect data, applications, and infrastructures operated over the cloud. As businesses and organizations increasingly use cloud services, the complexity and volume of cyber threats escalate. Cloud security is important to ensure compliance with rigorous regulatory requirements and industry standards. It plays a crucial role in enabling the safe adoption of cloud technologies, enabling innovation and agility.

The book also addresses the human element in a chapter on human resources security and education, recognizing that technology alone cannot safeguard against threats without informed and well-equipped personnel. The book also has chapters dedicated to cybersecurity operations, access control management, and supply chain security, highlighting the critical role of advanced technologies in detecting, mitigating, and responding to threats. A chapter on business continuity management emphasizes the importance of resilience and preparedness in the face of disruptions.

Given the complexity of today's regulatory landscape, this book provides great guidance on compliance across many sectors, including financial institutions, health care, technology, and retail. The last two chapters, which focus on privacy in an AI-driven landscape and AI governance and regulations, offer a forward-looking perspective on the ethical, legal, and societal implications of today's fast-paced world.

We used to say that we “stand on the brink of a new era.” Well, that new era has arrived. The integration of AI into cybersecurity practices is no longer a futuristic vision but today’s reality. The discussions in the last two chapters of this book are crucial for developing robust frameworks that protect against sophisticated threats and also ensure the responsible use of emerging technologies. I hope you find this book to be a roadmap for navigating the complexities of cybersecurity in the age of AI—and not just another cybersecurity book. I hope that it will equip you with the knowledge, strategies, and insights needed to create dynamic and resilient cybersecurity programs and policies.

## **Credits**

Figure 15.1 & 15.2 - Gegear/Shutterstock

Figure 11.3 - X Corp.

Figure 14.9 - United States department of Health and Human Services

Figure 17.5 - People and AI Research

# Chapter 2

## Cybersecurity Policy Organization, Format, and Styles

### *Chapter Objectives*

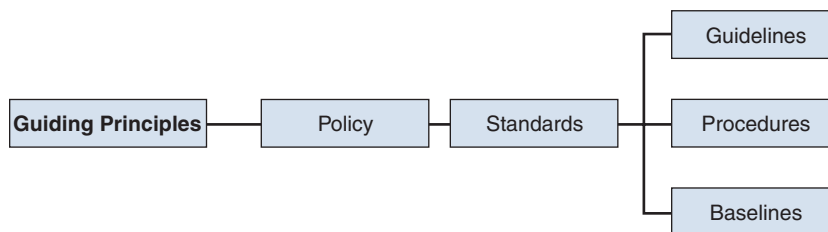
**After reading this chapter and completing the exercises, you will be able to do the following:**

- Explain the differences between a policy, a standard, a procedure, a guideline, and a plan.
- Know how to use plain language when creating and updating your cybersecurity policy.
- Identify the different policy elements.
- Include the proper information in each element of a policy.

In Chapter 1, “Understanding Cybersecurity Policy and Governance,” you learned that policies have played a significant role in helping us form and sustain our social, government, and corporate organizations. In this chapter, we begin by examining the hierarchy and purpose of guiding principles, policy, standards, procedures, and guidelines, as well as adjunct plans and programs. Returning to our focus on policies, we examine the standard components and composition of a policy document. You will learn that even a well-constructed policy is useless if it doesn’t deliver the intended message. The end result of complex, ambiguous, or bloated policy is, at best, noncompliance. At worst, negative consequences result as such policies may not be followed or understood. In this chapter, you will be introduced to “plain language,” which involves using the simplest, most straightforward way to express an idea. Plain-language documents are easy to read, understand, and act on. By the end of the chapter, you will have the skills to construct policy and companion documents. This chapter focuses on cybersecurity policies in the private sector and not policies created by governments of any country or state.

## Policy Hierarchy

As you learned in Chapter 1, a policy is a mandatory governance statement that presents management's position. A well-written policy clearly defines guiding principles, provides guidance to those who must make present and future decisions, and serves as an implementation roadmap. Policies are important, but alone they are limited in what they can accomplish. Policies need supporting documents to give them context and meaningful application. Standards, baselines, guidelines, and procedures each play a significant role in ensuring implementation of a governance objective. The relationship between the documents is known as the **policy hierarchy**. In a hierarchy, with the exception of the topmost object, each object is subordinate to the one above it. In a policy hierarchy, the topmost objective is the guiding principles, as illustrated in Figure 2-1.



**FIGURE 2-1** Policy Hierarchy

Cybersecurity policies should reflect the guiding principles and organizational objectives. This is why it is very important to communicate clear and well-understood organizational objectives within an organization. Standards are a set of rules and mandatory actions that provide support to a policy. Guidelines, procedures, and baselines provide support to standards. Let's take a closer look at each of these concepts.

## Standards

Standards serve as specifications for the implementation of policy and dictate mandatory requirements. For example, you might have a remote worker policy that states the following:

- This policy ensures that all employees understand their obligations to maintain a secure, productive, and efficient work environment while working from a remote location.
- This policy applies to all employees who are approved to work remotely, either on a full-time, part-time, or temporary basis.
- Employees must be reachable via phone, email, or video conferencing during core work hours.
- Company-issued equipment should be used for work purposes only and should be maintained in a secure manner.
- Employees must adhere to the organization's data security policy, including but not limited to, use of the VPN, use of approved cloud services, secure data transfer, and storage solutions.

The remote worker standard would then dictate the required characteristics, such as the following:

- MFA must be enabled for all accounts accessing corporate resources.
- All devices used for remote work must have up-to-date anti-malware software installed.
- Laptops and workstations used for remote work must have full-disk encryption enabled.
- No sensitive data should be stored locally unless approved and encrypted. Use corporate cloud storage solutions when possible.
- Only software approved by the IT department may be installed on work devices.
- Keep all operating systems and applications updated with the latest security patches.
- Remote devices and activity may be audited periodically for compliance with this standard.
- Failure to adhere to this standard may result in disciplinary actions, as described in the Remote Work Policy.

Another example of a standard is a common configuration of infrastructure devices such as routers and switches. An organization may have dozens, hundreds, or even thousands of routers and switches, and it might have a “standard” way of configuring authentication, authorization, and accounting (AAA) for administrative sessions. It might use TACACS+ or RADIUS as the authentication standard mechanism for all routers and switches within the organization.

As you can see, a policy represents expectations that are not necessarily subject to changes in technology, processes, or management. A standard, on the other hand, is very specific to the infrastructure.

Standards are determined by management, and unlike policies, they are not subject to authorization by the board of directors. Standards can be changed by management as long as they conform to the intent of the policy. A difficult task of writing a successful standard for a cybersecurity program is achieving consensus by all stakeholders and teams within an organization. In addition, a standard does not have to address everything that is defined in a policy. Standards should be compulsory and must be enforced to be effective.

## Baselines

A *baseline* serves as a standard guideline or set of specifications that is applicable to a particular category or group within an organization. These groups can be defined by different factors such as the platform (including specific operating systems and their versions), device type (like laptops, servers, desktops, routers, switches, firewalls, and mobile devices), ownership status (whether devices are employee-owned or corporate-owned), and location (such as onsite or remote workers).

The main purpose of establishing baselines is to ensure uniformity and consistency across the organization's technological environment. For instance, in the context of a policy for remote workers, a baseline might require that all Windows devices used by remote employees adhere to a specific Active Directory Group Policy configuration. This standard configuration is used to technically enforce security requirements, ensuring that all devices within this group meet a consistent level of security compliance. This approach helps in managing and securing IT resources effectively, particularly in diverse and distributed environments.

## Guidelines

*Guidelines* are best thought of as teaching tools. The objective of a guideline is to help people conform to a standard. In addition to using softer language than standards, guidelines are customized for the intended audience and are not mandatory. Guidelines are akin to suggestions or advice. A guideline related to the remote worker standard in the previous example might read like this:

- Use MFA all the time. MFA is a security measure that requires you to provide two or more forms of identification before you can access your account. This usually means entering your password (something you know) plus a second form of identification—like a code sent to your phone (something you have) or a face recognition scan (something you are).
- Store your device in a secure place when it is not in use to minimize the risk of theft or unauthorized access.
- Regularly back up important files to the corporate cloud storage solution, not to personal cloud or local storage.
- Use secure methods to delete sensitive information from your device rather than just moving files to the recycle bin.

Guidelines are recommendations and advice to users when certain standards do not apply to the environment. Guidelines are designed to streamline certain processes according to best practices and must be consistent with the cybersecurity policies. At the same time, guidelines often are open to interpretation and do not need to be followed to the letter.

## Procedures

*Procedures* are instructions for how a policy, a standard, a baseline, and guidelines are carried out in a given situation. Procedures focus on actions or steps, with specific starting and ending points. There are four commonly used procedure formats:

- **Simple step:** Lists sequential actions. There is no decision making.



- **Hierarchical:** Includes both generalized instructions for experienced users and detailed instructions for novices.
- **Graphic:** Uses either pictures or symbols to illustrate the step.
- **Flowchart:** Used when a decision-making process is associated with the task. Flowcharts are useful when multiple parties are involved in separate tasks.

### Note

As with guidelines, when designing procedures, it is important to know both your audience and the complexity of the task. In Chapter 9, “Cybersecurity Operations (CyberOps), Incident Response, Digital Forensics, and Threat Hunting,” we discuss in detail the use of incident response playbooks and other standard operating procedures (SOPs).

Procedures should be well documented and easy to follow to ensure consistency and adherence to policies, standards, and baselines. Like policies and standards, they should be well reviewed to ensure that they accomplish the objective of the policy and that they are accurate and remain relevant.

## Plans and Programs

The function of a plan is to provide strategic and tactical instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain time frame, usually with defined stages and with designated resources. Plans are sometimes referred to as programs. For our purposes, the terms are interchangeable. Here are some examples of information security–related plans we discuss in this book:

- Vendor management plan
- Incident response plan
- Business continuity plan
- Disaster recovery plan

Policies and plans are closely related. For example, an incident response policy generally includes the requirement to publish, maintain, and test an incident response plan. Conversely, the incident response plan gets its authority from the policy. Quite often, the policy will be included in the plan document.

### In Practice

#### Policy Hierarchy Review

Let's look at an example of how standards, guidelines, and procedures support a policy statement:

- The policy requires that all media should be encrypted.
- The standard specifies the type of encryption that must be used.
- The guideline illustrates how to identify removable media.
- The procedure provides instructions for encrypting the media.

## Writing Style and Technique

Style is critical. A reader's first impression of a document is based on its style and organization. If the reader is immediately intimidated, the contents become irrelevant. Keep in mind that the role of policy is to guide behavior. That can happen only if the policy is clear and easy to use. How the document flows and the words you use will make all the difference in how the policy is interpreted. Know your intended reader and write in a way that is understandable. Use terminology that is relevant. Most importantly, keep it simple. Policies that are overly complex tend to be misinterpreted. Policies should be written using plain language.

### Using Plain Language

The term *plain language* means using the simplest, most straightforward way to express an idea.

No single technique defines plain language. Rather, plain language is defined by results: It is easy to read, understand, and use. Studies have proven that documents created using plain-language techniques are effective in a number of ways:<sup>1</sup>

- Readers understand documents better.
- Readers prefer plain language.
- Readers locate information faster.
- Documents are easier to update.
- It is easier to train people.
- Plain language saves time and money.

Even confident readers appreciate plain language. It enables them to read more quickly and with increased comprehension. The use of plain language is spreading in many areas of American culture, including governments at all levels, especially the federal government, health care, the sciences, and the legal system.

**FYI: Warren Buffet on Using Plain Language**

The following excerpt from the preface to the Securities and Exchange Commission's *A Plain English Handbook* was written by Berkshire Hathaway co-founder, chair, and CEO Warren Buffett:

For more than forty years, I've studied the documents that public companies file. Too often, I've been unable to decipher just what is being said or, worse yet, had to conclude that nothing was being said.

Perhaps the most common problem, however, is that a well-intentioned and informed writer simply fails to get the message across to an intelligent, interested reader. In that case, stilted jargon and complex constructions are usually the villains.

One unoriginal but useful tip: Write with a specific person in mind. When writing Berkshire Hathaway's annual report, I pretend that I'm talking to my sisters. I have no trouble picturing them: Though highly intelligent, they are not experts in accounting or finance. They will understand plain English, but jargon may puzzle them. My goal is simply to give them the information I would wish them to supply me if our positions were reversed. To succeed, I don't need to be Shakespeare; I must, though, have a sincere desire to inform.

No siblings to write to? Borrow mine: Just begin with "Dear Doris and Bertie."

Source: Securities and Exchange Commission, "A Plain English Handbook: How to Create Clear SEC Disclosure Documents," <https://www.sec.gov/pdf/handbook.pdf>.

## The Plain Language Movement

It seems obvious that everyone would want to use plain language, but as it turns out, that is not the case. There is an enduring myth that to appear official or important, documents should be verbose. The result has been a plethora of complex and confusing regulations, contracts, and, yes, policies. In response to public frustration, the plain language movement began in earnest in the early 1970s.

In 1971, the National Council of Teachers of English in the United States formed the Public Double-speak Committee. In 1972, U.S. President Richard Nixon created plain language momentum when he decreed that the "Federal Register be written in 'layman's terms.'" The next major event in the U.S. history of plain language occurred in 1978, when U.S. President Jimmy Carter issued Executive Orders 12044 and 12174, with the goal of making government regulations cost-effective and easy to understand. In 1981, U.S. President Ronald Reagan rescinded Carter's executive orders. Nevertheless, many continued their efforts to simplify documents; by 1991, eight states had passed statutes related to plain language.

In 1998, President Clinton issued a Presidential Memorandum requiring government agencies to use plain language in communications with the public. All subsequent administrations have supported this memorandum. In 2010, plain-language advocates achieved a major victory when the Plain Writing Act was passed. This law requires federal government agencies to write publications and forms in a "clear, concise, well-organized" manner, following plain language guidelines.

We can take a cue from the government and apply these same techniques when writing policies, standards, guidelines, and plans. The easier a policy is to understand, the better the chance of compliance.

### FYI: Plain Language Results

This is an example of using plain language provided by the U.S. government.

#### **Before**

Infants and children who drink water containing lead in excess of the action level could experience delays in their physical or mental development. Children could show slight deficits in attention span and learning abilities. Adults who drink this water over many years could develop kidney problems or high blood pressure.

#### **After**

Lead in drinking water can make you sick. Here are some possible health effects of high lead levels in your drinking water:

Children:

- Delayed growth
- Learning disabilities
- Short attention span

Adults:

- Kidney problems
- High blood pressure

Source: Plain Language Action and Information Network (PLAIN), “Lead in Water” example, <https://www.plainlanguage.gov/examples/before-and-after/lead-warning>.

## **Plain Language Techniques for Policy Writing**

The Plain Language Action and Information Network (PLAIN) describes itself on its website (<https://plainlanguage.gov>) as a group of federal employees from many agencies and specialties who support the use of clear communication in government writing. In March 2011, PLAIN published the Federal Plain Language Guidelines. Some of the guidelines are specific to government publications. Many are applicable to both government and industry. The 10 guidelines listed here are pertinent to writing policies and companion documents:

1. Write for your audience. Use language your audience knows and is familiar with.
2. Write short sentences. Express only one idea in each sentence.

3. Limit a paragraph to one subject. Aim for no more than seven lines.
4. Be concise. Leave out unnecessary words. Instead of “for the purpose of,” use “to.” Instead of “due to the fact that,” use “because.”
5. Don’t use jargon or technical terms when you can use everyday words that have the same meaning.
6. Use active voice. A sentence written in active voice shows the subject acting in standard English sentence order: subject–verb–object. Active voice makes it clear who is supposed to do what. It eliminates ambiguity about responsibilities. Not “it must be done” but “you must do it.”
7. Use “must,” not “shall,” to indicate requirements. “Shall” is imprecise. It can indicate either an obligation or a prediction. The word “must” is the clearest way to convey to your audience that they have to do something.
8. Use words and terms consistently throughout your documents. If you use the term “senior citizens” to refer to a group, continue to use this term throughout your document. Don’t substitute another term, such as “the elderly” or “the aged.” Using a different term may cause the reader to wonder if you are referring to the same group.
9. Omit redundant pairs or modifiers. For example, instead of “cease and desist,” use either “cease” or “desist.” Even better, use a simpler word, such as “stop.” Instead of saying “the end result was the honest truth,” say “the result was the truth.”
10. Avoid double negatives and exceptions to exceptions. Many ordinary terms have a negative meaning, such as unless, fail to, notwithstanding, except, other than, unlawful (“un-” words), disallowed (“dis-” words), terminate, void, insufficient, and so on. Watch out for them when they appear after “not.” Find a positive word to express your meaning.

Want to learn more about using plain language? The official website of PLAIN has a wealth of resources, including the Federal Plain Language Guidelines, training materials and presentations, videos, posters, and references.

### **In Practice**

#### **Understanding Active and Passive Voice**

Here are some key points to keep in mind concerning active and passive voice:

- Voice refers to the relationship of a subject and its verb.
- Active voice refers to a verb that shows the subject acting.
- Passive voice refers to a verb that shows the subject being acted upon.

## Active Voice

A sentence written in active voice shows the subject acting in standard English sentence order: subject–verb–object. The subject names the agent responsible for the action, and the verb identifies the action the agent has set in motion. Example: “George threw the ball.”

## Passive Voice

A sentence written in passive voice reverses the standard sentence order. Example: “The ball was thrown by George.” George, the agent, is no longer the subject but now becomes the object of the preposition “by.” The ball is no longer the object but now becomes the subject of the sentence, where the agent preferably should be.

## Conversion Steps

To convert a passive sentence into an active one, take these steps:

1. Identify the agent.
2. Move the agent to the subject position.
3. Remove the helping verb (to be).
4. Remove the past participle.
5. Replace the helping verb and participle with an action verb.

## Examples of Conversion

**Original:** The report has been completed.

**Revised:** Stefan completed the report.

**Original:** A decision will be made.

**Revised:** Derek will decide.

## In Practice

### U.S. Army Clarity Index

The Clarity Index was developed to encourage plain writing. The index has two factors: average number of words per sentence and percentage of words longer than three syllables. The index adds together the two factors. The target is an average of 15 words per sentence and 15% of the total text being composed of three syllables or less. A resulting index between 20 and 40 is ideal and indicates the right balance of words and sentence length. In the following example (excerpted from Warren Buffet’s SEC introduction), the index is composed of an average of 18.5 words per sentence, and 11.5% of the words are three syllables or less. At an index of 30, this text falls squarely in the ideal range!

Sentence	Number of Words per Sentence	Number and Percentage of Words with Three or More Syllables
For more than forty years, I've studied the documents that public companies file.	13	Two words: $2/13 = 15\%$
Too often, I've been unable to decipher just what is being said or, worse yet, had to conclude that nothing was being said.	23	One word: $1/23 = 4\%$
Perhaps the most common problem, however, is that a well-intentioned and informed writer simply fails to get the message across to an intelligent, interested reader.	26	Three words: $3/26 = 11\%$
In that case, stilted jargon and complex constructions are usually the villains.	12	Two words: $2/12 = 16\%$
Total	74	46%
Average	18.5	11.5%
<b>Clarity Index</b>	<b><math>18.5 + 11.5 = 30</math></b>	

## Policy Format

Writing policy documents can be challenging. Policies are complex documents that must be written to withstand legal and regulatory scrutiny and at the same time must be easy for a reader to read and understand. The starting point for choosing a format is identifying the policy audience.

### Understand Your Audience

Who a policy is intended for is referred to as the *policy audience*. It is imperative during the planning portion of the security policy project to clearly define the audience. Policies may be intended for a particular group of employees based on job function or role. For example, an application development policy is targeted to developers. Other policies may be intended for a particular group or individual based on organizational role, such as a policy defining the responsibility of the chief information security officer (CISO). The policy, or portions of it, can sometimes apply to people outside the company, such as business partners, service providers, contractors, or consultants. The policy audience is a potential resource during the entire policy life cycle. Indeed, who better to help create and maintain an effective policy than the very people whose job it is to use those policies in the context of their everyday work?

## Policy Format Types

Organize before you begin writing! It is important to decide how many sections and subsections you will require before you begin writing. Designing a template that allows the flexibility of editing will save considerable time and reduce aggravation. In this section, you will learn about the different sections and subsections of a policy, as well as the policy document formation options.

There are two general ways to structure and format a policy:

- **Singular policy:** Write each policy as a discrete document.
- **Consolidated policy:** Group together similar and related policies.

Consolidated policies are often organized by section and subsection.

Table 2-1 illustrates policy document format options.

**TABLE 2-1** Policy Document Format Options

Format	Example
Singular policy	Chief information security officer (CISO) policy: Specific to the role and responsibility of the information security officer.
Consolidated policy	Governance policy: Addresses the role and responsibilities of the board of directors, executive management, chief risk officer, CISO, compliance officer, legal counsel, auditor, IT director, and users.

The advantage of creating individual policies is that each policy document can be short, clean, crisp, and targeted to its intended audience. The disadvantage is the need to manage multiple policy documents and the chance that they will become fragmented and lose consistency. The advantage of a consolidated policy is that it presents a composite management statement in a single voice. The disadvantages are the potential size of the document and the difficulty the reader may have locating applicable sections.

In the first edition of this book, we limited our study to singular policy documents. Since then, both the use of technology and the regulatory landscape have increased exponentially—only outpaced by escalating threats. In response to this ever-changing environment, the need for policies and the number of policies has grown. For many organizations, managing singular policies has become unwieldy. The current trend is toward consolidation. Throughout this edition, we have consolidated policies by security domain.

Regardless of which format you choose, you should not include standards, baselines, guidelines, or procedures in your policy document. If you do, you will end up with one big unruly document. And you will undoubtedly encounter one or more of the following problems:

- **Management challenge:** Who is responsible for managing and maintaining a document that has multiple contributors?



- **Difficulty of updating:** Because standards, guidelines, and procedures change far more often than policies, updating this whale of a document will be far more difficult than if these elements were properly treated separately. Version control will become a nightmare.
- **Cumbersome approval process:** Various regulations as well as the corporate operating agreement require that the board of directors approve new policies as well as changes. Mashing it all together means that every change to a procedure, guideline, or standard will potentially require the board to review and approve it. This will become very costly and cumbersome for everyone involved.

## Policy Components

Policy documents have multiple sections or components (see Table 2-2). How the components are used and in what order depends on which format—singular or consolidated—you choose. In this section, we examine the composition of each component. Consolidated policy examples are provided in the “In Practice” sidebars.

**TABLE 2-2** Policy Document Components

Component	Purpose
Version control	To track changes
Introduction	To frame the document
Policy heading	To identify the topic
Policy goals and objectives	To convey intent
Policy statement	Mandatory directive
Policy exceptions	To acknowledge exclusions
Policy enforcement clause	Violation sanctions
Administrative notations	Additional information
Policy definitions	Glossary of terms

## Version Control

Best practices dictate that policies are reviewed annually to ensure that they are still applicable and accurate. Of course, policies can (and should) be updated whenever there is a relevant change driver. Version control, as it relates to policies, is the management of changes to the document. The version is usually identified by a number or letter code. Major revisions generally advance to the next letter or digit (for example, from 2.0 to 3.0). Minor revisions generally advance as a subsection (for example, from 2.0 to 2.1). Version control documentation should include the change date, the name of the person or persons making the change; a brief synopsis of the change; the name of the person, committee, or board that authorized the change; and the effective date of the change.

- For a singular policy document, this information is split between the policy heading and the administrative notation sections.
- For a consolidated policy document, a version control table is included either at the beginning of the document or at the beginning of a section.

In Practice

Version Control Table

A consolidated policy document includes a version control table. The table is located after the title page, before the table of contents. Version control provides the reader with a history of the document. Here’s an example:

V.	Editor	Purpose	Change Description	Authorized By	Effective Date
1.0	S. Ford, EVP		Original	Sr. management committee	2024-07-17
1.1	S. Ford, EVP	Subsection addition	2.5: Disclosures to Third Parties.	Sr. management committee	2024-08-14
1.2	S. Ford, EVP	Subsection update	4.4: Border Device Management 5.8: Wireless Networks	Sr. management committee	2025-02-25
—	S. Ford, EVP	Annual review	No change	Sr. management committee	2025-07-18
2.0	B. Lin, CIO	Section revision	Revised “Section 1.0: Governance and Risk Management” to reflect internal reorganization of roles and responsibilities	Acme, Board of Directors	2025-09-19

Introduction

Think of the introduction as the opening act. This is where authors first meet the readers and have the opportunity to engage them. Here are the objectives of the introduction:

- To provide context and meaning
- To convey the importance of understanding and adhering to the policy
- To acquaint the reader with the document and its contents
- To explain the exemption process as well as the consequence of noncompliance
- To reinforce the authority of the policy

The first part of the introduction should make the case for why the policy is necessary. It is a reflection of the guiding principles, defining for the reader the core values the company believes in and is committed to. This is also the place to set forth the regulatory and contractual obligations that the company has—often by listing which regulations, such as GLBA, HIPAA, or MA CMR 17 201, pertain to the organization as well as the scope of the policy.

The second part of the introduction should leave no doubt that compliance is mandatory. A strong statement of expectation from a senior authority, such as the chair of the board, CEO, or president, is appropriate. Users should understand that they are unequivocally and directly responsible for following the policy in the course of their normal employment or relationship with the company. This part of the introduction should also make clear that questions are welcome, and a resource is available who can clarify the policy and/or assist with compliance.

The third part of the introduction should describe the policy document, including the structure, categories, and storage location (for example, the company intranet). It should also reference companion documents such as standards, guidelines, programs, and plans. In some cases, the introduction includes a revision history, the stakeholders who may have reviewed the policy, and who to contact to make any modifications.

The fourth part of the introduction should explain how to handle situations where compliance may not be feasible. It should provide a high-level view of the exemption and enforcement process. The section should also address the consequences of willful noncompliance.

- For a singular policy document, the introduction should be a separate document.
- For a consolidated policy document, the introduction serves as the preface and follows the version control table.

## **In Practice**

### **Introduction**

The introduction has five objectives: to provide context and meaning, to convey the importance of understanding and adhering to the policy, to acquaint the reader with the document, to explain the exemption process and the consequence of noncompliance, and, finally, to thank the reader and reinforce the authority of the policy. Each objective is called out in the following example:

[Objective 1: Provide context and meaning]

The 21st century environment of connected technologies offers us many exciting present and future opportunities. Unfortunately, there are those who seek to exploit these opportunities for personal, financial, or political gain. We, as an organization, are committed to protecting our clients, employees, stakeholders, business partners, and community from harm and to providing exceptional service.

The objective of our Cybersecurity Policy is to protect and respect the confidentiality, integrity, and availability of client information, company proprietary data, and employee data, as well as the infrastructure that supports our services and business activities.

This policy has been designed to meet or exceed applicable federal and state information security-related regulations, including but not limited to sections 501 and 505(b) of the Gramm-Leach-Bliley Act (GLBA) and MA CMR 17 201 as well as our contractual obligations.

The scope of the Cybersecurity Policy extends to all functional areas and all employees, directors, consultants, contractors, temporary staff, co-op students, interns, partners and third-party employees, and joint venture partners, unless explicitly excluded.

[Objective 2: Convey the importance of understanding and adhering to the policy]

Diligent information security practices are a civic responsibility and a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee and affiliate to know, understand, and adhere to these policies and to conduct their activities accordingly. If you have any questions or would like more information, I encourage you to contact our Compliance Officer at x334.

[Objective 3: Acquaint the reader with the document and its contents]

At first glance, the policy [or policies, if you are using singular policy documents] may appear daunting. If you take a look at the table of contents [or list, if you are using singular policy documents], you will see that the Cybersecurity Policy is organized by category. These categories form the framework of our Cybersecurity Program. Supporting the policies are implementation standards, guidelines, and procedures. You can find these documents in the Governance section of our online company library.

[Objective 4: Explain the consequence of noncompliance as well as the exception process]

Where compliance is not technically feasible or justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the chief operating officer (COO), including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the president have the authority to grant waivers.

Willful violation of this policy [or policies, if you are using singular policy documents] may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors and consultants, and dismissal for interns and volunteers. Additionally, individuals may be subject to civil and criminal prosecution.

[Objective 5: Thank the reader and provide a seal of authority]

I thank you in advance for your support, as we all do our best to create a secure environment and to fulfill our mission.

—Anthony Starks, Chief Executive Officer (CEO)

## Policy Heading

A **policy heading** identifies the policy by name and provides the reader with an overview of the policy topic or category. The format and contents of the heading significantly depend on the format (singular or consolidated) you are using:

- A singular policy must be able to stand on its own, which means it is necessary to include significant logistical detail in each heading. The information contained in a singular policy

heading may include the organization or division name, category (section), subsection, policy number, name of the author, version number, approval authority, effective date of the policy, regulatory cross-reference, and a list of supporting resources and source material. The topic is generally self-explanatory and does not require an overview or explanation.

- In a consolidated policy document, the heading serves as a section introduction and includes an overview. Because the version number, approval authority, and effective date of the policy have been documented in the version control table, it is unnecessary to include them in section headings. Regulatory cross-reference (if applicable), lead author, and supporting documentation are found in the Administrative Notation section of the policy.

### **In Practice**

#### **Policy Heading**

A consolidated policy heading serves as the introduction to a section or category.

Section 1: Governance and Risk Management

#### **Overview**

Governance is the set of responsibilities and practices exercised by the board of directors and management team with the goal of providing strategic direction, ensuring that organizational objectives are achieved, risks are managed appropriately, and enterprise resources are used responsibly. The principal objective of an organization's risk management process is to provide those in leadership and data steward roles with the information required to make well-informed decisions.

### **Policy Goals and Objectives**

*Policy goals and objectives* act as a gateway to the content to come and the security principle they address. This component should concisely convey the intent of the policy. Note that even a singular policy can have multiple objectives. We live in a world where business matters are complex and interconnected, which means that a policy with a single objective might be at risk of not covering all aspects of a particular situation. It is therefore important, during the planning phase, to pay appropriate attention to the different objectives the security policy should seek to achieve.

- A singular policy lists the goals and objectives either in the policy heading or in the body of the document.
- In a consolidated policy document, the goals and objectives are grouped and follow the policy heading.

## In Practice

### Policy Goals and Objectives

Goals and objectives should convey the intent of the policy. Here's an example:

Goals and Objectives for Section 1: Governance and Risk Management

- To demonstrate our commitment to information security
- To define organizational roles and responsibilities
- To provide the framework for effective risk management and continuous assessment
- To meet regulatory requirements

## Policy Statement

Up to this point in the document, we have discussed everything but the actual policy statement. The **policy statement** is a high-level directive or strategic roadmap. This is the section where we lay out the rules that need to be followed and, in some cases, reference the implementation instructions (standards) or corresponding plans. Policy statements are intended to provide action items as well as the framework for situational responses. Policies are mandatory. Deviations or exceptions must be subject to a rigorous examination process.

## In Practice

### Policy Statement

The bulk of the final policy document is composed of policy statements. Here is an example of an excerpt from a governance and risk management policy:

#### 1.1. Roles and Responsibilities

- 1.1.1. The board of directors will provide direction for and authorize the Cybersecurity Policy and corresponding program.
- 1.1.2. The chief operating officer (COO) is responsible for the oversight of, communication related to, and enforcement of the Cybersecurity Policy and corresponding program.
- 1.1.3. The COO will provide an annual report to the board of directors that provides them with the information necessary to measure the organization's adherence to the Cybersecurity Policy objectives and to gauge the changing nature of risk inherent in lines of business and operations.

1.1.4. The chief information security officer (CISO) is charged with the implementation of the Cybersecurity Policy and standards including but not limited to:

- Ensuring that administrative, physical, and technical controls are selected, implemented, and maintained to identify, measure, monitor, and control risks, in accordance with applicable regulatory guidelines and industry best practices
- Managing risk assessment–related remediation
- Authorizing access control permissions to client and proprietary information
- Reviewing access control permissions in accordance with the audit standard
- Responding to security incidents

1.1.5. In-house legal counsel is responsible for communicating to all contracted entities the information security requirements that pertain to them as detailed within the Cybersecurity Policy and the Vendor Management Program.

## Policy Exceptions and the Exemption Process

Realistically, there will be situations in which it is not possible or practical—or perhaps may even be harmful—to obey a policy directive. This does not invalidate the purpose or quality of the policy. It just means that some special situations will call for *exceptions* to the rule. *Policy exceptions* are agreed waivers that are documented within the policy. For example, in order to protect its intellectual property, Company A has a policy that bans digital cameras from all company premises. However, a case could be made that the HR department should be equipped with a digital camera to take pictures of new employees to paste them on their ID badges. Or maybe the security officer should have a digital camera to document the proceedings of evidence gathering after a security breach has been detected. Both examples are valid reasons a digital camera might be needed. In these cases, an exception to the policy could be added to the document. If no exceptions are ever to be allowed, this should be clearly stated in the policy statement section as well.

An *exemption* or *waiver process* is required for exceptions identified after the policy has been authorized. The exemption process should be explained in the introduction. Only the method or process for requesting an exemption—and not the criteria or conditions for exemptions—should be detailed in the policy. Trying to list all the conditions to which exemptions apply can lead to creating a loophole in the exemption itself. It is also important that the process follow specific criteria under which exemptions are granted or rejected. Whether an exemption is granted or rejected, the requesting party should be given a written report with clear reasons either way.

Finally, it is recommended that you keep the number of approved exceptions and exemptions low, for several reasons:

- Too many built-in exceptions may lead employees to perceive the policy as unimportant.
- Granting too many exemptions may create the impression of favoritism.
- It can become difficult to keep track of and successfully audit a large number of exceptions and exemptions.

If there are too many built-in exceptions and/or exemption requests, it may indicate that the policy is not appropriate in the first place. At that point, the policy should be subject to review.

### In Practice

#### Policy Exception

Here's a policy exception that informs the reader who is not required to conform to a specific clause and under what circumstances and whose authorization:

At the discretion of in-house legal counsel, contracted entities whose contracts include a confidentiality clause may be exempted from signing nondisclosure agreements.

The process for granting post-adoption exemptions should be included in the introduction. Here's an example:

Where compliance is not technically feasible or as justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the COO, including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the president have the authority to grant waivers.

#### Policy Enforcement Clause

The best way to deliver the message that policies are mandatory is to include the penalty for violating the rules. The ***policy enforcement clause*** is where the sanctions for non-adherence to the policy are unequivocally stated to reinforce the seriousness of compliance. Obviously, you must be careful with the nature of the penalty. It should be proportional to the rule that was broken, whether it was accidental or intentional, and the level of risk the company incurred.

An effective method of motivating compliance is proactive training. All employees should be trained in the acceptable practices presented in the security policy. Without training, it is hard to fault employees for not knowing they were supposed to act in a certain fashion. Imposing disciplinary actions in such situations can adversely affect morale. We take a look at various training, education, and awareness tools and techniques in later chapters.

### In Practice

#### Policy Enforcement Clause

This example of a policy enforcement clause advises the reader, in no uncertain terms, what will happen if they do not obey the rules. It belongs in the introduction and, depending on the circumstances, may be repeated within the policy document:

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors and consultants, and dismissal for interns and volunteers. Additionally, individuals are subject to civil and criminal prosecution.



## **Administrative Notations**

The purpose of *administrative notations* is to refer the reader to additional information and/or provide a reference to an internal resource. Notations include regulatory cross-references; the names of corresponding documents, such as standards, guidelines, and programs; supporting documentation such as annual reports or job descriptions; and the policy author's name and contact information. You should include only notations that are applicable to your organization. However, you should be consistent across all policies.

- A singular policy incorporates administrative notations either in the heading, at the end of the document, or split between the two locations. How this is handled depends on the company's policy template.
- In a consolidated policy document, the administrative notations are located at the end of each section.

### **In Practice**

#### **Administrative Notations**

Administrative notations are a reference point for additional information. If the policy is distributed in electronic format, it is a great idea to hyperlink the notations directly to the source document.

#### **Regulatory Cross-Reference**

Section 505(b) of the Gramm-Leach-Bliley Act

MA CMR 17 201

#### **Lead Author**

B. Lin, Chief Information Officer

b.lin@example.com

#### **Corresponding Documents**

Risk Management Standards

#### **Vendor Management Program**

Supporting Documentation

Job descriptions as maintained by the Human Resources Department

## Policy Definitions

The *policy definition section* is a glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with. Adding definitions to the overall document will aid the target audience in understanding the policy and will therefore make the policy a much more effective document.

The general rule is to include definitions for any instance of industry-specific, technical, legal, or regulatory language. When deciding what terms to include, it makes sense to err on the side of caution. The purpose of the security policy document is communication and education. The target audience for this document usually encompasses all employees of the company and sometimes outside personnel. Even if some technical topics are well known to all in-house employees, some of those outside individuals who come in contact with the company—and therefore are governed by the security policy—may not be as well versed in the policy’s technical aspects.

Simply put, before you begin writing down definitions, it is recommended that you first define the target audience for whom the document is crafted and cater to the lowest common denominator to ensure optimum communication efficiency.

Another reason definitions should not be ignored is for the legal ramifications they represent. An employee cannot pretend to have thought that a certain term used in the policy meant one thing when it is clearly defined in the policy itself. When you’re choosing which words will be defined, therefore, it is important to look not only at those that could clearly be unknown but also at those that should be defined to remove any and all ambiguity. A security policy could be an instrumental part of legal proceedings and should therefore be viewed as a legal document and crafted as such.

### In Practice

#### Terms and Definitions

Any term that may not be familiar to the reader or is open to interpretation should be defined.

Here’s an example of an abbreviation:

*MOU*—Memorandum of Understanding

Here’s an example of a regulatory reference:

*MA CMR 17 201—Standards for the Protection of Personal Information of Residents of the Commonwealth* establishes minimum standards to be met in connection with the safeguarding of personal information of Massachusetts residents.

And, finally, here are a few examples of security terms that might be included:

- **Distributed Denial of Service (DDoS):** An attack in which there is a massive volume of IP packets from multiple sources. The flood of incoming packets consumes available resources, resulting in denial of service to legitimate users.
- **Exploit:** A malicious program designed to exploit, or take advantage of, a single vulnerability or set of vulnerabilities.

- **Phishing:** An attack in which the attacker presents to a user a link that looks like a valid, trusted resource. A user who clicks it is prompted to disclose confidential information such as their username and password.
- **Pharming:** A technique an attacker uses to direct a customer's URL from a valid resource to a malicious one that could be made to appear as the valid site to the user. From there, an attempt is made to extract confidential information from the user.
- **Malvertising:** The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.
- **Logic bomb:** A type of malicious code that is injected into a legitimate application. An attacker can program a logic bomb to delete itself from the disk after it performs the malicious tasks on the system. Examples of these malicious tasks include deleting or corrupting files or databases and executing a specific instruction after certain system conditions are met.
- **Trojan horse:** A type of malware that executes instructions to delete files, steal data, or compromise the integrity of the underlying operating system. Trojan horses typically use a form of social engineering to fool victims into installing such software on their computers or mobile devices. Trojans can also act as backdoors.
- **Backdoor:** A piece of malware or a configuration change that allows an attacker to control the victim's system remotely. For example, a backdoor can open a network port on the affected system so that the attacker can connect and control the system.

## Summary

You now know that policies need supporting documents to give them context and meaningful application. Standards, guidelines, and procedures provide a means to communicate specific ways to implement our policies. We create our organizational standards, which specify the requirements for each policy. We offer guidelines to help people comply with standards. We create sets of instructions known as procedures to ensure that tasks are consistently performed. The format of a procedure—simple step, hierarchical, graphic, or flowchart—depends on the complexity of the task and the audience. In addition to creating policies, we create plans or programs to provide strategic and tactical instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain time frame, usually with defined stages and with designated resources.

Writing policy documents is a multistep process. First, we need to define the audience for which the document is intended. Then, we choose the format. Options are to write each policy as a discrete document (singular policy) or to group like policies together (consolidated policy). Finally, we need to decide upon the structure, including the components to include and in what order.

The first and arguably most important section is the introduction. This is our opportunity to connect with the reader and to convey the meaning and importance of our policies. The introduction should be written by the “person in charge,” such as the CEO or president. This person should use the introduction to reinforce company-guiding principles and correlate them with the rules introduced in the security policy.

Specific to each policy are the heading, goals and objectives, policy statement, and (if applicable) exceptions. The heading identifies the policy by name and provides the reader with an overview of the policy topic or category. The goals and objectives convey what the policy is intended to accomplish. The policy statement lays out the rules that need to be followed and may reference the implementation instructions (standards) or corresponding programs. Policy exceptions are agreed waivers that are documented within the policy.

An exemption or waiver process is required for exceptions identified after a policy has been authorized. The policy enforcement clause is where the sanctions for willful non-adherence to the policy are unequivocally stated to reinforce the seriousness of compliance. Administrative notations refer the reader to additional information and/or provide references to internal resources. The policy definition section is a glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with.

Recognizing that the first impression of a document is based on its style and organization, we studied the work of the plain language movement. Using plain language helps produce documents that are easy to read, understand, and use. We looked at 10 techniques from the Federal Plain Language Guideline that we can (and should) use for writing effective policies. In the next section of the book, we put these newfound skills to use.

## Test Your Skills

### MULTIPLE CHOICE QUESTIONS

1. The policy hierarchy is the relationships between which of the following?
  - A. Guiding principles, regulations, laws, and procedures
  - B. Guiding principles, standards, guidelines, and procedures
  - C. Guiding principles, instructions, guidelines, and programs
  - D. None of the above
2. Which of the following statements best describes the purpose of a standard?
  - A. To state the beliefs of an organization
  - B. To reflect the guiding principles
  - C. To dictate mandatory requirements
  - D. To make suggestions
3. Which of the following statements best describes the purpose of a guideline?
  - A. To state the beliefs of an organization
  - B. To reflect the guiding principles
  - C. To dictate mandatory requirements
  - D. To help people conform to a standard
4. Which of the following statements best describes the purpose of a baseline?
  - A. To measure compliance
  - B. To ensure uniformity across a similar set of devices
  - C. To ensure uniformity and consistency
  - D. To make suggestions
5. Simple step, hierarchical, graphic, and flowchart are examples of which of the following formats?
  - A. Policy
  - B. Program
  - C. Procedure
  - D. Standard

6. Which of the following terms best describes instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain time frame, usually with defined stages and with designated resources?
  - A. Plan
  - B. Policy
  - C. Procedure
  - D. Package
7. Which of the following statements best describes a disadvantage to using the singular policy format?
  - A. The policy can be short.
  - B. The policy can be targeted.
  - C. You may end up with too many policies to maintain.
  - D. The policy can easily be updated.
8. Which of the following statements best describes a disadvantage to using the consolidated policy format?
  - A. Consistent language is used throughout the document.
  - B. Only one policy document must be maintained.
  - C. The format must include a composite management statement.
  - D. The document may end up being very long.
9. Policies, standards, guidelines, and procedures should all be in the same document.
  - A. True
  - B. False
  - C. Only if the company is multinational
  - D. Only if the documents have the same author
10. Version control is the management of changes to a document and should include which of the following elements?
  - A. Version or revision number
  - B. Date of authorization or date that the policy took effect
  - C. Change description
  - D. All of the above

11. What is an exploit?
- A. A phishing campaign
  - B. A malicious program or code designed to exploit, or take advantage of, a single vulnerability or set of vulnerabilities
  - C. A network or system weakness
  - D. A protocol weakness
12. The name of the policy, policy number, and overview belong in which of the following sections?
- A. Introduction
  - B. Policy heading
  - C. Policy goals and objectives
  - D. Policy statement
13. The aim or intent of a policy is stated in the \_\_\_\_\_.
- A. introduction
  - B. policy heading
  - C. policy goals and objectives
  - D. policy statement
14. Which of the following statements is true?
- A. A security policy should include only one objective.
  - B. A security policy should not include any exceptions.
  - C. A security policy should not include a glossary.
  - D. A security policy should not list all step-by-step measures that need to be taken.
15. The \_\_\_\_\_ contains the rules that must be followed.
- A. policy heading
  - B. policy statement
  - C. policy enforcement clause
  - D. policy goals and objectives list
16. A policy should be considered \_\_\_\_\_.
- A. mandatory
  - B. discretionary
  - C. situational
  - D. optional

17. Which of the following best describes policy definitions?
- A. A glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with
  - B. A detailed list of the possible penalties associated with breaking rules set forth in the policy
  - C. A list of all the members of the security policy creation team
  - D. None of the above
18. The \_\_\_\_\_ contains the penalties that would apply if a portion of the security policy were to be ignored by an employee.
- A. policy heading
  - B. policy statement
  - C. policy enforcement clause
  - D. policy statement of authority
19. What component of a security policy does the following phrase belong to? “Wireless networks are allowed only if they are separate and distinct from the corporate network.”
- A. Introduction
  - B. Administrative notation
  - C. Policy heading
  - D. Policy statement
20. There may be situations in which it is not possible to comply with a policy directive. Where should the exemption or waiver process be explained?
- A. Introduction
  - B. The policy statement
  - C. Policy enforcement clause
  - D. Policy exceptions
21. The name of the person/group (for example, executive committee) that authorized the policy should be included in the \_\_\_\_\_.
- A. version control table or policy statement
  - B. heading or policy statement
  - C. policy statement or policy exceptions
  - D. version control table or policy heading



22. When you're drafting a list of exceptions for a security policy, the language should \_\_\_\_\_.
- A. be as specific as possible
  - B. be as vague as possible
  - C. reference another, dedicated document
  - D. None of the above
23. If supporting documentation would be of use to the reader, it should be \_\_\_\_\_.
- A. included in full in the policy document
  - B. ignored because supporting documentation does not belong in a policy document
  - C. listed in either the policy heading or administrative notation section
  - D. included in a policy appendix
24. When writing a policy, standard, guideline, or procedure, you should use language that is \_\_\_\_\_.
- A. technical
  - B. clear and concise
  - C. legalese
  - D. complex
25. Readers prefer plain language because it \_\_\_\_\_.
- A. helps them locate pertinent information
  - B. helps them understand the information
  - C. saves time
  - D. All of the above
26. Which of the following is not a characteristic of plain language?
- A. Short sentences
  - B. Using active voice
  - C. Technical jargon
  - D. Seven or fewer lines per paragraph
27. Which of the following is the best term to use when indicating a mandatory requirement?
- A. must
  - B. shall
  - C. should not
  - D. may not

28. A company that uses the term “employees” to refer to workers who are on the company payroll should refer to them throughout their policies as \_\_\_\_\_.
- A. workforce members
  - B. employees
  - C. hired hands
  - D. workers
29. Which of the following statements is true regarding policy definitions?
- A. They should be included and maintained in a separate document.
  - B. The general rule is to include definitions for any topics except technical, legal, or regulatory language.
  - C. The general rule of policy definitions is to include definitions for any instance of industry-specific, technical, legal, or regulatory language.
  - D. They should be created before any policy or standards.
30. Even the best-written policy will fail if which of the following is true?
- A. The policy is too long.
  - B. The policy is mandated by the government.
  - C. The policy doesn’t have the support of management.
  - D. All of the above.

## EXERCISES

### EXERCISE 2.1: Creating Standards, Guidelines, and Procedures

The University System has a policy that states, “All students must comply with their campus attendance standard.”

1. You are tasked with developing a standard that documents the mandatory requirements (for example, how many classes can be missed without penalty). Include at least four requirements.
2. Create a guideline to help students adhere to the standard you created.
3. Create a procedure for requesting exemptions to the policy.

### EXERCISE 2.2: Writing Policy Statements

1. Who would be the target audience for a policy related to campus elections?
2. Keeping in mind the target audience, compose a policy statement related to campus elections.
3. Compose an enforcement clause.

**EXERCISE 2.3: Writing a Policy Introduction**

1. Write an introduction to the policy you created in Exercise 2.2.
2. Generally an introduction is signed by an authority. Who would be the appropriate party to sign the introduction?
3. Write an exception clause.

**EXERCISE 2.4: Writing Policy Definitions**

1. The purpose of policy definitions is to clarify ambiguous terms. If you were writing a policy for an on-campus student audience, what criteria would you use to determine which terms should have definitions?
2. What are some examples of terms you would define?

**EXERCISE 2.5: Understanding Baselines**

The goal of this exercise is to understand what baselines are, why they are important, and the different types of baselines.

1. Read articles or watch tutorials on the importance of baselines in IT security.
2. Reflect on how baselines can contribute to uniformity and security in various IT environments.
3. Explore different tools and methodologies for baseline management across platforms such as Windows, Linux, and network devices.
4. Create a detailed security baseline for a chosen IT environment. Choose an IT environment that you are familiar with or interested in, such as Windows desktops, Linux servers, or network routers.
5. Document the standard configurations for the system.
6. Define appropriate security policies including password policies and security protocols. List approved software and version numbers. Outline procedures for regular updates and patches.
7. Compare your baseline with existing standards or best practices found in your research to evaluate its completeness and robustness.

## PROJECTS

### PROJECT 2.1: Comparing Security Policy Templates

1. Search online for “cybersecurity policy templates.”
2. Read the documents and compare them.
3. Identify the policy components that were covered in this chapter.
4. Search for a real-world policy, such as Tufts University’s Two-factor Authentication Policy, at <https://it.tufts.edu/univ-pol>.
5. Choose a couple terms in the policy that are not defined in the policy definitions section and write a definition for each.

### PROJECT 2.2: Researching New York City’s AI Bias Law

The objective of this project is to research the requirements, implications, and real-world application of New York City’s AI Bias Law in hiring practices and why it was failing after being enacted.

#### PART 1: Background Research

Goal: Gain a foundational understanding of the AI Bias Law and its objectives.

1. Research and read articles, official documents, and other credible sources detailing New York City’s AI Bias Law. Focus on understanding the definitions of Automated Employment Decision Tools (AEDTs) and the scope of the law.
2. Summarize the key elements of the law:
  - What are AEDTs?
  - What requirements does the law impose on employers using these tools?
  - What are the intended outcomes of the law?

#### PART 2: Exploring Implications and Challenges

Goal: Analyze the potential impacts of the law on employers and job seekers, and identify challenges in its implementation.

1. Consider the implications for employers in terms of compliance costs and changes to hiring practices. Reflect on how the law affects job seekers, especially those from marginalized groups.
2. Investigate any reported difficulties or controversies associated with implementing the law. Consider technical, legal, and ethical challenges.
3. Identify any criticisms or support from various stakeholders including businesses, advocacy groups, and legal experts.

4. Examine how companies have responded to the law and the real-world effectiveness of such regulations.
5. Choose one or more companies that have implemented measures to comply with the AI Bias Law. If specific company examples are scarce, consider hypothetical scenarios based on industry standards.
6. Analyze the steps these companies have taken to audit their AEDTs.
7. Evaluate the transparency of the published audit results and any actions taken based on those results.
8. Write a detailed report on your findings, highlighting effective practices and areas where companies may fall short in compliance.

### PROJECT 2.3: Testing the Clarity of a Policy Document

1. Locate your school's cybersecurity policy. (It may have a different name.)
2. Select a section of the policy and use the U.S. Army's Clarity Index to evaluate the ease of reading. (See the "In Practice: U.S. Army Clarity Index" sidebar for instructions.)
3. Explain how you would make the policy more readable.

#### Case Study

##### Clean Up the Library Lobby

The library includes the following exhibition policy:

Requests to utilize the entrance area at the library for the purpose of displaying posters and leaflets give rise to the question of the origin, source, and validity of the material to be displayed. Posters, leaflets, and other display materials issued by the Office of Campus Security, Office of Student Life, the Health Center, and other authoritative bodies are usually displayed in libraries, but items of a fractious or controversial kind, while not necessarily excluded, are considered individually.

The lobby of the school library is a mess. Plastered on the walls are notes, posters, and cards of all sizes and shapes. It is impossible to tell current from outdated messages. It is obvious that no one is paying any attention to the library exhibition policy. You have been asked to evaluate the policy and make the changes needed to achieve compliance.

1. Consider your audience. Rewrite the policy using plain language guidelines. You may encounter resistance to modifying the policy, so document the reason for each change, such as changing passive voice to active voice, eliminating redundant modifiers, and shortening sentences.

2. Expand the policy document to include goals and objectives, exceptions, and a policy enforcement clause.
3. Propose standards and guidelines to support the policy.
4. Propose how you would suggest introducing the policy, standards, and guidelines to the campus community.

## Reference

1. Baldwin, C., *Plain Language and the Document Revolution*. Lamplighter, 1999.

### Regulations Cited

“Executive Order—Improving Government Regulations,” accessed April 2024, <https://www.presidency.ucsb.edu/ws/?pid=30539>.

“A History of Plain Language in the Government,” accessed April 2024, <https://www.plainlanguage.gov/about/history/>.

“Executive Order 13563—Improving Regulation and Regulatory Review,” accessed April 2024, <https://obamawhitehouse.archives.gov/the-press-office/2011/01/18/executive-order-13563-improving-regulation-and-regulatory-review>.

“Public Law 111-274—Oct. 13, 2010 [Plain Writing Act],” accessed April 2024, <https://www.govinfo.gov/content/pkg/PLAW-111publ274/pdf/PLAW-111publ274.pdf>.

### Additional Reference

Krause, M., and H. F. Tipton. *Information Security Management Handbook*, 5th ed. CRC Press, 2004.

## A

**ABAC (attribute-based access control), 397–398**

**acceptable use agreement, 256–257, 270–271, 278, 420**

**access control, 384. *See also* authentication; layered security; remote access**

accounting, 398

attribute-based, 397–398

authentication, 385

by characteristic, 392

by knowledge, 388–390

multifactor, 391, 393

by ownership or possession, 390–391

passwordless, 413–415

discretionary, 394

ePHI (electronic personal health information), 575–576

facility, 572

identification, 385, 388

infrastructure, 399

layered security, 403

segmentation, 400–402

mandatory, 394

need-to-know principle, 387

network, 410. *See also* NAC (network access control)

object/subject, 385

payment card industry, 610–612

policy, 395

principle of least privilege, 387

role-based, 394–395, 396–397

rule-based, 395

security posture, 386

default deny, 386

open, 386

separation of duties, 387–388

user, 416–417

administrative accounts, 418–419

monitoring, 419–420

policy, 417

zero trust, 396

**accountability, 28, 92**

**accounting, 92, 398**

**ACL (access control list), 393**

**acquirer, 601**

**active voice, 55**

**AD (Active Directory), 159, 498**

**adaptable policy, 16–17**

**address randomization, 452**

**administrative account controls, 418–419**

**administrative notations policy, 66**

**administrative safeguards, HIPAA, 562**

assigned security responsibility, 564

business associate contracts and other arrangements, 570–571

contingency plans, 568–570

evaluation, 570

information access management, 565–566

security awareness and training, 566–567

security incident procedures, 567–568  
 security management process, 563–564  
 workforce security, 564–565

### **adoption, policy, 32**

### **agreement**

acceptable use, 256–257, 270–271, 420  
 confidentiality, 256–257, 269–270

### **AI (artificial intelligence), 13. *See also* “Guidelines for Secure AI System Development”; LLM (largelanguage model)**

applications, privacy concerns, 636  
 BOMs (bill of materials), 440–441  
 on the cloud, 166–167  
 explainable, 663–665  
 generative, 653–654  
 governance, 654  
     AI Risk Management Framework, 657–661  
     “Blueprint for an AI Bill of Rights”, 655–656  
     European Artificial Intelligence Board, 666–667  
     Executive Order 14110: Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, 655, 656–657  
     government and society-wide approaches, 665–666  
     “Guidelines for Secure AI System Development”, 670–673  
     NAIAC (US National AI Advisory Committee), 666  
     society-wide approach, 667  
 importance of high accuracy and precision, 661–663  
 inference, 661  
 leveraging to enhance privacy protections, 645–646  
 as a privacy protector and challenger, 636  
 privacy-preserving techniques, 637  
 as a service, 167  
 threat intelligence, 338–339  
 US policy, 4

### **algorithm/s, 454**

AI, 167, 653  
 asymmetric key, 456  
 Luhn, 603  
 machine learning, 338  
 Shor’s, 460  
 symmetric key, 456

### **allowlist, 406**

### **alpha phase, 445**

### **amendments, US Constitution, 7**

### **Americans with Disabilities Act, 263**

### **amplification attack, 91**

### **analysis and adjustment, OpEx/CapEx, 137**

### **API (application programming interface), DLP solutions, 243**

### **apparent data files, 303**

### **application/s**

AI, privacy concerns, 636  
 development policy, 453  
 dynamic data, 451  
 OWASP Top 10, 449  
 proxy, 405  
 security, 13  
 web  
     injection, 450  
     input validation, 451

### **APT (advanced persistent threat), 165–166**

### **architecture**

ISO 17789, 151–152  
 zero trust, 12. *See also* zero trust

### **ASLR (address space layout randomization), 452**

### **assessment, 529**

business impact, 482–484  
 risk, 202–203, 321  
     business continuity, 480–481  
     FAIR (Factor Analysis of Information Risk), 205  
     NIST RMF, 205



OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 204–205

threat, 524

## **asset/s, 11**

digital, 540–541

information, 221, 222

role of the data owner, 222–223

role of the information security officer, 224

inventory

controlling entity, 239

description, 238

hardware, 237, 238–239

software, 237

unique identifier, 237–238

management, 221, 239–240

## **assurance, 92**

information, 94–95

software, 448

test, 529

## **ASV (approved scanning vendor), 601**

## **asymmetric key, 456**

## **ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems), 683**

## **ATM card. *See also* PCI DSS (Payment Card Industry Data Security Standard)**

liability for unauthorized use, 600

skimming, 612

## **attack/s**

backdoor, 682–683

DDoS (distributed DoS)

amplification, 91

botnet, 91

direct, 91

reflected, 91

DoS (denial-of-service), 90–93, 325

evasion, 326

model inversion and extraction, 682

phishing, 539

prompt injection, 674–677

SolarWinds, 436

## **attainable policy, 16**

## **audience, policy, 56**

## **audit, 529**

business continuity plan, 501

controls, 576–577

cybersecurity, 187, 207

ISMS (information security management system), 102

report, 187

work papers, 502

## **Australia, Privacy Act of 1988, 24–25**

## **authentication, 92, 385, 577. *See also* password**

by characteristic, 392

credentials, 452

factors, 422

by knowledge, 388–390

mobile device, 414

multifactor, 155, 391, 393

multilayer, 393

mutual, 410

out-of-band, 391

by ownership or possession, 390–391

passwordless, 413–415, 423

policy, 398–399

## **authorization, 92, 385, 565. *See also* access control**

cybersecurity policy, 183

entry, 295

model, 393

permissions, 393

policy, 189, 393–394

## **automation, IAM (identity and access management), 157–161**

## **availability, 89–90**

DoS attack, 90–93

FIPS-199 (Federal Information Processing Standard 199), 227–228

threats, 90

## **AWS (Amazon Web Services), physical security practices, 292–293**

## B

---

**backdoor attack, 682–683**

**background check, 261–263, 278, 295–296**

**backup and restore, 569, 574**

**Bank Holding Company Act of 1956 (United States), 515–516**

**banking. *See* financial institution**

**Banking Act of 1933 (United States), 515–516**

**Basel III, 477**

**baseline, 48–49**

**Bell-LaPadula model, 225**

**beta phase, 445**

**BIA (business impact assessment), 482–484**

**Biba model, 225**

**Biden, Joe**

Executive Order 14028: Improving the Nation's Cybersecurity, 4

Executive Order 14110: Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, 4

**biometric system, 392, 414**

**black box test, 529–530**

**blackout, 300**

**blue team, 407**

**“Blueprint for an AI Bill of Rights”, 655–656**

**board of directors, 189**

approval of information security program, 522–524, 543

information security and GLBA compliance report, 532–533

**border device policy, 407–409**

**botnet, 91, 325**

**breach**

AT&T, 622

British Airways, 638

DarkBeam, 610

integrity, 323

Marriott International, 639

notification, 361

effectiveness, 365–366

federal agencies, 363

GLBA financial institution customer information, 361

HIPAA (Health Insurance Portability and Accountability Act of 1996), 362–363, 585–586

policy, 366

state laws, 364–365

Veterans Administration, 363–364

OnePlus, 610

PHI (personal healthcare information), 585

PII (personally identifiable information), 323

public relations, 367

residual risk, 203

Safe Harbor Provision, 584–585

VERIS community database, 389

**brownout, 300**

**browser-based data, 303**

**BSCA (Bank Service Company Act (United States), 531**

**buffer overflow, 91**

**Buffett, Warren, on using plain language, 52**

**bugs, 88–89**

**business. *See also* CE (covered entity); service provider; small business; vendor**

client, 181

corporate account takeover, 539

impact analysis, 568

impact assessment, 482–484

risk, 204

Torah laws, 7

-as-usual approach, 605–606

**business associate, 578–579, 582, 583**

**business continuity, 474**

cloud service, 493–494. *See also* cloud/cloud computing, BC/DR (business continuity/disaster recovery)

for data centers, 494–495

disaster response plan, 488–489

command and control centers, 489

communication, 490

- organizational structure, 489
- relocation strategies, 490–492
- education, 488
- emergency preparedness, 475–476
- governance, 485–486
- operational management, 486
- plan, 485, 500, 502
  - audit, 501
  - testing methodologies, 500–501
- policy, 487
- regulatory requirements, 477–478
- resilient organization, 476–477
- risk assessment, 480–481, 504
- risk management, 479
- tactical activities, 486–487
- team, 486
- threat assessment, 479–480

**BYOD (bring your own device), 299**

## C

**C&A (certification and accreditation), 443**

**CA (certificate authority), 456**

**California Security Breach Information Act, 26, 364**

**Cambridge Analytica scandal, 638**

**Canada. See PIPEDA (Personal Information Protection and Electronic Documents Act)**

**candidate data, 260**

**CapEx (capital expenditures), 136**

- analysis and adjustment, 137
- cloud computing, 137
- cloud/cloud computing, 135–136

**cardholder data environment, 602, 604, 612**

**CCPA (California Consumer Privacy Act), 22, 640**

- comparing with other data protection regulations, 644–645
- versus GDPR, 641
- key provisions and compliance requirements, 640–641

**CE (covered entity). See also business associate; HIPAA (Health Insurance Portability and Accountability Act of 1996)**

- breach notification requirements, 585–586
- business associate contracts, 578–579
- Safe Harbor Provision, 584–585

**centralized control and coordination, cloud computing, 142**

**CER (crossover error rate), 392**

**CERT (computer emergency response team), national, 346**

**certification**

- business continuity management, 488
- CISA, 188

**chain of custody, 329, 358**

**change control, 162**

**change drivers, cybersecurity policy, 190**

**characteristic, authentication by, 392**

**CIA triad, 81–82, 118**

- availability, 89–90
  - DoS attack, 90–93
  - threats, 90
- confidentiality, 84, 88
  - data classification, 83
  - encryption, 83
  - hacktivism, 84
  - laws, 84
- FIPS-199 (Federal Information Processing Standard 199), 226–228
- integrity, 88–89
- owners, 93–94

**cipher text, 453–454**

**CISA (Cybersecurity & Infrastructure Security Agency), 322. See also “Guidelines for Secure AI System Development”**

- BOD (Binding Operational Directive) 22–01, Reducing the Significant Risk of Known Exploited Vulnerabilities”, 86
- certification, 188
- KEV catalog, 85–86

**Cisco ESA, 243**

**Clarity Index, 55–56****Clarke, Richard, 11****classification, 245**

fire, 301–302

information, 224–225

federal government, 226–228

life cycle, 226

national security, 228–230

private sector, 225, 230–231

security incident, 327–328

small business, 241–242

workspace, 296

**cloud/cloud computing, 13**

AI (artificial intelligence), 166–167

attributes, 133

auditor, 152

BC/DR (business continuity/disaster recovery), 493

best practices, 493–494

disaster recovery phase, 497

operational contingency plans, 495

operational contingency procedures,  
495–496

recovery procedures, 497–498

resumption phase, 499–500

service provider dependencies, 499

versus traditional data centers, 494–495

bursting, 135

carrier, 152

consumer, 151

cost-benefit analysis, 135

analysis and adjustment, 137

CapEx (capital expenditures), 135–136, 137

OpEx (operational expenditures), 136, 137

cybersecurity risks

advanced persistent threats and sophisticated  
malware, 165–166

data breaches and loss, 154–155

IAM (identity and access management),  
155–156

insider threats, 164–165

lack of visibility and control over data, 163

misconfiguration and inadequate change  
control, 161–162

elasticity, 134

FaaS (function as a service), 140

FinServ LLP case study, 138–139

functional layers, 152–153

governance, 141, 147–148

centralized control and coordination, 142

standardization and compliance, 142–146

IaaS (infrastructure as a service), 140

IAM (identity and access management),  
155–156, 157–161

identity federation, 156–157

information security controls, 106–107

ISO 17789, 151–152, 153

multitenancy, 150–151

-native, 12

PaaS (platform as a service), 140

physical security, 292–293

provider, 148–150, 151–152

regulator, 152

SaaS (software as a service), 139

scalability, 134

security assessment, 23

service models, 139–140

service partner, 152

shadow IT, 146–147

shared responsibility model, 141

SSAE 18 (Statement on Standards for  
Attestation Engagements No. 18), 149

transferring regulatory responsibilities and costs  
to the, 148–150

**CloudLock, 243****CMM (capability maturity model), 188–189****code, 448**

infrastructure as, 149

input validation, 451

output validation, 451–452

**cognitive password, 389–390**

**cold site, 491**

**command and control centers, 489**

**communication**

disaster response plan, 490

information sharing and coordination, 336

policy, 30–31

**company property, disposal, 240–241**

**compliance. *See also* administrative safeguards; enforcement; GLBA (Gramm-Leach Bliley Act); HIPAA (Health Insurance Portability and Accountability Act of 1996); regulation/regulatory requirements; standard/s**

cloud, 143–145

leveraging providers, 148–150

outsourcing, 148–150

GLBA (Gramm-Leach Bliley Act). *See* GLBA (Gramm-Leach Bliley Act)

officer, 186

PCI DSS (Payment Card Industry Data Security Standard)

assessment, 617

merchant, 616

report, 619

validation, 616–617

risk, 525

**confidentiality, 84, 88**

agreement, 256–257, 269–270, 278

data classification, 83

encryption, 83

FIPS-199 (Federal Information Processing Standard 199), 227

hacktivism, 84

laws, 84

**consent, background check, 262**

**consolidated policy, 57, 62**

**Constitution of the United States, 7–8**

**content filtering, 406**

**contingency plan, 485, 568–570**

**continuity planning, 479**

**contract, business associate, 570–571, 578–579**

**controlling entity, 239**

**controls, 203, 543. *See also* access control**

audit, 576–577

business-as-usual approach, 605–606

device and media, 573–574

fire prevention, 301

integrity, 577

malware, 610

offensive/defensive, 199

physical. *See* physical security

preventive, 481

**coordination centers, 346**

**COPPA (Children’s Online Privacy Protection Act), 22**

**core functions, CSF (NIST Cybersecurity Framework), 112–114**

**corporate account takeover fraud advisory, 539**

**corporate culture, 8–9**

guiding principles, 8

negative, 8–10

positive, 10

**cost-benefit analysis, cloud computing, 135**

analysis and adjustment, 137

CapEx (capital expenditures), 135–136, 137

OpEx (operational expenditures), 136, 137

**COTS (commercial off-the-shelf software), 445**

**COVID-19 pandemic, 476–477**

**CPSA (Card Production Security Assessor), 618**

**CPTED (Crime Prevention Through Environmental Design), 294**

**CRA (Cyber Resilience Act), 195–197**

**credit card. *See also* PCI DSS (Payment Card Industry Data Security Standard)**

elements, 603

liability for unauthorized use, 600

skimming, 612

**crime. See cybercrime**

**critical infrastructure sectors, 2–3**

**cryptography/cryptographic, 453, 462–463**

decryption, 454

encryption, 453, 455

cipher text, 453–454

regulatory requirements, 455

key, 455–456

asymmetric, 456

management, 457–458, 459

public, 456

symmetric, 456

post-quantum, 460

approaches, 460

challenges and progress, 461

**CSAF (Common Security Advisory Framework), 439**

**CSIRT (computer security incident response team), 339–341, 346**

**CSPM (cloud security posture management), 163**

**CTAP (Client to Authenticator Protocol), 415**

**culture**

corporate, 8–9

negative, 8–10

positive, 10

shaping, 8

**CVSS (Common Vulnerability Scoring System), 84**

CVE-2024–20305 vulnerability, 85

CVE-2024–23222 vulnerability, 84–85

versus EPSS, 86–87

metric groups, 342

scoring, 86

**CWE (Common Weakness Enumeration), 450**

**cyber, 11**

**Cyber Essentials, 24**

**cyber range, 529**

**cybercrime, 11, 435. See also breach**

corporate account takeover, 539

data card breach, 610

identity theft, 537

**cyber-insurance, 200**

**cybersecurity, 6. See also NIST, Cybersecurity Framework; security**

audit, 207

critical infrastructure sectors, 2–3

education, 272–273

“EU CRA Roadmap”, 4–5

forensic evidence, 328–329

framework, 94, 118

governance, 179

integrated approach, 178

objective, 28–29, 34

policy/ies, 10, 177

audit, 187

authorization, 183

change drivers, 190

client synopsis, 181–182

evaluation, 187

life cycle, 28–29

risk assessment, 206

risk management, 202

risk response, 200

user-level, 180

vendor, 180

vulnerability disclosure, 180

regulatory requirements, 179

risk, 197–198

silo-based approach, 177, 178

standards. *See also* standards

ISO (International Organization for Standardization), 96

ISO/IEC 27000 series, 97–98

steering committee, 186

strategic alignment, 178–179

training policy, 277

**Cybersecurity Coalition, “EU CRA Roadmap”, 4–5**

## D

### **D33ds Company, 390**

### **DAC (discretionary access control), 394**

### **data. *See also* information**

- apparent, 303
- breach, 154–155. *See also* breach
  - notification requirements, 360–366
  - PII (personally identifiable information), 323
  - report, 306
  - residual risk, 203
- browser-based, 303
- cache, 303
- candidate, 260
- classification, 83
- confidential, 231
- custodian, 187
- de-identification, 447
- destruction, 304
  - degaussing, 304–305
  - disk wiping, 304
- on devices, 303–304
- dummy, 447
- dynamic, 451
- exfiltration, 243
- hidden, 303
- integrity, 88
- internal use, 231
- mining, 517
- in motion, 577–578
- owner, 187, 222–223
- protected, 230–231
- removing from drives, 304
- at rest, 83
- temporary, 303
- user, 187

### **data center**

- business continuity and disaster recovery
  - strategies, 494–495
- fire threats, 301–302

### **Data Protection Act 2018, 24, 643–645** **database**

- EMR (electronic medical records), 447
- VERIS, 389

### **DDoS (distributed DoS) attack, 90**

- amplification, 91
- botnet, 91
- direct, 91
- reflected, 91

### **deactivation, 500**

### **debit card. *See also* PCI DSS (Payment Card Industry Data Security Standard)**

- liability for unauthorized use, 600
- skimming, 612

### **declassification, 232, 245**

### **decryption, 454**

### **default deny, 386**

### **defense-in-depth, 11–13**

### **defensive control, 199**

### **degaussing, 304–305**

### **de-identification, 447**

### **denylist, 406**

### **derivative classification, 230**

### **destruction**

- company property, 240–241
- data, 304
  - degaussing, 304–305
  - disk wiping, 304
- physical, 305

### **detection and analysis phase, incident response, 333–334**

### **detection systems, perimeter, 294**

### **DFARS (Defense Federal Acquisition Regulation Supplement), 22–23**

### **digital assets, 540–541**

### **digital certificate, 456–457**

### **digital forensic evidence, 328, 357–358**

### **digital privacy, 635**

### **digital signature, 454**

### **DIH (designated incident handler), 347**

**direct DDoS attack, 91**

**directors, duty of care, 183**

**disaster recovery in cloud services, 493–495, 497, 499**

**disaster response plan, 488–489, 493–495**

- command and control centers, 489
- communication, 490
- organizational structure, 489
- recovery, 569
- relocation strategies, 490–492
- small business, 503

**disclosure**

- sensitive information, 680
- vulnerability, 180–181

**disk wiping, 304**

**disposal, 443. *See also* destruction**

- company property, 240–241
- devices containing data, 303–304
- ePHI (electronic personal health information), 574

**dissemination, policy, 31**

**distributed governance model, 184. *See also* leaders and leadership**

**DLP (data loss prevention), 242–255**

**DMZ, 400**

**documents**

- CSAF, 439
- HIPAA Security Rule, 580–581
- incident, 350
- plain-language, 46
- VEX (Vulnerability Exploitability eXchange), 439

**domains, security, 81**

**DoS (denial-of-service) attack, 90–93, 325**

- buffer overflow, 91
- model, 678–679

**dual control, 418**

**dummy data, 447**

**duty of care, 183**

**dynamic data, 451**

## E

---

**education. *See also* training**

- business continuity management, 488
- cybersecurity, 272–273
- policy, 31
- security, 276–277

**EFTA (Electronic Fund Transfer Act), 600**

**elasticity, 134**

**electronic monitoring policy, 267**

**emergency preparedness. *See also* disaster response plan**

- disasters, 475–476
- policy, 478

**employee. *See also* job**

- acceptable use agreement, 270–271
- agreement policy, 271
- confidentiality agreement, 269–270
- life cycle, 257–259
- orientation, 267
- payroll
  - Form I-9, 265
  - Form W-4, 265–266
- recruitment, 259
  - interview, 260
  - job postings, 259
- remote worker security, 411–413
- right to privacy, 262
- screening, 261
- screening policy, 264
- security awareness and training program, 272
- security clearance investigation, 264–265
- termination, 268, 269
- user provisioning, 266

**enclave network, 400**

**encryption, 83, 453, 455**

- cipher text, 453–454
- digital signature, 454
- hash, 454
- homomorphic, 637



- message integrity, 454
- regulatory requirements, 455
- endorsement, policy, 14–15**
- enforceable policy, 17–18**
- enforcement**
  - clause, 65
  - FTC Safeguards Act, section 5, 520
  - GLBA (Gramm-Leach Bliley Act), 20, 516
  - HIPAA (Health Insurance Portability and Accountability Act of 1996), 582, 583–584, 586–587
  - policy, 32
- environmental sustainability, 308–309**
- ePHI (electronic personal health information), 21, 558, 570**
  - access control, 575–576
  - backup and storage, 574
  - disposal policies, 574
  - reuse policies, 574
  - transmission security, 577–578
- EPSS (Exploit Prediction Scoring System), versus CVSS, 86–87**
- equipment**
  - power protection, 299–300
  - theft, 306–307
- errors, 88–89, 392**
- ESG (environmental, social, and governance), 515**
- essential services, 482**
- “EU CRA Roadmap”, 4–5**
- European Artificial Intelligence Board, 666–667**
- European Union**
  - AI Act, 4, 667–669
  - CRA (Cyber Resilience Act), 4, 195–197
  - CSA (Cyber Solidarity Act), 5
  - fintech, regulation, 541
  - GDPR (General Data Protection Regulation), 23, 637
    - comparing with other data protection regulations, 644–645

- impact on businesses, 638–639
- key principles, 637–638
- regulatory requirements, 194
- rights for individuals, 639–640
- scope, 639–640
- evaluation, cybersecurity policy, 187**
- evasion attack, 326**
- event, 323**
- evidence, 349**
  - chain of custody, 329, 358
  - digital forensic, 328, 357–358
  - storing and retaining, 359
- exam, regulatory, 535–536, 544**
- exceptions, policy, 64**
- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 4**
- Executive Order 14110: Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, 655, 656–657, 669**
- exemption, policy, 61, 64–65, 69**
- exploit, 343**

## F

---

- FaaS (function as a service), 140**
- facility access controls, 572**
- factors, authentication, 422**
- FAIR (Factor Analysis of Information Risk), 205**
- false negative, 325, 406**
- false positive, 325, 406**
- FAR (Federal Acquisition Regulation), 22–23**
- fault, 300**
- FCBA (Fair Credit Billing Act), 600**
- FCC (Federal Communications Commission), 478**
- Federal Register, 519**
- federated learning, 637**
- feedback**
  - incident response, 337

output validation, 451–452

policy, 33

## **FERPA (Family Educational Rights and Privacy Act of 1974), 26**

## **FFIEC (Federal Financial Institutions Examination Council)**

Cybersecurity Assessment Tool, 527–528

*Information Technology Examination Handbook InfoBase*, 502, 526

Supplement to the Authentication in an Internet Banking Environment Guidance, 538–539

Uniform Rating System for Information Technology, 536

## **FIDO2, 414–415**

## **financial institution. See also Interagency Guidelines for Safeguarding Member Information**

acquirer, 601

board approval of information security program, 522–524, 543

Cybersecurity Assessment Tool, 527–528

data breach, 361

ESG (environmental, social, and governance), 515

FFIEC IT Handbook, 526

GLBA (Gramm-Leach Bliley Act)

definition of financial institution, 516

Information Protection Directive, 517–518

regulatory oversight, 518–519

information, integrity, 89

information security program, 520–521

adjusting, 531–532

reporting to the board, 532–533

information security training, 528–529

inherent risk, 524

Interagency Guidelines for Safeguarding Member Information, 520–522

managing and controlling risk, 525–526

New York Department of Financial Services cybersecurity regulation, 533–535

notification requirements, 538

regulatory compliance, 514–515

regulatory examination, 535–536

residual risk, 524

response program, 537–538

risk assessment, 524–525

threat assessment, 524

## **FinServ LLP case study, 138–139**

## **fintech, 539–541**

## **FIPS-199 (Federal Information Processing Standard 199), 226–228**

## **fire, 301**

containment and suppression, 301

detection, 301

prevention controls, 301

protection, 301–302

## **firewall**

application proxy, 405

NAT (network address translation), 405

network-based, 404–405

packet filter, 404–405

PAT (port address translation), 405

policy, 403

## **FIRST (Forum of Incident Response and Security Teams), 86**

## **first-party risk, 200**

## **FISMA (Federal Information Security Management Act), 21, 93, 245**

## **“Five A’s” of information security, 92–93**

## **flowchart, 50**

## **FOIA (Freedom of Information Act), 226**

## **forensic evidence**

cybersecurity, 328–329

digital, 328

## **Form I-9, 265**

## **format, policy, 57–58**

## **formatting, hard drive, 304**

## **framework, 80–81, 118. See also ISO/IEC 27000 series; PCI DSS (Payment Card Industry Data Security Standard)**

Basel III, 477

CIA triad, 81–82, 118

availability, 89–90

confidentiality, 82–84, 88

integrity, 88–89

owners, 93–94

Common Security Advisory, 345, 439

CVSS (Common Vulnerability Scoring System), 84–85

cybersecurity, 94

EPSS (Exploit Prediction Scoring System), 86–87

FIDO2, 414–415

MITRE ATLAS, 683

MITRE ATT&CK, 352–353

NIST AI Risk Management, 657–658

core functions, 658

implementation, 658–661

NIST Cybersecurity, 110

core functions, 112–114

implementation examples, 114–115

informative references, 114

objective, 111–112

scope, 112

SecretCorp, 115–116

NIST Privacy, 116–117

regulatory, impact on cloud computing, 143–145

Risk Management, 205

Secure Software Development, 444–445

## **FTC (Federal Trade Commission), 516**

consumer complaints, 520

notice of security breach, 362

Safeguards Act, 519–520

## **full-scale testing, 501**

## **functional exercises, 501**

## **functional layers, cloud, 152–153**

# **G**

## **GDPR (General Data Protection Regulation), 23, 637**

Article 33, 323

versus CCPA, 641

comparing with other data protection regulations, 644–645

impact on businesses, 638–639

key principles, 637–638

regulatory requirements, 194

right to be forgotten, 639

rights for individuals, 639–640

scope, 640

## **generative AI, 653–654**

## **Glass-Steagall Act (United States), 515–516**

## **GLBA (Gramm-Leach Bliley Act), 20, 516, 542. *See also* Interagency Guidelines for Safeguarding Member Information**

definition of financial institution, 516

Information Protection Directive, 517–518

information security and GLBA compliance report, 532–533

involving the board of directors, 522–524

notice of security breach, 361

regulatory oversight, 518–519

regulatory requirements, 193

risk assessment, 524–525

Section IIIC-2: Training, 528–529

Section IIIC-3: Testing, 529–530

Section III-D: Oversee Service Provider, 530–531

Section III-E: Adjust the Program, 531–532

Title 5, 517

## **global policy, 28**

## **governance, 113, 179, 207**

AI, 654

AI Risk Management Framework, 657–661

“Blueprint for an AI Bill of Rights”, 655–656

European Artificial Intelligence Board, 666–667

Executive Order 14110: Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, 655, 656–657

government and society-wide approaches, 665–666

“Guidelines for Secure AI System Development”, 670–673

- NAIAC (US National AI Advisory Committee), 666
  - society-wide approach, 667
  - business continuity management, 485–486
  - cloud, 141, 147–148
    - centralized control and coordination, 142
    - standardization and compliance, 142–146
  - distributed model, 184
  - information security, 105–106
  - NIST definition, 177
  - subcategories of the Cybersecurity Framework, 191–193
  - government**
    - use of plain language, 52–53
    - wide approaches to AI governance, 665–666
  - guest network, 400**
  - guidelines, 49, 53–54. See also Interagency Guidelines for Safeguarding Member Information**
  - “Guidelines for Secure AI System Development”, 670–671**
    - AI supply chain security, 672–673
    - provider and user responsibility, 671–672
  - guiding principles, 8, 47**
- 
- ## H
- hacktivism, 84, 87**
  - handling standards, 233–235**
  - hard drive**
    - deleting a file, 304
    - formatting, 304
    - physical destruction, 305
  - hardware**
    - assets, 237
    - logical address, 238–239
  - hashing, 454**
  - heading, policy, 61–62**
  - healthcare sector. See also HIPAA (Health Insurance Portability and Accountability Act of 1996)**
    - identity federation, 156–157
    - notice of security breach, 362–363
  - hidden data, 303**
  - hierarchical procedures, 50**
  - hierarchy, policy, 47, 182**
  - HIPAA (Health Insurance Portability and Accountability Act of 1996), 21, 477–478, 556–557, 570–571**
    - administrative safeguards, 562
      - assigned security responsibility, 564
      - business associate contracts and other arrangements, 570–571
      - contingency plans, 568–570
      - evaluation, 570
      - information access management, 565–566
      - security awareness and training, 566–567
      - security incident procedures, 567–568
      - security management process, 563–564
      - workforce security, 564–565
    - Breach Notification Rule, 585–586
    - CE (covered entity), 558–559
    - enforcement, 583, 586–587
      - proactive, 584
      - state attorney general, 584
    - implementation specifications, 561
    - notice of security breach, 362–363
    - organizational requirements, 578–579
    - physical safeguards, 571
      - device and media controls, 573–574
      - facility access controls, 572
      - workstation security, 573
      - workstation use, 572
    - regulatory requirements, 194
    - Safe Harbor Provision, 584–585
    - security rule, 558–559
      - categories, 560–561
      - documentation, 580–581
      - mapping to the NIST Cybersecurity Framework, 581
      - objective, 559–560

- policies and procedures, 580
  - technical safeguards, 574–575
    - access control, 575–576
    - audit controls, 576–577
    - integrity controls, 577
    - person or entity authentication, 577
    - transmission security, 577–578
  - training, 584
- HITECH (Health information Technology for Economic and Clinical Health) Act, 21, 362–363, 557, 581–582**
- homomorphic encryption, 637**
- honoring the public trust, 10**
- host security, 12**
- hot site, 490–491**
- human resources. See employee; onboarding; recruitment, employee**

---

**I**

- IaaS (infrastructure as a service), 140**
- IaC (infrastructure as code), 149**
- IAM (identity and access management)**
  - automating, 157–161
  - identity federation, 156–157
  - risks, 155–156
- ICAO (International Civil Aviation Organization), 478**
- ICO (Information Commissioner's Office), 24**
- ICT (information and communication technology), 108–109**
- identification, 385, 388, 447**
- identity federation, 156–157**
- identity management, 385–386**
- identity theft, 537, 538**
- IDS (intrusion detection system), 405–406**
- impact, 203, 226, 482–484**
- implementation**
  - AI RMF, 658–661
  - examples, 114–115

- ISMS (information security management system), 99–100
- policy, 32
- specification, 567
- specifications, HIPAA, 561
- incident/incident response, 114, 187, 322–324, 567–568**
  - containment, eradication, and recovery phase, 334
  - coordination centers, 346
  - definition, 323–324
  - detection and analysis phase, 333–334
  - documents, 350
  - DoS (denial-of-service) attack, 325
  - versus event, 323
  - evidence
    - chain of custody, 329, 358
    - cybersecurity forensic, 328–329
    - digital forensic, 328, 357–358
    - storing and retaining, 359
  - false negative, 325
  - false positive, 325
  - inappropriate usage, 326
  - information sharing and coordination, 336
  - intentional unauthorized access or use, 324–325
  - malware, 326
  - MSSP (managed security service provider), 346–347
  - operationalizing threat intelligence, 336–338
  - personnel, 347–348
  - plan, 330–331
  - playbook, 335
  - post-incident activity phase, 335
  - preparation phase, 333
  - preparedness, 321–322
  - program, 330, 332, 537–538
  - providers, 346–347
  - reporting, 328
  - severity level, 326–328
  - SIGMA, 356

SOP (standard operating procedure), 331

tabletop exercises, 336

team

computer security, 339–341

product security, 341–345

training, 348–349

true positive, 325

using AI, 338–339

working with law enforcement, 350–351

### **inclusive policy, 18–19**

### **India, Information Technology Act of 2000, 25–26**

### **inference, 661**

### **information**

asset, 11, 221, 222

role of the data owner, 222–223

role of the information security officer, 224

assurance, 94–95

classification, 224–225

federal government, 226–228

life cycle, 226

policy, 232

private sector, 225, 230–231

small business, 241–242

confidential, 84. *See also* confidentiality

custodian, 94

declassification, 232

handling standards, 233–235

labeling, 233

national security, 228–230

derivative classification, 230

original classification, 230

nonpublic personal, 231

organizational, 221–222

owner, 93, 118

ownership policy, 224

personal, 26, 27

reclassification, 232–233

SC (security category), 227, 228

security, 6. *See also* CIA triad

controls, 102–103

financial institution. *See* Interagency Guidelines for Safeguarding Member Information

“Five A’s”, 92–93

framework, 80–81. *See also* framework

governance, 105–106

honoring the public trust, 10

multidisciplinary approach, 523

testing, 529

training, 528–529

system, 222

systems inventory, 236–237

asset inventory characteristics and attributes, 237–240

hardware assets, 237

software assets, 237

### **Information Technology Act (India, 2000), 25–26**

### **informative references, CSF (NIST Cybersecurity Framework), 114, 191–193**

### **infrastructure, 422**

access control, 399. *See also* layered security

layered security, 403

segmentation, 400–402

as code, 149

critical, 2–4

as a service, 140

### **inherent risk, 202, 524**

### **injection, 450**

### **innovation, 16–17**

### **input validation, 451**

### **insider threat, 164–165, 268, 274–276, 406**

### **integrated approach, cybersecurity, 178**

### **integrity**

breach, 323

controls, 577

FIPS-199 (Federal Information Processing Standard 199), 227

message, 454

system, 88

**Interagency Guidelines for Safeguarding Member Information, 520–521, 542**

- board approval of information security program, 522–524
- delegation of responsibilities, 522–523
- managing and controlling risk, 525–526
- Supplement A, 537–538
- terminology, 521–522
- training, 528–529

**internal audit, 187**

**internal use data, 231**

**interview, job candidate, 260**

**introduction, policy, 59–61**

**inventory. *See also* asset/s**

- AI BOM (artificial intelligence bill of materials), 440–441
- information systems, 236–237
  - asset inventory characteristics and attributes, 237–240
  - hardware assets, 237
  - policy, 241
  - software assets, 237
- SBOM (software bill of materials), 345, 437–438
  - enhancing vulnerability management, 438
  - promoting transparency and trust, 438

**IoC (indicator of compromise), 351, 387**

**IP (intellectual property), DLP (data loss prevention), 242–255**

**IP address, 403**

**IPS (intrusion prevention system), 405–406**

- evasion attacks, 326
- false positive/false negative, 325

**IRC (incident response coordinator), 347**

**IRT (incident response team), 347–348**

**ISMS (information security management system)**

- auditing, 102
- implementation, 99–100
- measurement, 100

**ISO (information security officer), 224**

**ISO (International Organization for Standardization), 81, 95–96, 118**

- 17788 document, 134
- 17789 Cloud Computing Reference Architecture, 151–152, 153
- importance of cybersecurity standards, 96

**ISO/IEC 27001: Information Security Management Systems—Requirements, 98–99, 341**

**ISO/IEC 27002: Code of Practice for Information Security Controls, 99, 291, 341, 434, 525–526**

- access control, 385
- asset management, 221
- business continuity management, 475
- compliance management, 558
- cryptography, 435
- incident management, 321

**ISO/IEC 27003: Information Security Management System Implementation Guidance, 99–100**

**ISO/IEC 27004: Information Security Management System—Measurement, 100**

**ISO/IEC 27005: Information Security Risk Management, 100–101, 341**

**ISO/IEC 27006: Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, 101**

**ISO/IEC 27007: Guidelines for Information Security Management Systems Auditing, 102**

**ISO/IEC 27008: Guidelines for Auditors on Information Security Controls, 102–103**

**ISO/IEC 27009: Sector-Specific Application of ISO/IEC 27001—Requirements, 103**

**ISO/IEC 27010: Information Security Management for Inter-Sector and Inter-Organizational Communications, 103–104**

**ISO/IEC 27011: Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002, 104–105**



**ISO/IEC 27013: Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000–1, 105**

**ISO/IEC 27014: Governance of Information Security, 105–106**

**ISO/IEC 27017: Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services, 106–107**

**ISO/IEC 27018: Code of Practice for Protection of PII in Public Clouds Acting as PII Processors, 107**

**ISO/IEC 27019: Information Security for Process Control in the Energy Industry, 107–108**

**ISO/IEC 27031: Guidelines for Information and Communication Technology Readiness for Business Continuity, 108–109**

**ISO/IEC 27033, 341**

**ISO/IEC 27099: Public Key Infrastructure—Practices and Policy Framework, 109–110**

**ISP (Internet service provider), 89**

## IT

- leadership, 142
- shadow, 146–147

## J

**Japan, PIPA (Personal Information Protection Act), 25**

## job

- candidate data, 260
- candidate interview, 260
- postings, 259
- recruitment policy, 260

## K

**KASLR (kernel address space layout randomization), 452**

**KEV catalog, 85–86**

## key, 463

- asymmetric, 456
- encryption, 455–456

management, 454, 457–458, 459

public, 456

compromise, digital certificate, 458

digital certificate, 456–457

symmetric, 456

## knowledge

authentication by, 388–390

cognitive password, 389–390

out-of-wallet challenge questions, 389–390

## L

### labeling, 233

**law/s. *See also* legislation; regulation/ regulatory requirements**

confidentiality, 84

enforcement, incident response, 350–351

### layered defense model, 292

### layered security, 423

allowlisting/denylisting, 406

border device administration and management, 407

content filtering, 406

firewall

application proxy, 405

NAT (network address translation), 405

network-based, 404–405

packet filter, 404–405

PAT (port address translation), 405

policy, 403

IDS/IPS, 405–406

### leaders and leadership

board of directors, 189

CISO (chief information security officer), 184–185

cybersecurity steering committee, 186

IT, 142

policy communication, 30–31

**legislation, 19, 20, 21, 193. *See also* GLBA (Gramm-Leach Bliley Act); HIPAA (Health Insurance Portability and Accountability Act of 1996)**



**legitimacy, global policy, 28****liability**

- director, 183
- subcontractor, 583
- unauthorized credit card, debit card, and ATM use, 600

**life cycle**

- employee, 257–259
- information classification, 226
- policy, 28–29
- secure development, 344
- systems development, 434

**lighting, perimeter, 294****likelihood of occurrence, 203****Linux, KASLR (kernel address space layout randomization), 452****LLM (large language model), 653–654**

- OWASP Top 10 Risks, 449, 674
  - backdoor attack, 682–683
  - excessive agency, 681
  - insecure output handling, 678
  - insecure plugin design, 680–681
  - model denial of service, 678–679
  - model inversion and extraction, 682
  - model theft, 682
  - overreliance, 681
  - prompt injection attacks, 674–677
  - sensitive information disclosure, 680
  - supply chain vulnerabilities, 679–680
  - training data poisoning, 678

**logical address, 238–239****Luhn algorithm, 603****LulzSec, 87****M****MAC (mandatory access control), 394****machine learning, 338, 653****malware, 326**

- controls, 610

Mirai botnet, 325

sophisticated, 165–166

**Massachusetts, 0201 CMR 17: Standards for the Protection of Personal Information Residents of the Commonwealth, 27, 364****maturity, 188****measurement, ISMS (information security management system), 100****medical information, integrity, 89****memory card, 391****merchant, 601–602, 616. See also PCI DSS (Payment Card Industry Data Security Standard)****message integrity, 454****metadata, 304****metric groups, CVSS, 342****MFA (multifactor authentication), 155, 391, 393, 423****Microsoft UAC (User Account Control), 418****Mirai botnet, 325****mirrored site, 492****misconfiguration, 161****MITRE**

- ATLAS framework, 683
- ATT&CK framework, 352–353

**mobile device, authentication, 414****mobile site, 491****model. See also AI (artificial intelligence)**

- authorization, 393
- capability maturity, 188–189
- denial of service, 678–679
- distributed governance, 184
- inversion and extraction attacks, 682
- large language. *See* LLM (large language model)
- layered defense. *See* layered defense model
- security
  - Bell-LaPadula, 225
  - Biba, 225
  - service, 139–140

SETA (Security, Education, Training, and Awareness), 256–257, 273

shared responsibility model, 141

theft, 682

## **monitoring**

legality, 420

network, 613–614

user access, 419–420

**MSSP (managed security service provider), 346–347**

**MTD (maximum tolerable downtime), 482–483**

**multidisciplinary approach, information security, 523**

**multilayer authentication, 393**

**multitenancy, 150–151**

**mutual authentication, 410**

# **N**

---

**NAC (network access control), 386, 410**

security posture, 386

threat-centric, 386–387

**NACD (National Association of Corporate Directors), 183**

**NAIAC (US National AI Advisory Committee), 666**

**NAT (network address translation), 405**

**National Laboratory of Medicine, “The discourse of organizational resilience before and after the global pandemic”, 476–477**

**national security information, 228–230**

derivative classification, 230

original classification, 230

**NCSL (National Conference of State Legislatures), 365**

**need-to-know principle, 387**

**negative corporate culture, 8–10**

**NERC (North American Electric Reliability Corporation), 478**

**network**

access control. *See* NAC (network access control)

-based firewall, 404–405

DMZ, 400

enclave, 400

guest, 400

infrastructure, 422

monitoring, 613–614

security, 12

segmentation, 400–402

untrusted, 400

virtual private. *See* VPN (virtual private network)

## **New York**

Department of Financial Services cybersecurity requirements, 27, 194, 533–535

SHIELD Act, 364

**NICE (National Initiative for Cybersecurity Education), 272–273**

insider threat analysis, 274–276

work roles and categories, 273–274

**NIS (Network and Information Systems) Directive, 23, 81, 194**

**NIST (National Institute of Standards and Technology)**

AI Risk Management Framework, 657–658

CSD (Computer Security Division), 94

Cybersecurity Framework, 110, 118, 176, 520

Asset Management category, 221

core functions, 112–114

governance subcategories, 191–193

implementation examples, 114–115

informative references, 114

mapping to HIPAA, 581

objective, 111–112

PR.IP-11 subcategory, 257

scope, 112

SecretCorp, 115–116

Framework for Improving Critical Infrastructure Cybersecurity, 4

governance, definition, 177

incident response plan, 331

information assurance framework, 94–95

informative references, 191–193

NICE (National Initiative for Cybersecurity Education), 272–274, 528

physical security documents, 291–292

Privacy Framework, 116–117, 118

publications, 95

RMF (Risk Management Framework), 205

SP 800–16, 276–277

SP 800–34: Contingency Planning Guide for Federal Information Systems, 478

SP 800–46: Guide to Enterprise Telework, Remote Access and Bring Your Own Device, 409

SP 800–50, 272

SP 800–61: Computer Security Incident Handling Guide, 321–322, 330–331, 334

SP 800–63B: Digital Identity Guidelines: Authenticaiton and Lifecycle Management, 389

SP 800–87, 357–358

SP-41: Guidelines on Firewalls and Firewall Policy, 403

SP-94: Guide to Intrusion Detection and Prevention Systems, 406

SSDF (Secure Software Development Framework), 444–445

vulnerability, definitions, 203

**Nixon, Richard, 52**

**nondisclosure agreement, 269–270**

**normative integration, 32**

**notification**

- financial institution, requirements, 538
- security breach, 27. *See also* breach, notification

**NPI (nonpublic information), DLP (data loss prevention), 242–255**

**NPPI (nonpublic personal information), 26, 231, 260, 518**

**NPPI (nonpublic personally identifiable information), 245**

## O

---

**object, access control, 385**

**object capability model, 393**

**objective**

- policy, 62–63
- threat hunting, 351

**obstacles, perimeter, 294**

**OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 204–205**

**OEP (occupant emergency plan), 490**

**offensive control, 199**

**OMB Memorandum M-07–16 “Safeguarding Information”, 323, 363**

**Omnibus Rule, 582**

**onboarding**

- orientation, 267
- payroll
  - Form I-9, 265
  - Form W-4, 265–266
- user provisioning, 266

**online privacy, 10**

**open security posture, 386**

**operational management, business continuity, 486**

**operational risk, 525**

**operationalizing, threat intelligence, 336–338, 339**

**OpEx (operational expenditures)**

- analysis and adjustment, 137
- cloud computing, 137
- cloud/cloud computing, 136

**opportunistic, 88**

**oral law, 6**

**organization. *See also* business; financial institution; healthcare sector; small business**

- cyber range, 529
- resilient, 476–477

**organizational information, 221–222**

**organizational requirements, HIPAA, 578–579**

**orientation, employee, 267**

**original classification, 230**

**OTP (one-time passcode), 390–391**

**out-of-band authentication, 391**

**out-of-wallet challenge questions, 389–390**

**output validation, 451–452**

**outsourcing, 18**

financial institution, 530

regulatory compliance, 148–150

**oversight, 189**

GLBA (Gramm-Leach Bliley Act), 518–519

service provider, 530–531

**oversubscription, 150–151**

**OWASP (Open Worldwide Application Security Project), 449, 462**

Top 10, 449

Top 10 Risks for LLM, 674

backdoor attack, 682–683

excessive agency, 681

insecure output handling, 678

insecure plugin design, 680–681

model denial of service, 678–679

model inversion and extraction, 682

model theft, 682

overreliance, 681

prompt injection attacks, 674–677

sensitive information disclosure, 680

supply chain vulnerabilities, 679–680

training data poisoning, 678

ZAP (Zed Attack Proxy), 449

**ownership**

asset, 222–223

authentication by, 390–391

## P

**P2PE (PCI Point-to-Point Encryption) assessor, 618**

**PaaS (platform as a service), 140**

**packet filter, 404–405**

**PAM (privileged access management), 159**

**PAN (primary account number), 602**

**passive voice, 55**

**password**

cognitive, 389–390

policy, 15–16

strength, 389

temporary, 389

**passwordless authentication, 413–415, 423**

**PAT (port address translation), 405**

**patching, 446**

**Paulison, David, 503**

**payroll**

Form I-9, 265

Form W-4, 265–266

**PCI DSS (Payment Card Industry Data Security Standard), 22, 149, 601**

account data, 602

business-as-usual approach, 605–606

cardholder data environment, 602, 604

compliance, 616

assessment, 617

report, 619

validation, 616–617

core principles, 604–605

CPSA (Card Production Security Assessor), 618

Luhn algorithm, 603

P2PE (PCI Point-to-Point Encryption) assessor, 618

PAN (primary account number), 602

penalties for noncompliance, 621

PFI (PCI Forensic Investigator), 618

QPA (Qualified Pin Assessor), 618

QSA (Qualified Security Assessor), 602, 618

regulatory requirements, 194

requirements, 606

build and maintain a secure network and systems, 607

DESV (Designated Entities Supplemental Validation), 615

- implement strong access control measures, 610–612
- maintain a cybersecurity policy, 614–615
- maintain a vulnerability management program, 609–610
- protect cardholder data, 608
- regularly monitor and test networks, 613–614
- SAQ (Self-Assessment Questionnaire), 619–620
- Secure Software Assessor, 618
- SLC (Secure Software Lifecycle) Assessor, 618 version 4.0, 605–606
- PDCA (Plan-Do-Check-Act) model, 99**
- PDM (Cisco Product Development Methodology), 344**
- perimeter security, 12, 294**
- permissions, 393**
- personal information, 26**
- personnel screening policy, 264**
- PHI (personal healthcare information)**
  - breach, definition, 585
  - notice of security breach, 362–363
- phishing, 539, 567**
- PHR (personal health record), 362**
- physical destruction, 305**
- physical safeguards, HIPAA, 571**
  - device and media controls, 573–574
  - facility access controls, 572
  - workstation security, 573
  - workstation use, 572
- physical security, 12. *See also* fire; power**
  - authorizing entry, 295
  - background checks, 295–296
  - on the cloud, 292–293
  - CPTED (Crime Prevention Through Environmental Design), 294
  - ensuring clear desks and clear screens, 298–299
  - layered defense model, 292
  - location-based threats, 293
  - perimeter, 294
  - small business, 307

- working in secure areas, 297–298
- workspaces, 296

## **PII (personally identifiable information)**

- breach, 323
- DLP (data loss prevention), 242–255

## **PIPEDA (Personal Information Protection and Electronic Documents Act), 24, 25, 641–643, 644–645**

## **PKI (public key infrastructure), 109, 456, 463. *See also* key**

## **PLAIN (Plain Language Action and Information Network), Federal Plain Language Guidelines, 53–54**

## **plain language, 46, 51–52**

- active voice, 55
- Buffett on, 52
- Clarity Index, 55–56
- converting passive voice to active, 55
- passive voice, 55
- in the U.S. government, 52–53

## **plan/planning, 482–483. *See also* business continuity**

- business continuity, 504–505
- contingency, 485, 568–570
- continuity, 479
- disaster response, 488–489
  - command and control centers, 489
  - communication, 490
  - organizational structure, 489
  - relocation strategies, 490–492
- incident response, 330–331
- operational contingency, 495
- policy, 29
- recovery, 485
- response, 485

## **playbook, incident response, 335**

## **plugin, LLM, 680–681**

## **policy/ies, 5**

- access control authorization, 395
- administrative and privileged account, 419

- administrative notations, 66
- adoption, 32
- application development, 453
- audience, 56
- authentication, 398–399
- authorization, 189, 393–394
- border device, 407–409
- business continuity management, 487
- business continuity plan, 485
- business continuity testing and maintenance, 502
- CISO, 185
- clear desk and clear screen, 298–299
- cloud governance, 145–146
- consolidated, 57
- cybersecurity, 6, 10, 177
  - audit, 187
  - authorization, 183
  - change drivers, 190
  - client synopsis, 181–182
  - evaluation, 187
  - incident response program, 332
  - risk assessment, 206
  - risk management, 202
  - risk response, 200
  - training, 277
  - user-level, 180
  - vendor, 180
  - vulnerability disclosure, 180
- Cybersecurity Steering Committee, 186
- data breach reporting and notification, 366
- data center and communications facilities
  - environmental safeguards, 302–303
- development
  - authorization, 30
  - planning, 29
  - research, 29
  - vetting, 30
  - writing, 30
- disaster recovery plan, 499
- electronic monitoring, 267
- emergency preparedness, 478
- emergency response plan, 492
- employee agreement, 271
- employee termination, 269
- enforcement clause, 65
- evidence handling and use, 359
- exceptions, 64, 65
- exemption, 61, 64–65, 69
- firewall, 403
- global, 28
- goals and objectives, 62–63
- guiding principles, 8
- heading, 61–62
- hierarchy, 47, 182
  - baselines, 48–49
  - guidelines, 49
  - plans and programs, 50
  - procedures, 49–50
  - standards, 47–48
- IAM, risks, 155–156
- incident definition, 324
- incident response authority, 349
- information classification, 232, 236
- information ownership, 222–223, 224
- information security, 6
- information security incident classification, 329–330
- introduction, 59–61
- inventory of information system assets, 241
- job recruitment, 260
- key management, 459
- life cycle, 28–29
- mobile device and media security, 307
- monitoring, 32
- monitoring system access and use, 420–421
- network segmentation, 402
- operational contingency plan, 496–497
- oral law, 6

- oversight, 189
- password, 15–16
- personnel screening, 264
- physical entry controls, 296
- physical security perimeter, 294
- plain language, 51–52
  - Clarity Index, 55–56
  - converting passive voice to active, 55
  - federal guidelines, 53–54
  - in the U.S. government, 52–53
- power consumption, 301
- procedures, 49–50
- procurement, 16
- publication, 30
  - communication, 30–31
  - dissemination, 31
  - education, 31
- remote access security, 410
- retiring, 33
- review, 33
- sanction, 563–564
- SDLC (systems development life cycle), 444
- secure disposal, 306
- singular, 57
- statement, 63–64
- successful, characteristics
  - adaptable, 16–17
  - attainable, 16
  - endorsement, 14–15
  - enforceable, 17–18
  - inclusive, 18–19
  - realistic, 15–16
  - relevant, 15
- system implementation and update, 447
- template, 57
- terms and definitions, 67
- Torah, 7, 34
- user access control, 417
- user provisioning, 266
- version control, 58–59
- violation, 17–18, 61
- working in secure areas, 297–298
- workspace classification, 296
- writing, 15
- port, 403**
- portal, remote access, 409–410**
- positive corporate culture, 10**
- post-mortem, incident response, 335**
- posture, security, 386, 422**
  - default deny, 386
  - open, 386
- power**
  - blackout, 300
  - brownout, 300
  - consumption policy, 301
  - protection, 299–300
  - spike, 300
  - surge, 300
- PQC (post-quantum cryptography), 460**
  - approaches, 460
  - challenges and progress, 461
- preparation phase, incident response, 333**
- Presidential Policy Directive 7: Protecting Critical Infrastructure, 3**
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, 3**
- pretexting, 517–518**
- preventive controls, 481**
- principle of least privilege, 387**
- privacy, 116. See also NIST (National Institute of Standards and Technology), Privacy Framework**
  - AI and, 636
  - in the digital age, 635
  - employee right to, 262, 267, 420
  - online, 10
  - student record, 26
- Privacy Act of 1988 (Australia), 24–25**
- privacy officer, 186**

**Privacy Rule, GLBA (Gramm-Leach Bliley Act), 517**

**private sector data classification, 230–231**  
**procedures, 49–50**

HIPAA Security Rule, 580

operational contingency, 495–496

recovery, 497–498

**procurement, policy, 16**

**product security, vulnerabilities, 342–343.**  
*See also* supply chain security

**program, 50**

incident response, 330, 332, 537–538

information security, 520–521, 531–532

security awareness and training, 272,  
 566–567

testing, 570

vulnerability management, 609–610

**protected data, 230–231**

**protocol, 403**

**provider. *See* service provider**

**PSIRT (product security incident response team), 341**

SBOM (software bill of materials), 345

vulnerability

chaining, 343

product security, 342–343

theoretical, 343–344

**public information, 231**

**public key, 456**

**public relations, data breach, 367**

**public trust, honoring, 10**

**publication/s**

Federal Register, 519

NIST (National Institute of Standards and  
 Technology), 95

policy, 30

communication, 30–31

dissemination, 31

education, 31

**purple team, 407**

## Q

**QPA (Qualified Pin Assessor), 618**

**QSA (Qualified Security Assessor), 602, 618**

**quantum computing, 460**

**qubit, 460**

## R

**RA (registration authority), 456**

**RBAC (role-based access control), 155–156,  
 394–395, 396–397**

**RC (release candidate), 445**

**realistic policy, 15–16**

**reciprocal site, 492**

**reclassification, 232–233, 245**

**recovery plan, 485**

**recruitment, employee, 259, 263. *See also***  
**screening prospective employees**

candidate application data, 260

interview, 260

job postings, 259

**red team, 407**

**reflected DDoS attack, 91**

**regulation/regulatory requirements, 19–20.**

***See also* financial information; healthcare sector; HIPAA (Health Insurance Portability and Accountability Act of 1996); Interagency Guidelines for Safeguarding Member Information**

business continuity management, 477–478

CCPA (California Consumer Privacy Act), 22,  
 640–641

COPPA (Children’s Online Privacy Protection  
 Act), 22

Cyber Essentials, 24

cybersecurity, 179

DFARS (Defense Federal Acquisition  
 Regulation Supplement), 22–23

encryption, 455

environmental sustainability, 308

FedRAMP (Federal Risk and Authorization



Management Program), 23

financial institution. *See* financial institution, regulatory compliance

fintech, 541

FISMA (Federal Information Security Management Act), 21

GDPR (General Data Protection Regulation), 23, 194

GLBA (Gramm-Leach Bliley Act), 193

HIPAA (Health Insurance Portability and Accountability Act of 1996), 194

New York Department of Financial Services, 27, 194, 533–535

NIS (Network and Information Systems) Directive, 23, 194

PCI DSS (Payment Card Industry Data Security Standard), 22, 194

PIPEDA (Personal Information Protection and Electronic Documents Act), 24

Privacy Act of 1988 (Australia), 24–25

Protection of Personal Information Act (South Africa, 2013), 25

responsibilities and costs, transferring to the cloud, 148–150

SOX (Sarbanes-Oxley) Act, 22

Supplement to the Authentication in an Internet Banking Environment Guidance, 538–539

**relevance, policy, 15**

**relocation strategies, 490–492**

**remote access, 409**

- mutual authentication, 410
- policy, 410
- portal, 409–410
- VPN (virtual private network), 409

**remote worker security, 411–413**

**removal, company property, 240–241**

**report**

- audit, 187
- data breach, 306
- information security and GLBA compliance, 532–533

- PCI DSS compliance, 619
- user access, 420
- VEX (Vulnerability Exploitability eXchange), 345

**reputational risk, 524**

**research, policy, 29**

**residual risk, 203, 480, 524**

**resilient organization, 476–477, 504**

**response plan, 485**

**retention, evidence, 359**

**retiring policies, 33**

**review, policy, 33**

**RFC 9116, 180–181**

**right**

- to be forgotten, 639
- to privacy, 262

**risk/s, 198, 207–208**

- acceptance, 199
- analysis, 563
- appetite, 201–202
- assessment, 202–203, 321
  - business continuity, 480–481
- FAIR (Factor Analysis of Information Risk), 205
- NIST RMF, 205
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 204–205
- avoidance, 199–200
- business categories, 204
- cloud computing
  - advanced persistent threats and sophisticated malware, 165–166
  - data breaches and loss, 154–155
- IAM (identity and access management), 155–156, 160–161
- insider threats, 164–165
- lack of visibility and control over data, 163
- misconfiguration and inadequate change control, 161–162

compliance, 525  
 cybersecurity, 198  
 first-party, 200  
 inherent, 202, 524  
 management, 199, 202, 479, 563  
 matrix, 659  
 mitigation, 199  
 operational, 525  
 reduction, 199  
 reputational, 524  
 residual, 203, 480, 524  
 response policy, 200  
 strategic, 524  
 third-party, 200  
 tolerance, 198, 201–202  
 transactional, 525  
 transfer, 199

**RPO (recovery point objective), 482–483**

**RTO (recovery time objective), 482–483**

**rule-based access control, 395**

**runtime defense, 452**

## S

**SaaS (software as a service), 139**

**Safe Harbor Provision, 584–585**

**safeguards, 543. See also administrative safeguards, HIPAA; physical safeguards, HIPAA; technical safeguards, HIPAA**

**Safeguards Rule, GLBA (Gramm-Leach Bliley Act), 517**

**sag, 300**

**SAMM (Software Assurance Maturity Model), 448, 462**

**sanction policy, 563–564**

**SBOM (software bill of materials), 345**

enhancing supply chain security, 437–438  
 enhancing vulnerability management, 438  
 promoting transparency and trust, 438

**SC (security category), 227, 228**

**SCAF (Common Security Advisory Framework), 345**

**scalability, 134**

**scope**

CSF (NIST Cybersecurity Framework), 112  
 GDPR (General Data Protection Regulation), 639–640

**scoring, CVSS (Common Vulnerability Scoring System), 86**

**screening prospective employees, 261–263**

**SDL (secure development life cycle), 344**

**SDLC (systems development life cycle), 434, 441–442, 462. See also software**

commercially available and open-source software, 445  
 development/acquisition phase, 442  
 disposal phase, 443  
 implementation/assessment phase, 443  
 initiation phase, 442  
 operations/maintenance phase, 443  
 policy, 444

**SDN (software-defined networking), 12**

**SecretCorp, 115–116**

**secure disposal policy, 306**

**Securities and Exchange Commission, *A Plain English Handbook*, 52**

**security**

application, 13  
 awareness, 272, 276  
 breach. *See* breach  
 business-as-usual approach, 605–606  
 clearance investigation, 264–265, 278  
 control, 99  
 domains, 81  
 education, 276–277  
 event, 323  
 host, 12  
 incident, 322–323. *See also* incident/incident response  
 definition, 323–324  
 versus event, 323

- information, 6. *See also* CIA triad
  - “Five A’s”, 92–93
  - framework, 80–81. *See also* framework
  - governance, 105–106
  - honoring the public trust, 10
- label, 393
- layered, 403
- model
  - Bell-LaPadula, 225
  - Biba, 225
- network, 12
- patch, 446
- perimeter, 12
- physical, 12. *See also* physical security
  - ISO/IEC 27002: Code of Practice for Information Security Controls, 291
  - NIST documents, 291–292
- posture, 386, 422
  - default deny, 386
  - open, 386
- remote worker, 411–413
- supply chain. *See* supply chain security
- system requirements, 441
- through obscurity, 245
- token, 414
- TPS (third-party software), 344
- training, 272, 276, 566–567
- workforce, 564–565
- workstation, 573
- “A Security-Oriented Approach to IP Addressing”, 405**
- security.txt, 180–181**
- SEI (Software Engineering Institute), CERT Division, 346**
- sensitive area, 612**
- separation of duties, 387–388, 418**
- service models, cloud computing, 139–140**
- service provider, 602. *See also* provider; vendor**
- cloud, 151–152**
  - dependencies, 499
  - leveraging for compliance needs, 148–150
  - oversight, 530–531
  - technology, 531
  - third-party, 530
- services, essential, 482**
- session management, 452**
- SETA (Security, Education, Training, and Awareness) model, 256–257, 273**
- severity level, incident, 326–328**
- shadow IT, 146–147**
- Shor’s algorithm, 460**
- shoulder surfing, 298**
- SIEM, 159**
- SIGMA, 356**
  - for incident response, 356
  - in threat hunting, 356–357
- signature, 392**
- silo-based approach, cybersecurity, 177, 178**
- simple step procedures, 49**
- singular policy, 57, 61–62**
- skimming, 612**
- SLA (service-level agreement), 89**
- small business**
  - data classification and handling, 241–242
  - disaster response plan, 503
  - human resources security practices, 277
  - IT personnel, 421
  - organizational roles and responsibilities, 201
  - physical security, 307
- smartcard, 391**
- SMC (secure multiparty computation), 637**
- social engineering, 517–518**
- social media, screening prospective employees, 262–263**
- society-wide approach to AI governance, 667**
- software. *See also* malware**

- assets, 237
- assurance maturity model, 448
- bill of materials, 345
- bugs, 88–89
- code, 448
- commercial off-the-shelf, 445
- description, 239
- development. *See also* SDLC (systems development life cycle)
  - output validation, 451–452
  - secure, 444–445
- open-source, 445
- Orion, 436
- releases, 445
- as a service, 139
- testing, 446
- third-party, security, 344
- updates, 446
- SolarWinds attack, 436**
- something you know, 389**
- SOP (standard operating procedure), 331**
- sophisticated malware, 165–166**
- South Africa, Protection of Personal Information Act (2013), 25**
- SOX (Sarbanes-Oxley) Act, 22**
- SSAE 18 (Statement on Standards for Attestation Engagements No. 18), 149**
- SSDF (Secure Software Development Framework), 444–445**
- standard/s, 47–48, 81. *See also* framework**
  - cloud services, 142–146
  - cross-sector international, 478
  - handling, 233–235
  - HIPAA, 562
    - access control, 575–576
    - assigned security responsibility, 564
    - audit controls, 576–577
    - business associate contracts and other arrangements, 570–571, 578–579
    - contingency plans, 568–570
    - device and media controls, 573–574
    - documentation, 580–581
    - evaluation, 570
    - facility access controls, 572
    - implementation specifications, 561
    - information access management, 565–566
    - integrity controls, 577
    - person or entity authentication, 577
    - policies and procedures, 580
    - security awareness and training, 566–567
    - security incident procedures, 567–568
    - security management process, 563–564
    - transmission security, 577–578
    - workforce security, 564–565
    - workstation security, 573
    - workstation use, 572
- ISO 17789 Cloud Computing Reference Architecture, 151–152, 153
- ISO/IEC, 97–98
  - ISO/IEC 27001: Information Security Management Systems—Requirements, 98–99
  - ISO/IEC 27002: Code of Practice for Information Security Controls, 99
  - ISO/IEC 27003: Information Security Management System Implementation Guidance, 99–100
  - ISO/IEC 27004: Information Security Management System—Measurement, 100
  - ISO/IEC 27005: Information Security Risk Management, 100–101
  - ISO/IEC 27006: Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, 101
  - ISO/IEC 27007: Guidelines for Information Security Management Systems Auditing, 102
  - ISO/IEC 27008: Guidelines for Auditors on Information Security Controls, 102–103
  - ISO/IEC 27009: Sector-Specific Application of ISO/IEC 27001—Requirements, 103

ISO/IEC 27010: Information Security Management for Inter-Sector and Inter-Organizational Communications, 103–104

ISO/IEC 27011: Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002, 104–105

ISO/IEC 27013: Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000–1, 105

ISO/IEC 27014: Governance of Information Security, 105–106

ISO/IEC 27017: Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services, 106–107

ISO/IEC 27018: Code of Practice for Protection of PII in Public Clouds Acting as PII Processors, 107

ISO/IEC 27019: Information Security for Process Control in the Energy Industry, 107–108

ISO/IEC 27031: Guidelines for Information and Communication Technology Readiness for Business Continuity, 108–109

ISO/IEC 27099: Public Key Infrastructure—Practices and Policy Framework, 109–110

SSAE 18 (Statement on Standards for Attestation Engagements No. 18), 149

**state law, breach notification, 364–365**

**status justification, 439**

**steering committee, 207**

**storing evidence, 359**

**strategic alignment, 178–179**

**strategic risk, 524**

**structured review, 500**

**student record, privacy, 26**

**subcontractor, liability, 583**

**subject, access control, 385**

**supply chain security**

AI (artificial intelligence), 672–673

AI BOMs (artificial intelligence bill of materials), 440–441

SBOM (software bill of materials), 437–438

enhancing vulnerability management, 438

promoting transparency and trust, 438

SolarWinds attack, 436

strategies for enhancing, 437

system security requirements, 441

threats, 436

VEX (Vulnerability Exploitability eXchange), 439

**sustainability, environmental, 308–309**

**symmetric key, 456**

**system. See also SDLC (systems development life cycle)**

implementation and update policy, 447

information, 222

information classification, 224–225

integrity, 88

security requirements, 441

## T

**table, version control, 59**

**tabletop exercises, 336, 500**

**tactical activities, business continuity management, 486–487**

**tailgating, 295**

**TC-NAC (threat-centric network access control), 386–387**

**team**

blue, 407

business continuity, 486

computer emergency response, 346

computer security incident response, 339–341

incident response, 187, 347–348

purple, 407

red, 407

US Computer Emergency Readiness, 322

**technical safeguards, HIPAA, 574–575**

access control, 575–576

audit controls, 576–577

- integrity controls, 577
- person or entity authentication, 577
- transmission security, 577–578

#### **template**

- AI RMF implementation, 658–661
- policy, 57

#### **temporary data files, 303**

#### **termination, employee, 268**

#### **testing**

- business continuity plan, 500–501
- full-scale, 501
- information security, 529
- network, 613–614
- program, 570
- software, 446

#### **theft, 306–307**

- identity, 537, 538
- model, 682

#### **theoretical vulnerability, 343–344**

#### **third-party risk, 200**

#### **threat/s, 202**

- advanced persistent, 165–166
- assessment, 524
- to availability, 90
- business continuity, 479–480
- centric network access control, 386–387
- hunting, 351
  - best practices, 354
  - MITRE ATT&CK framework, 352–353
  - objectives, 351
  - phases, 351–352, 354–355
  - proactive, 355
  - SIGMA, 356–357
- insider, 164–165, 268, 274–276
- intelligence
  - operationalizing, 336–338, 339
  - using AI, 338–339
- location-based, 293
- quantum computers, 460

- source, 202
- supply chain, 436

#### **tools**

- asset management, 239–240
- CSPM (cloud security posture management), 163
- Cybersecurity Assessment, 527–528
- DLP (data loss prevention), 242–255
- SIEM, 159
- What-If, 665
- XAI (explainable AI), 664–665
- ZAP (Zed Attack Proxy), 449

#### **Torah, 7, 34**

#### **training. *See also* NICE (National Initiative for Cybersecurity Education)**

- data poisoning, 678
- HIPAA, 584
- incident response, 348–349
- information security, 528–529
- LLM (large language model), 653–654
- security, 272, 276, 566–567

#### **transactional risk, 525**

#### **true positive, 325, 406**

#### **Trump, Donald, Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 4**

#### **trust boundary, 677**

#### **trusted network, 400**

#### **TSP (technology service provider), 531**

#### **TTPs (tactics, techniques, and procedures), 351**

## **U**

#### **UCaaS (unified communications as a service), 412**

#### **Uniform Rating System for Information Technology, 536**

#### **United Kingdom**

- Cyber Essentials, 24
- Data Protection Act 2018, 24, 643–644
- ICO (Information Commissioner's Office), 24

**United States**

Americans with Disabilities Act, 263

Bank Holding Company Act of 1956, 515–516

Banking Act of 1933, 515–516

BSCA (Bank Service Company Act (United States), 531

COPPA (Children’s Online Privacy Protection Act), 22

Data Protection Act 2018, 24

DFARS (Defense Federal Acquisition Regulation Supplement), 22–23

EFTA (Electronic Fund Transfer Act), 600

FCBA (Fair Credit Billing Act), 600

FCC (Federal Communications Commission), 478

Federal Plain Language Guidelines, 53–54

FedRAMP (Federal Risk and Authorization Management Program), 23

FERPA (Family Educational Rights and Privacy Act of 1974), 26

fintech, regulation, 541

FIPS-199 (Federal Information Processing Standard 199), 226–228

FISMA (Federal Information Security Management Act), 21

FOIA (Freedom of Information Act), 226

Glass-Steagall Act, 515–516

national security information, 228–230

PCI DSS (Payment Card Industry Data Security Standard), 22

plain language movement, 52–53

Plain Writing Act of 2010, 52

SOX (Sarbanes-Oxley) Act, 22

**untrusted network, 400**

**updates, software, 446**

**uptime, 89**

**US Army Clarity Index, 55–56**

**US Department of Health and Human Services, 556, 557, 583, 584**

**US Department of Homeland Security, CISA (Cybersecurity & Infrastructure Security**

**Agency)xr. See CISA (Cybersecurity & Infrastructure Security Agency)**

**US Veterans Administration, notice of security breach, 363–364**

**US-CERT (U.S. Computer Emergency Readiness Team), 322, 346**

**user access control, 416–417**

administrative accounts, 418–419

monitoring, 419–420

policy, 417

privileged account, 419

**user provisioning, 266**

**user-level cybersecurity policies, 180**

**V**

**validation, 499**

**value, asset, 11**

**vendor**

approved scanning, 601

cybersecurity policies, 180

TPS security, 344

**version control, policy, 58–59**

**vetting, policy, 30**

**VEX (Vulnerability Exploitability eXchange), 345, 439**

**violation, policy, 61**

**VPN (virtual private network), 409, 412**

**vulnerability/ies. See also CVSS (Common Vulnerability Scoring System); VEX (Vulnerability Exploitability eXchange)**

chaining, 343

CVE-2024–20305, 85

CVE-2024–23222, 84–85

disclosure policies, 180

NIST definitions, 203

patching, 446

product security, 342–343

security.txt, 180–181

status justification, 439

supply chain, 679–680  
theoretical, 343–344

## W

---

**WAN (wide area network), software-defined, 12**

**warm site, 491**

**web application**

injection, 450

input validation, 451

**web cache, 303**

**WebAuthn, 415**

**What-If Tool, 665**

**white box test, 529–530**

**Wofford, Cynthia, 612**

**workforce security, 564–565**

**workspace, physical security, 296**

**write blocker, 328**

**writing, policy, 15, 30**

audience, 56

plain language, 51–52

active voice, 55

Clarity Index, 55–56

federal guidelines, 53–54

passive voice, 55

in the U.S. government, 52–53

## X-Y-Z

---

**XAI (explainable AI), 663–665**

**XDR (extended defense and response), 159–160**

**Yahoo! password compromise, 390**

**ZAP (Zed Attack Proxy), 449**

**zero trust, 4, 12, 396–397, 412**