

- Access control. *See also* Authentication; Authorization; Identification
- administrative access, 80
 - broken, 110, 111
 - data access, 165, 166
 - and firewalls, 63, 64
 - inactive user accounts, 128
 - inventory of assets and list of personnel, 160
 - Least Privileged Access Control, 49, 105, 124
 - logical access control, 48, 49
 - measures, implementing. *See* Implement strong access control measures objective methodology, 67
 - physical access control, 40, 41, 48, 49, 131–139
 - remote access control, 53, 125, 147, 162, 163
 - terminated users, 127
 - unique ID, 124–131
- Account number
- defined, 12
 - Primary Account Number (PAN), 12, 83–85, 87, 97, 105
- Acquirer, defined, 14
- Administrative access, 80. *See also* Access control
- Adware, 101
- American Express, 7, 15, 16, 86
- Annual review
- information security policy, 158
 - testing. *See* Testing
- Antivirus software, 99–102, 142
- Approved Scanning Vendor, 16
- Assessment tools, 175, 176
- Audit logs, 101, 144, 147. *See also* Log management
- Audit trails, 29, 82, 101, 135, 136, 141, 142–148. *See also* Log management
- Authentication
- and access control, 48, 49, 126–131, 159
 - and audit trails, 143, 144
 - broken, 111
 - electronic, 49, 50
 - and encryption, 52
 - multi-factor, 50
 - non-consumer users and administrators, 126–131
 - OWASP policy guidelines, 111–113
 - and remote access control, 53, 125, 147
 - sensitive authentication data, 84
 - single-factor, 50
- Authorization, 48, 49, 52, 53. *See also* Access control
- Automatic disconnect, 161, 162
- Availability, 25, 26, 79
- Back-out procedures, 108, 109
- Back-up media, audit trail files, 146
- Backup media, storage of, 40, 41, 136
- Balanced Scorecard, 39
- Baselines, 30, 31, 179
- Biometrics, 50, 124, 125

- Brute force attacks, 129, 130, 143
- Buffer overflows, 110, 114, 115
- Build and maintain secure network
 - objective
 - control objectives, 6, 7
 - overview, 61, 63
 - requirement 1 (firewall configuration to protect cardholder data), 63–75
 - requirement 2 (vendor supplied defaults), 76–81
 - requirement A.1 (hosting providers protect cardholder data environment), 81, 82
- Business need to know. *See* Least Privileged Access Control
- Capability Maturity Model Integration (CMMI), 33
- Card brand security programs, 8
- Card validation code or value, 12, 13, 85, 86
- Cardholder, defined, 12
- Cardholder data
 - defined, 12
 - firewalls, use of to protect. *See* Firewalls
 - importance of protecting, 5
 - physical access control, 131–139
 - protecting. *See* Protect cardholder data objective
- Cardholder data environment, 14, 48, 49, 80–82
- Cardholder Information Security Program (CISP), 7
- Carnegie Mellon University CERT Information Center, 57, 58, 120
- Center for Internet Security (CIS), 78
- CERT (Computer Emergency Response Team), 57, 58, 120
- Change control, 107–110, 147
- CIA Triangle, 25, 26, 79
- Ciphertext, 50, 52
- Classification systems for information, 23, 24, 26
- Clocks, synchronizing, 144, 145
- CMMI, 33
- COBIT, 32
- Column level encryption, 88, 89
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 32
- Common Vulnerability Scoring System (CVSS-SIG), 39
- Communication
 - network models and data communications, 42, 43
 - roles and responsibilities of employees and contractors, 163
 - secure, 53
 - security awareness, 38
- Compensating controls, 93–96
- Compliance
 - life cycle, 177, 178
 - responsibility for, 182–184
 - risk, 8, 2
 - strategic plan for, 180, 181
 - team, 177, 178
- Computer forensics, 58–60
- Computer Security Incident Response Team (CSIRT), 58
- Confidentiality, 25–26, 52
- Configuration
 - changes, 104, 107–110
 - routers, securing and synchronizing configuration files, 73
 - servers, 119–121
 - standards. *See* Configuration standards
- Configuration standards
 - configuration changes, 104, 107–110
 - firewalls, 64–75
 - routers, 70
 - for system components, 78
- Connected entities, 171, 172
- Consumer confidence, 6
- Control objectives
 - access control measures, implementing. *See* Implement strong access control measures objective
 - cardholder data, protecting. *See* Protect cardholder data objective

- categories of, 6, 7, 61
- information security policy, maintaining. *See* Maintain information security policy
- objective
- monitoring and testing networks. *See* Regularly monitor and test networks objective
- secure network, building and maintaining. *See* Build and maintain secure network objective
- vulnerability management program, maintaining. *See* Maintain vulnerability management program objective
- Control Objectives for Information and related Technology (COBIT), 32
- Controls, types of, 31, 34
- Cookies, 110, 111, 114
- COSO framework, 32
- Cost-benefit analysis, 21–23, 27
- Costs of data breaches, 9–11
- Critical files, 153, 154
- Cross-site scripting (XSS) attacks, 114
- Custom applications, 106, 110, 121, 122, 148, 153, 154
- CVSS-SIG, 39
- Data classification, 23, 24, 26
- Data communications, 42, 43
- Data storage, 83–90, 117
- Decryption, 51, 87, 88, 112
- Defaults, vendor-installed, 76–81
- Defense-in-depth security model, 28, 29, 57, 132
- Demilitarized zone (DMZ), 44, 71, 72, 74, 75
- Denial of service attacks, 48, 118, 119
- Destruction, 41, 94, 139
- Digital forensics, 58–60
- Discover, 7, 86
- Distribution of media and keys, 41, 93, 136
- DMZ. *See* Demilitarized zone (DMZ)
- Domain Name System (DNS), 44, 78
- Due diligence, 172, 182
- Dynamic packet filtering, 72, 90
- E-commerce, 5, 6
- Electronic Authentication Guideline*, 49, 50
- Employees
 - antivirus software for, 99–101
 - background checks, 167
 - critical employee-facing technologies, usage policies, 159–163
 - firewalls, 74
 - security awareness program, 166, 167
 - training, 37, 38
- Encryption, 50–53, 77, 78, 80, 83, 84, 86–97, 117, 126
- Error handling, 116, 117
- Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, 55, 56
- Executive-level support, 177
- Facility entry controls, 132–135
- Federal Information Security Management Act (FISMA), 33
- File infectors, 100
- File integrity monitoring, 153
- File level encryption, 88, 89. *See also* Encryption
- File Transfer Protocol (FTP), 46, 68
- Financial risk, 8, 9
- Firewalls, 43, 44, 63–75, 121, 122
- Forensics, 58–60, 82
- FTP (File Transfer Protocol), 46, 68
- Full disk encryption, 88, 89
- General pack radio service (GPRS), 97
- Global system for mobile communications (GSM), 97
- Guide to Computer Security Log Management*, 45, 46, 142
- Guide to Integrating Forensic Techniques into Incident Response*, 58
- Guide to Intrusion Detection and Prevention Systems*, 46

- Guideline on Network Security*
Testing, 150
 Guidelines, 30, 31
- Hash algorithm, 51, 52, 117
 Historical background, 7, 8
 Hosting provider, 13, 80–82
 Hypertext Transfer Protocol (HTTP), 46, 53, 54, 66, 68, 70
 Hypertext Transfer Protocol Secure (HTTPS), 53, 54
- Identification. *See also* Access control
 IP address as, 118
 logical access control, 48, 49
 Personal Identification Number (PIN), 13, 85–87
 remote access control, 53
 unique ID and access control, 124–131
 visitor identification requirements, 40, 41, 134–136
- Implement strong access control
 measures objective
 control objectives, 6, 7
 overview, 123
 requirement 7 (restrict access to cardholder data by business need to know), 124
 requirement 8 (assign unique ID to each person with computer access), 124–131
 requirement 9 (restrict physical access to cardholder data), 131–139
- Incident response, 57, 58, 164, 165, 168–171
- Information classification system, 23, 24, 26
- Information risk management, 20–23
- Information security, generally
 security control frameworks, 31–34
 terminology, 29–31
- Information Shield, 29
- Injection flaws, 115
- Integrity, 25, 26, 52
- International Standards Organization (ISO), 32
- Internet firewalls. *See* Firewalls
- Internet Protocol Security (IPSEC), 46, 55, 96, 97, 125
- Intranet firewalls. *See* Firewalls
- Intrusion detection and prevention (IDS/IPS), 46–48, 147, 152, 153, 170
- Inventory controls, 40, 41
- IP masquerading, 75
- ISO. *See* International Standards Organization (ISO)
- Issuer, defined, 14
- IT Infrastructure Library (ITIL), 32
- Japan Credit Bureau (JCB), 7, 86
- Keys and key management, 50–52, 88, 90–96, 117
- Least Privileged Access Control, 49, 105, 124, 145, 146
- Local area network (LAN), 56, 97, 146
- Log management, 44–46, 82, 101, 142–148. *See also* Audit trails
- Logical access control, 48, 49
- Magnetic stripe data (track data), 13, 85
- Maintain information security policy
 objective
 control objectives, 6, 7
 overview, 155
 requirement 12 (maintain policy that addresses information security), 156–172
- Maintain vulnerability management
 program objective
 control objectives, 6, 7
 overview, 99
 requirement 5 (antivirus software), 99–101
 requirement 6 (develop and maintain secure systems and applications), 101–122
- Malware, 46–48, 57, 100
- Management/administrative controls, 31, 34

- Management responsibilities, 163, 164
- MasterCard, 7, 15–17, 86
- Media access code (MAC), 97
- Media storage, 136–139
- Merchant bank, 11
- Merchants, 14–16
- Metrics, 39, 179
- Monitoring, 40, 41, 44–46, 164–166
- Monitoring and testing networks.
 - See Regularly monitor and test networks objective
- National Institute of Standards and Technology (NIST), 78
 - Special Publication 800-42, *Guideline on Network Security Testing*, 150
 - Special Publication 800-48 Revision 1 (draft), *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, 56, 57
 - Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, 39
 - Special Publication 800-63, *Electronic Authentication Guideline*, 49, 50
 - Special Publication 800-80 (draft), 39
 - Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, 58
 - Special Publication 800-92, *Guide to Computer Security Log Management*, 45, 46, 142
 - Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems*, 46
 - Special Publication 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, 55, 56
- Need to know. See Least Privileged Access Control
- Network access points, 40, 41
- Network address translation (NAT), 75
- Network models, 42, 43
- Network scanning, 149, 150
- Networks, 70, 96, 97. See also Build and maintain secure network objective;
Wireless networks
- Nonrepudiation, 52
- Open System Interconnection Model (OSI model), 42, 43, 54
- Open Web Application Security Project (OWASP), 99, 109–122
- Operational/physical controls, 31, 34
- Operational risk, 8, 9
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 33
- Paper media, storage of, 41
- Passwords, 76–81, 106, 112, 117, 125–131
- Payment Card Industry Data Security Standards (PCI DSS)
 - assessment tools, 175, 176
 - background, 7, 8
 - compliance, importance of, 5, 6
 - control objectives, overview, 6, 7.
 - See also Control objectives and e-commerce, 5, 6
 - need for, 8
 - and risk management, 8–10
 - strategy and program development, 177, 178
 - terminology, 11–14
- Payment Card Industry Security Standards Council
 - approved vendors, 182
 - control objectives, categories of, 6, 7, 61
 - formation of, 8
 - terminology, 11–14
- Payment card transactions, steps, 11, 15–17
- Payment cardholder environment, 13
- Penetration testing, 150–152
- Perimeter security, 28, 29, 43, 44, 68, 73, 83. See also Firewalls
- Personal Identification Number (PIN), 13, 85–87

- Physical access control, 48, 49, 131–139
- Physical security, 40, 41
- PIN (Personal Identification Number), 13, 85–87
- PIN Verification Value (PVV), 13
- Policies, 29, 30. *See also* Maintain information security policy objective
- Ponemon Institute *2007 Annual Study: U. S. Cost of a Data Breach*, 10, 11
- Port address translation (PAT), 75
- POS (Point of Sale), 13
- Primary Account Number (PAN), 12, 83–85, 87, 97, 105
- Procedures, 30, 31, 158, 159
- Program management, 179–184
- Protect cardholder data objective
 - control objectives, overview, 6, 7
 - overview, 83
 - requirement 3 (protect stored cardholder data), 83–90
 - requirement 3.4, compensating controls for (PCI DSS Appendix B), 90–96
 - requirement 4 (encrypt transmission of cardholder data across open public networks), 96, 97
- Public networks, 96, 97
- PVV (PIN Verification Value), 13
- Quarterly network scan, 16
- RADIUS (Remote Authentication Dial-In User Service), 53, 125, 147
- Regularly monitor and test networks objective
 - control objectives, 6, 7
 - overview, 141
 - requirement 10 (track and monitor all access to network resources and cardholder data), 142–148
 - requirement 11 (regularly test security systems and processes), 148–154
- Remote access control, 53, 125, 147, 162, 163
- Remote Authentication Dial-In User Service (RADIUS), 53, 125, 147
- Reputation risk, 8, 9
- RFC 1918 address space, 75
- Risk
 - analysis, 26, 27
 - assessment, 21, 24–26, 157, 158
 - categories, 8, 9
 - management, 20–23, 26–28
- Role-Based Access Control, 49
- Routers, 68–70, 73
- SANS, 78, 120
- SDLC (system development life cycle), 35–37, 104, 105
- Secure network, building and maintaining. *See* Build and maintain secure network objective
- Secure Shell (SSH), 54, 66, 68, 70, 80
- Secure Sockets Layer/Transport Layer Security (SSL/TLS), 46, 54, 66, 68, 70, 80, 97, 125
- Security alerts, 154
- Security audit procedures, 176
- Security awareness, 37, 38
- Security breaches, 170. *See also* Incident response
- Security control frameworks, 31–34
- Security patches, 101, 102, 104, 115
- Security scanning procedures, 176
- Segregation of duties, 105
- Self-assessment tools, 175, 176
- Self-audit, 179, 180
- Sensitive authentication data, defined, 13
- Server Set Identifiers (SSIDs), 77
- Servers, 70–75, 78, 79, 119–121
- Service providers, 14, 16, 17, 167, 168, 171, 172
- Simple Network Management Protocol (SNMP), 76, 77
- Software
 - change detection, 147
 - configuration changes, 104, 107–110
 - file integrity monitoring, 153
 - patches, 101, 102, 115
 - testing, 148–154

- Software Development Life Cycle (SDLC), 35–37, 103, 104, 106, 107
- Spyware, 46, 100, 101
- SSH (Secure Shell), 54, 66, 68, 70, 80
- SSL/TLS (Secure Sockets Layer/Transport Layer Security), 54, 55, 66, 68, 70, 80, 97, 125
- Standards, 29–31
 - configuration standards. *See* Configuration standards
 - National Institute of Standards and Technology. *See* National Institute of Standards and Technology (NIST)
- Stateful inspection, 72
- Strategy, 20, 21, 23, 25, 180, 181
- Structured query language (SQL), 91, 110, 115
- SysAdmin Audit Network Security Network (SANS), 78, 120
- System configuration changes, 107–110
- System development life cycle (SDLC), 35–37, 104, 105
- System security parameters, 79
- TCP/IP model, 43, 53
- Technical/logical controls, 34
- Terminal access controller access control system (TACACS), 125
- Testing
 - access control, 110, 111
 - incident response plan, 169
 - and information risk management, 21
 - network connections and firewall configuration, 64
 - networks, 141. *See also* Regularly monitor and test networks
 - objective
 - operational functionality, 108
 - penetration testing, 150–152
 - regression testing, 107
 - security patches and system and software configuration changes, 104
 - security systems and processes, 148–154
 - and separation of duties, 105
 - test data, 105, 106
- Threats, 24–26, 157
- Tokens, 50, 87, 114, 125, 135
- Training, 8, 37, 38, 170, 171
- Transmission Control Protocol/Internet Protocol (TCP/IP) model, 43, 53
- Transport protocols, 46
- Trojan horses, 100
- 2007 Annual Study: U. S. Cost of a Data Breach*, 10, 11
- Unnecessary functionality, 79, 80
- Usage policies, 159–163
- User account administration, 165
- User names, 106, 125
- Vendors
 - activation of modem connections for, 162
 - default settings by, changing, 76–81
 - enabling accounts for, 128
 - Information Shield, 29
 - selecting, 182, 184
 - support/maintenance accounts, deletion or disablement of, 76
- Virtual Private Networks (VPNs), 54, 55, 66, 68, 70, 80, 97, 125
- Viruses, 99–102
- Visa, 7, 15–17, 86
- Visitor identification requirements, 40, 41, 134–136
- VPN (Virtual Private Network), 54, 55, 66, 68, 70, 80, 97, 125
- Vulnerability
 - alert services and updating standards, 102, 103
 - identifying, policy on, 157
 - management. *See* Maintain vulnerability management program
 - objective
 - risk analysis, 26
 - scan, 149, 151
 - threat distinguished, 24, 25

- Web applications, 110–122
- Web sites
 - OWASP, 110
 - PCI Council, 8
- WiFi protected access technology,
 - 77, 78, 97
- Wired equivalent privacy (WEP) keys,
 - 77, 78, 97
- Wireless local area network (WLAN),
 - 56, 97
- Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, 56, 57
- Wireless networks, 55–57, 70, 71, 73,
 - 77, 78, 96, 97, 146, 150
- Worms, 46, 100
- WPA and WPA2, 77, 97

<http://www.pbookshop.com>