Index

Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.

A

AAA (authentication, authorization, and accounting), 45, 46
abstract machine concept, 90, 91
Acceptable Use Policies (AUPs), 129
acceptance in risk treatment, 202–203
access control lists (ACLs)
   DAC, 87
   firewalls, 360
   overview, 69
access controls domain, 61–62
   administrative access controls, 69–70, 70
authentication. See authentication categories, 67
cloud, 432–433
Common Body of Knowledge, 6
DAC, 86–87
description, 62–63
exam essentials, 114–115
geographic, 48
identification, 70–72, 71
logical controls, 68–69
mandatory. See mandatory access control nondiscretionary, 87
overview, 40–41
physical controls, 67–68
protected resources, 63–64
purpose, 64–66
review questions, 116–120
subjects and objects, 66–67, 66
summary, 113
system-level, 86
temporal, 48
written lab, 115
access points. See wireless access points (WAPs)
Access principle in European Convention on Human Rights, 129
account-level access control, 94
   account deactivation, 52
   authentication, 95–96
authorized use policies, 101
callback, 100
contractor accounts, 100–101
dual control, 94
guest accounts, 100
last login notification, 99
lockout policy, 99
privileged accounts, 96–97
role-based access control, 101–103, 102–103
user accounts, 97–99
violation warning screen, 100, 100
account life cycle, 97
Account Lockout settings, 412–413
Accountability principle in European Convention on Human Rights, 129
accountability statements in security policies, 131
accounting
   in AAA, 45, 46
   in access control, 41
   in configuration management, 137
accusations during investigations, 231
ACLs (access control lists)
   DAC, 87
   firewalls, 360
   overview, 69
acquire time in biometrics, 81
acronyms, 33
actions, threat, 187
Active Directory (AD), 71, 348, 350
active network monitoring, 208, 341
ActiveX technology, 410
ad hoc wireless networks, 373, 374
Adams, Carlisle, 279
add-ons, malicious, 409–410
Address Resolution Protocol (ARP), 327, 339
adherence statements in incident response policies, 225
Adleman, Leonard, 283
administrative controls, 63, 69–70, 70, 189
administrative requirements for BYOD, 51
administrators, communicating monitoring results with, 216
Advanced Encryption Standard (AES), 32, 278–279
advanced persistent threats (APTs), 392, 394
Advanced Privacy Settings dialog box, 495, 495
adware, 395
AES (Advanced Encryption Standard), 32, 278–279
affinity rules for storage clustering, 455
agents
key recovery, 293
SNMP, 212
threat, 187
agile development process, 141
AHs (authentication headers), 307, 345
AIC triad, 38–39
air gaps, 306, 400–401
alarms in incident response plans, 227
ALE (annualized lost expectancy), 196–197
alert severity level for syslogs, 213
alerts in incident response plans, 227–229
algorithms in cryptography, 263–264, 271–272
alternate processing strategies in disaster recovery plans, 245–247
alternate sites, 172–173
American National Standards Institute (ANSI), 329
accreditation by, 4
description, 37
American Standard Code for Information Interchange (ASCII), 319
analysis
evidence, 238–239, 238
incident response plans, 227–228
risk, 190, 194–199
analytics in monitoring, 212–213
annualized lost expectancy (ALE), 196–197
annualized rate of occurrence (ARO), 197
anomaly-based monitoring systems, 365
anonymous workstation access, 414–415
ANSI (American National Standards Institute), 329
accreditation by, 4
description, 37
antennas for wireless access points
placement, 379
types, 380–381
anti-affinity rules in storage clustering, 455
anti-malware and anti-spyware software, 405
antivirus program logs, 343
APEC (Asia-Pacific Economic Cooperation), 444
applets, 409–410
Applicant Endorsement Assistance Form, 14
Application layer in OSI model, 329
applications
centralized application management, 423–424
cloud. See cloud
exam essentials, 458
logs, 342
review questions, 460–463
summary, 457
workstations, 422–423
written lab, 459
APTs (advanced persistent threats), 392, 394
architecture models in mandatory access control, 91–94
armored viruses, 397
ARO (annualized rate of occurrence), 197
ARP (Address Resolution Protocol), 327, 339
artificial intelligence, 83
ASCII (American Standard Code for Information Interchange), 319
Asia-Pacific Economic Cooperation (APEC), 444
assessment
vs. analysis, 198
forensic investigation results, 239
risk, 199–201, 200
assets
disaster recovery plans, 244
in information gathering, 198
managing, 142–143
risk management, 185–186
Associate of (ISC)2, 8
assurance of accountability, 107–108
assurance procedures, 64
asymmetric cryptography
algorithms, 267
keys, 266–267
non-key-based, 284
overview, 280–284, 281, 283
attachments, 403–404
attacks
business continuity plans for, 159
on cryptography, 296–297
on intrusion prevention systems, 206–207
terms and concepts, 393–401
wireless networks, 378
audience statements in security policies, 131
audits and auditing
  in access control, 41
  in configuration management, 137
  logs, 342
  passwords, 75
  in privilege management, 52
  trusted systems, 91
  user accounts, 98
AUPs (Acceptable Use Policies), 129
AUPs (Authorized Use Policies)
  applications, 422
  description, 101
  new hires, 52, 69–70, 70
authentication
  in AAA, 45, 46
  account-level access control, 95–96
  certificate-based, 95
  description, 41
  devices, 95
  factors, 74
  internetworks, 109–112
  local users, 348–350, 348
  multifactor, 84–85
  overview, 72–73
  remote user authentication services, 346–347
  reverse, 95–96
  session-level access control, 104
  single-factor, 84
  something you are, 79–83, 79, 82
  something you do, 82–83
  something you have, 77–78, 78
  something you know, 74–77, 76–77
  token-based access control, 85–86, 85
authentication, authorization, and accounting
  (AAA), 45, 46
authentication headers (AHs), 307, 345
Authenticode certificates, 410
authorization
  in AAA, 45, 46
  in access control, 41
  security policies, 131
Authorized Use Policies (AUPs)
  applications, 422
  description, 101
  new hires, 52, 69–70, 70
automated log off, 417
automated power-down, 417
automatic failover, 251
availability in CIA triad, 39
availability zones, 443
avoidance in risk treatment, 203
awareness of security policies, 135–136

B
back doors, 395
backups, 247–248
  differential, 248–249, 249
  full, 248
  incremental, 249, 250
  mirrored, 248
  policies, 129
  routers, 363
  storage considerations, 250
  workstations, 414
badges, 78, 78
bandwidth throttling, 381
barcode readers, 148
base stations, cellular, 375
baseband transmission method, 325
baselines
  incident response plans, 227
  intrusion detection systems, 364, 364
  network security, 356–357
  routers, 363
  security policies, 132–133
bastion hosts, 354
BCPs. See business continuity plans (BCPs)
behavior-based malware detection, 365, 413
Bell-LaPadula model, 92
Beta videotape recording standard, 35
BIAs (business impact analyses), 161–165, 164–165, 241–242, 242
Biba information model, 92–93
big data environments, 449–451
biometric signatures, 79
biometrics, 79–83, 79, 82
birthday attacks, 297
blacklists, 67, 360
block ciphers
  description, 271–273
  modes, 273–276, 274–276
Blowfish algorithm, 279
bluebugging, 378
bluejacking, 378
bluesnarfing, 378
Bluetooth Special Interest Group, 377
Bluetooth technology, 377, 427
booking exam, 21–22
boot sector viruses, 396
borderless computing, 443
bot herders, 393
botnets, 393
BRDs (business requirements documents), 141
breaks, exam, 24
Brewer-Nash model, 94
briefing papers, 156
Bring Your Own Cloud (BYOC), 432
Bring Your Own Device (BYOD) policies, 51, 150, 425–427
broadband transmission method, 326
browsers in mobile devices, 427
brute force attacks, 296
BS 7799 standard, 124
buffer overflow attacks, 395
building components availability in disaster recovery plans, 244
bus topology, 330, 331
business continuity plans (BCPs)
description, 240–241
developing, 160, 161
overview, 157–160
terms, 241–242
testing and drills, 252–253
business processes risk category, 185
business requirements documents (BRDs), 141
business security classification, 298
BYOC (Bring Your Own Cloud), 432
BYOD (Bring Your Own Device) policies, 51, 150, 425–427
CAM (centralized application management), 423–424
cancelling exam, 21–22
Candidate Background Qualifications, 22
candidate information bulletin (CIB), 8
CAP (Certified Authorization Professional), 11
capabilities lists
  - DAC, 87
government classification, 88
capability tables, 69
CAPTCHA characters, 76, 76
captive portals, 379
carrier sense multiple access/collision avoidance (CSMA/CA) protocol, 335
carrier sense multiple access/collision detection (CSMA/CD) protocol, 335
carrier sense multiple access (CSMA) protocol, 335
CAs (certificate authorities), 95, 268, 301–302
CAST-256, 279
categories in security, 39–40
CBC (cipher block chaining) mode, 274, 274
CBK (Common Body of Knowledge), 2–3, 6–8
CBT (computer-based training), 155
CCBs (change control boards), 142
CCFP (Certified Cyber Forensics Professional), 11
CCMP (Cipher Block Chaining Message Authentication Code Protocol), 372
CD (compact disc) standardization, 35
CEHs (certified ethical hackers), 391
cellular technologies, 369–373, 375, 376
centralized application management (CAM), 423–424
centralized authentication in internetworks, 109
centralized key management, 293
CER (Crossover Error Rate), 81
CERT (Computer Emergency Response Team), 209
certificate authorities (CAs), 95, 268, 301–302
certificate revocation lists (CRLs), 302
certificates
  - authentication, 95
  - Authenticode, 410
cryptography, 267–268, 300–301, 300, 302
expiration and revocation, 302
viewing, 497–499, 498–499
certifications
  - maintenance, 9–10
types, 10–12
Certified Authorization Professional (CAP), 11
Certified Cyber Forensics Professional (CCFP), 11
Certified ethical hackers (CEHs), 391
Certified Information Systems Security Professional (CISSP), 2–3
Certified Secure Software Lifecycle Professional (CSSLP), 11–12
CFB (cipher feedback) mode, 274–275, 275
chain of custody in forensic investigations, 238
challenge-and-response systems, 76, 76
change
  managing, 142
  passwords, 74
  proposals, 137
  security policies, 135
change advisory boards (CABs), 142
change control boards (CCBs), 142
chapters, 16
charters for incident response policies, 224
checklist tests for recovery, 169–170, 252
chosen ciphertext attacks, 296
chosen plaintext attacks, 296
CIA triad, 38–39, 38
CIB (candidate information bulletin), 8
cipher block chaining (CBC) mode, 274, 274
Cipher Block Chaining Message Authentication
  Code Protocol (CCMP), 372
cipher feedback (CFB) mode, 274–275, 275
cipher suites, 295
ciphertext, 265
ciphertext-only attacks, 297
circuit-switched networks, 334
CISSP (Certified Information Systems Security Professional), 2–3
Clark-Wilson model, 93
Class II transmitters, 377
classification
  cryptography, 297–299
  information policy, 144–145
  labels, 87–89
  process, 145–147
clean screens and desktops, 416–418
clear text, 265
clearance levels, 145
clearing keys, 306
client encroachment in cloud-based security, 112–113
clipper chip, 294
clipping levels
incident response plans, 226
intrusion detection systems, 364, 364
cloaking technique, 381
cloud
  applications, 438–442
  characteristics, 432–434
  communication, 430–432
  community, 435
  concepts, 429–430
  data processing in, 439–440
  data storage in, 441–442
  data transmission and movement, 440–441
disaster recovery plans, 246
hybrid, 435–436
Infrastructure as a Service, 437–438
legal and privacy concepts, 442–449
overview, 428–429
Platform as a Service, 437
private, 434–435
public, 435
security overview, 111–113
Software as a Service, 436–437
virtualization security, 449
clustering
disaster recovery, 250–251
software-defined networks, 454–455
t coaxial cable, 325
Code of Ethics, 2, 22, 136
code signing, 423
cold sites, 172, 246
collisions, 265–266
collusion, 265
color codes in government classification, 88–89
commercial hackers, 391
common access cards (CACs), 78
Common Body of Knowledge (CBK), 2–3, 6–8
communication
  cloud, 430–432
  converged networks, 340
disaster recovery plans, 245
incident response plans, 230–231
monitoring results, 215–216
risk assessment information, 201
security policies, 135–136
software releases, 141
community clouds, 435
compact disc (CD) standardization, 35
compensating controls, 190
compliance in cryptography, 298–299
computer-based training (CBT), 155
Computer Emergency Response Team (CERT), 209
computer worms, 393
confidential classification, 88
confidentiality in CIA triad, 38–39
confirmation email, 23
confusion in cryptography, 271
connection models for networks, 334
connection time limits, 104
connectionless protocols, 328
Consent principle in European Convention on
Human Rights, 129
constrained view control, 104–105
consultants, policies for, 131
containment in incident response, 233–234
content-based access control, 106
contextual–based access control, 106
continued certification, 9–10
continuing professional education (CPE)
  credits, 9–10, 14
continuous authentication, 104
continuous monitoring
  networks, 341
  risk management, 208–209
contracted sites, 246
contractor accounts, 100–101
contractors, policies for, 131
contractual privacy obligations, 444
contractual requirements, policies for, 126
control plane for routers, 362
controls. See also access controls domain
  in configuration management, 137
  risk management, 43, 189–190
converged network communications, 340
cookies, 95
  managing, 494–495, 494–495
  overview, 402–404, 403
cooperative sites, 173
coodinators for software releases, 141
copiers, documents stored on, 408
copper cable, 323–324, 325
Corporate Owned Personally Enabled (COPE)
  programs, 427–428
corporate policies, 125–126
corporate-wide security training, 52
cost in risk treatment, 202
counter (CTR) mode, 276, 276
countermeasures, 63
  incident response plans, 235
  malicious code, 405–408, 406–407
  threats, 190
courier services for backups, 250
covered channels, 396
CPE (continuing professional education)
  credits, 9–10, 14
criminals, 391
crime, business continuity plans for, 158–159
critical severity level for syslogs, 213
CRLs (certificate revocation lists), 302
Cross-Site Request Forgery (CSRF), 395
Cross Site Scripting (XSS), 359, 395
Crossover Error Rate (CER), 81
cryptanalysis, 265
cryptograms, 265
cryptography domain
  algorithm evolution, 32, 32
  algorithm problems, 49–50
  asymmetric, 280–285, 281, 283
  attacks on, 296–297
  block ciphers, 272–276, 274–276
  certificates, 300–302, 300
  cipher suites, 295
  cloud data, 442
  Common Body of Knowledge, 7
data classification and regulatory
  requirements, 297–299
digital watermarks, 287
eccentric curve and quantum cryptography, 285
ephemeral keys, 295
exam essentials, 311–313
hashing, 287–290, 288
history, 263
hybrid, 286
key escrow, 293–294
key length, 291
key management, 294–295, 303–306
keyed-hash message authentication code, 290–291
Message Authentication Code, 290
mobile devices, 427
non-repudiation, 291–292
overview, 262
perfect forward secrecy, 296
public key infrastructure, 299–300
review questions, 314–316
secure protocols, 306–310
steganography, 286, 287
summary, 311
symmetric, 276–280, 277
terms and concepts, 263–272
wireless networks, 372
workstations, 419–420
written lab, 313
cryptology, 265
cryptoprocessors, 420
cryptosystems, 265
cryptovariables, 266
CSMA (carrier sense multiple access) protocol, 335
CSMA/CD (carrier sense multiple access/collision detection) protocol, 335
CSMA/CA (carrier sense multiple access/collision avoidance) protocol, 335
CSRF (Cross-Site Request Forgery), 395
CSSLP (Certified Secure Software Lifecycle Professional), 11–12
cumulative employment experience, 8–9
customers, working with, 54
cyberwarfare, 392

data in transit, 105, 144
Data Link layer in OSI model, 326
data management policies, 143
classification process, 145–147
data states, 144
ILM, 144
information classification policy, 144–145
data plane for routers, 362
data processing in cloud, 439–440
data protection impact assessments (PDIsAs), 446
data transmission methods in OSI model, 325–326
data warehouse, 449–451
database administrators, communicating monitoring results with, 216
DCDs (dedicated computing devices), 430
deactivation of user accounts, 52, 98–99, 101
debug severity level for syslogs, 213
decentralized authentication, 109–110
decentralized key management, 294
decoding, 265
decryption, 264
dedicated computing devices (DCDs), 430
dedicated hosting in Infrastructure as a Service, 437
default passwords
avoiding, 74
endpoint devices, 149
routers, 362
Defense Advanced Research Projects Agency (DARPA), 321
defense-in-depth strategy, 64–65, 65
definitions in incident response policies, 225
delivery methods for training executives, 157
management, 156
users, 155
demilitarized zones (DMZs), 353–354, 354
department of Defense (DoD) directives, 4–5, 5
deprovisioning accounts, 97–98
derived keys, 304
DES (Data Encryption Standard), 32, 32, 278
desk check tests, 252
desktops
virtual, 455–456
workstations, 416–418
destruction of keys, 305–306
detection. See also intrusion detection systems (IDSs)
incident response plans, 227
in security, 40
deterrence, 64–65
devices
- authentication, 95
endpoint. See endpoint devices
monitoring, 211
diagnostic tools
- cookie management, 494–495, 494–495
Event Viewer, 495–497, 496–497, 503–505, 503–507
hash values, 507–509, 508–509
Microsoft Baseline Security Analyzer, 488–491, 489–490
Microsoft Password Checker, 491, 492
SmartScreen Filter, 492–493, 493
Windows Certificate Manager, 497–499, 499
dictionary attacks, 297
differential backups, 248–249, 249
differential cryptanalysis attacks, 297
Diffie, Whitfield, 284
Diffie-Hellman key exchange algorithm, 284–285
diffusion in cryptography, 271
digital certificates. See certificates
digital convergence, 340
digital environments
- business continuity plans for, 159
incident scenes, 236
digital finger print images, 79
Digital Rights Management (DRM), 287
digital signatures, 282, 283
digital watermarks, 287
directional antennas, 380
Directive 95/46 EC, 444–446
directory transversal, 395
disabling ports, 356
disaster recovery plans (DRPs)
- alternate sites, 172–173
asset identification, 244
backups, 247–250, 250–250
communication plans, 245
description, 240
disaster preparation, 243–244
disaster types, 243, 243
electronic vaulting, remote journaling, and clustering, 250–251
overview, 165–166, 242–243
processing strategies, 245–247
RAID, 251–252
restoration planning, 247
restoration resources, 244
strategies, 167–168, 169
testing and drills, 169–171, 252–253
Disclosure principle in European Convention on Human Rights, 129
discretionary access control (DAC), 86–87
distribution of keys, 303
DMAIC (Define, Measure, Analyze, Improve, and Control), 125
DMZs (demilitarized zones), 353–354, 354
document reviews in information gathering, 199
documentation of security policies, 134
DoD (Department of Defense) directives, 4–5, 5
Domain Name System (DNS), 339
domains in Common Body of Knowledge, 6–8
double file extension attacks, 398
drills for DRPs and BCPs, 252–253
drive-by attacks, 378
DRM (Digital Rights Management), 287
DRPs. See disaster recovery plans (DRPs)
dual accounts, 97
dual control systems, 94, 304
dual-homed firewalls, 358
due care, 44
due diligence, 44
dwell time in keystroke dynamics, 83
Dynamic Host Configuration Protocol (DHCP), 326
dynamic ports, 338
dynamic routes, 362
dynamic routing protocols, 361
dynamic threat analysis appliances, 409

E

EAM (emergency action message), 94
East/West data path, 452
EBCDIC (Extended Binary Coded Decimal Interchange Code), 319, 329
EC (erasure coding), 441–442
ECB (electronic codebook) mode, 274
ECC (elliptic curve cryptography), 285
ECPA (Electronic Communications Privacy Act of 1986), 447
EDI (electronic data interchange), 318
endpoint devices
application security, 422–423
centralized application management, 423–424
data sanitization, 421
defense, 149
health compliance, 148–149
mobile, 426–428
overview, 148
policies, 149–150
stolen, 424–425
user threats, 410–415, 412

enforcement statements, 132
enforcing security policies, 134–135
enrollment time in biometrics, 81
enterprise risk management (ERM), 207–208
enterprise-wide security policies, 129
ephemeral keys, 295
erasure coding (EC), 441–442
ERM (enterprise risk management), 207–208
error messages in Event Viewer, 503–505, 503–507
error rate
in authentication, 73
in biometrics, 81
error severity level for syslogs, 213
escape characters in SQL, 396
escrow passwords, 97
ESP (Encapsulating Security Payload), 307
ESP (Encapsulating Security Protocol), 346
Ethernet protocol, 335
EULAs (End-User License Agreements), 422–423
European Convention on Human Rights, 129
European Data Protection Directive (EDPD), 299
European Economic Area (EEA), 446
event triage, 187
Event Viewer
error messages, 503–505, 503–507
logs, 495–497, 496–497
events
handling, 224–226
incident response plans, 226
logs, 342
monitoring, 213–214
Evercookies, 402–403
evidence in forensic investigations
chain of custody, 238
guidelines, 236
investigation and analysis, 238–239, 238
volatility, 237

evil twin attacks, 378

exams, 17

booking, 21–22

exam essentials, 25–26

goals, 20

preparing for, 17–18

study time, 18–20, 18–19

summary, 25

taking, 22–24

exclusive or (XOR) function in cryptography, 268–269, 271–272

executing cloud-based applications, 438–439

executives

communicating monitoring results with, 216

training, 156–157

explicit actions, 50

explicit firewall rules, 359

explicitly allowed lists, 67

exposure factor (EF), 197

exposure in risk management, 190

Extended Binary Coded Decimal Interchange Code (EBCDIC), 319, 329

extended TACACS (XTACACS), 347

external threats, 188

external users, working with, 54

extranet users, working with, 54

F

F/FTP cable, 324

F/UTP cable, 324

Facebook, 49

facial recognition, 79

False Acceptance Rate (FAR) in biometrics, 81

false negatives, 73

false positives, 73

False Rejection Rate (FRR) in biometrics, 81

FAR (False Acceptance Rate) in biometrics, 81

Faraday bags, 234

Federal Communications Commission (FCC), 370

Federal Information Processing Standard (FIPS), 32, 32, 192

Federal Information Security Management Act (FISMA), 192

Federal Rules of Civil Procedure (FRCP), 448

federated access, 111, 351, 351

fees, exam, 21

fiber fabric, 332

fiber-optic transmissions, 322–323

file extension attacks, 398

file infecting viruses, 396

File Transfer Protocol (FTP), 338, 415

filters

MAC addresses, 356

SmartScreen Filter, 492–493, 493

spam, 368

visual security, 417

finger image identifier records, 79

fingerprint technology, 79

fingerprints, 79, 402

fingerscan technology, 79

FIPS (Federal Information Processing Standard), 32, 32, 192

fire events, business continuity plans for, 158

firewalls

in authentication, 73

overview, 357

packet filter, 357–358

proxy, 358

rules, 359–360

stateful packet inspection, 358–359

web application, 359

workstations, 419

firmware for routers, 362

FISMA (Federal Information Security Management Act), 192

fixes, software, 139

flight time in keystroke dynamics, 83

focus in training

executives, 156

management, 155

users, 154

forensic investigations

assessment results, 239

evidence

chain of custody, 238

investigation and analysis, 238–239, 238

volatility, 237

guidelines, 235–236

incident scenes, 236–237

principles, 237

formal access policies for external data, 106

formal briefings in management training, 156

Formal Risk Modeling, 195
forwarding plane for routers, 362
frames in OSI model, 326
FRCP (Federal Rules of Civil Procedure), 448
frequency analysis in cryptography, 297
frequency in training
executives, 157
management, 156
users, 155
FRR (False Rejection Rate) in biometrics, 81
FTP (File Transfer Protocol), 338, 415
full backups, 248
full interrupt tests, 171, 253
full-time incident response teams, 232
functional incident response teams, 232
functional policies, 127

G

gain for antennas, 381
GAP (Global Academic Program), 15
General Data Protection Regulation (GDPR), 445–446
geographic access control, 48
geolocation and geotagging, 83
GLBA (Gramm-Leach-Bliley Act), 446
Global Academic Program (GAP), 15
globally unique identifiers (GUIDs), 350
goals, exam, 20
government
security classifications, 87–89, 298
standards, 4, 36
Gramm-Leach-Bliley Act (GLBA), 446
Group Policy manager
passwords, 151
role-based access control, 101–102, 102
guarded alert level in incident response plans, 229
guest access policy, 130
guest accounts, 100
“Guide for Conducting Risk Assessments,” 199
guidelines
event and incident handling policy, 226
security policies, 133, 134
“Guidelines for Media Sanitization,” 421
GUIDs (globally unique identifiers), 350

H

hackers, 391
hacktivists, 392
Hadoop Distributed File System, 450
hardening workstations, 425
hardware
destruction, 421
trusted systems, 90
hardware key storage, 293
hardware security module modules (HSMs), 305
hashing and hashing algorithms
cryptography, 287–290, 288
hash value calculations, 507–509, 508–509
process, 266
S/KEY password system, 86
Health Insurance Portability and Accountability Act (HIPAA), 49, 69, 446
HealthCare Information Security and Privacy Practitioner (HCISPP), 11
heart/pulse pattern recognition, 83
Heartbleed bug, 309–310
Hellman, Martin, 284
heuristic-based detection, 365, 414
HIDPs (host-based intrusion detection/prevention systems), 426
HIDPs (host intrusion detection systems), 364
HIPAA (Health Insurance Portability and Accountability Act), 49, 69, 446
HMAC (keyed-hash message authentication code), 290–291
hoaxes, virus, 396
hop counters, 361
host-based firewalls, 419
host-based intrusion detection/prevention systems (HIDPs), 426
host clustering
software-defined networks, 454
virtualization, 456
host intrusion detection systems (HIDPs), 364
hosted applications in Software as a Service, 436
hosting in cloud, 437–438
hot patches, 139
hot sites, 172, 245–246
hotfixes for software, 139
HSMs (hardware security module modules), 305
HTTP forgery attacks, 359
human-caused events
human resources — intentional vulnerabilities

business continuity plans for, 158
risk category, 185
human resources, working with, 53
hybrid clouds, 435–436
hybrid cryptography, 286
hybrid wireless networks, 373
Hypervisor, 456
countermeasures, 235
creating, 226–229
incident response containment and restoration, 233–234
incident response records, 232–233
incident response teams, 231–232
law enforcement and media communication, 229–231
security event information, 233
review questions, 256–259
summary, 253–254
written lab, 255
incident response policies, 130, 224–226
incident response records, 232–233
incident response teams, 231–232
incident scenes, 236–237
incidents, defined, 226
included by exception lists, 67
incremental backups, 249, 250
industrial security classification, 298
industry standards, 4, 36–37
Information Assurance (IA) workforce, 4
information classifications, 88, 144–145
information-gathering techniques, 198–199
Information life cycle management (ILM), 144
information risk management (IRM), 183–184
information security management systems (ISMSs), 124–125, 191
information security operations center (ISOC), 209–210
information severity level for syslogs, 213
Information Technology Infrastructure Library (ITIL), 125
Information Technology Laboratory (ITL), 194
information technology risk category, 185
Infrastructure as a Service (IaaS), 112, 437–438
infrastructure mode for wireless networks, 373, 374
initialization vectors in cryptography, 264–265
innerduct interior tube design for fiber-optic cable, 323
insider threats, 187, 392
Institute of Electrical and Electronics Engineers (IEEE), 37
instructions procedures in security policies, 133
intangible assets, 142, 186
Integrated Services Digital Network (ISDN), 334
integrity in CIA triad, 39
intentional vulnerabilities, 188
interference in copper cable, 324–325
interim processing strategies in disaster recovery plans, 245–247
intermediary certificate authorities, 301
internal use classification, 88
International Assigned Numbers Authority (IANA), 295
International Data Encryption Algorithm (IDEA), 279
International Electrotechnical Commission (IEC), 125, 191
International Information Systems Security Certification Consortium (ISC)², 2
certifications, 3–4
Department of Defense directives, 4–5, 5
exam essentials, 25–26
history, 3
industrial and government standards, 4
recognition, 4
summary, 25
International Organization for Standardization (ISO)
description, 37
standards, 124–125, 191
international regulations for cloud, 444
Internet Assigned Numbers Authority (IANA) for ports, 336
Internet Control Message Protocol (ICMP), 211, 339
Internet Engineering Task Force (IETF), 37, 340
Internet Explorer
cookie management, 494–495, 494–495
SmartScreen Filter, 492–493, 493
Internet Key Exchange (IKE), 307, 346
Internet Message Access Protocol (IMAP), 339
Internet of Things (IoT), 148, 340
Internet Protocol (IP) addresses
IPv4 and IPv6, 326–327, 327
network address translation, 354–355
subnetting, 352–353, 352
Internet Protocol Security (IPsec), 306–308, 345–346, 346
internetwork trust architectures, 108–111
interruption tests, 171
interviews in information gathering, 198–199
intrusion detection (ID), 364
intrusion detection systems (IDSs)
host-based, 426
vs. intrusion prevention systems, 366–367
overview, 364
intrusion prevention systems (IPSs)
attacks on, 206–207
in authentication, 73
host-based, 426
vs. intrusion detection systems, 366–367
malware detection, 409
overview, 364–365
wireless, 365–366
invocation property, 92–93
IPv4 and IPv6, 326–327, 327
iris scans, 79, 79
IRM (information risk management), 183–184
ISDN (Integrated Services Digital Network), 334
ISMSs (information security management systems), 124–125, 191
ISO/IEC 27000 series of standards, 124–125, 191
ISO (information security operations center), 209–210
isolation with virtual machines, 456
ITIL (Information Technology Infrastructure Library), 125
ITL (Information Technology Laboratory), 194

J
jail-broken phones, 427
Java applets, 409–410
JBOD (just a bunch of disks), 454
JeOS (just enough operating system), 453
job rotation policies, 48, 48
jurisdiction in cloud-based security, 113
just a bunch of disks (JBOD), 454
just enough operating system (JeOS), 453

K
Kamkar, Samy, 402
KDCs (key distribution centers), 303, 349
KEKs (key encrypting keys), 304
Kerberos authentication protocol
internetworks, 110–112
key distribution, 303
non-repudiation, 292
overview, 348–350, 348
Keteyian, Armen, 408
key distribution centers (KDCs), 303, 349
key encrypting keys (KEKs), 304
key fobs, 85
key pairs, 266, 271
key space, 263
keyed-hash message authentication code (HMAC), 290–291
keyloggers, 393
keys in cryptography, 266–267, 303
asymmetric, 280–285, 281, 283
clustering, 265–266
distributing, 303
generating, 303
key encrypting keys, 304
key escrow, 293–294
length, 291
managing, 294–295
retrieval, 304–305
storage and destruction, 305–306
stretching, 270
symmetric, 277–279, 277
keystroke dynamics, 83
known plaintext attacks, 296
Koblitz, Neil, 285

L
L2F (Layer 2 Forwarding), 344
L2TP (Layer 2 Tunneling Protocol), 344
labels for backups, 250
labor availability in disaster recovery plans, 244
LANs (local area networks), 318, 377
last login notification, 99
Law Enforcement Access Field (LEAF), 294
law enforcement and incident response plans, 229–230
Layer 1 in OSI model, 322–326, 325
Layer 2 Forwarding (L2F), 344
Layer 2 in OSI model, 326
Layer 2 Tunneling Protocol (L2TP), 344
Layer 3 in OSI model, 326–327
Layer 4 in OSI model, 328, 328
Layer 5 in OSI model, 328–329
Layer 6 in OSI model, 329
Layer 7 in OSI model, 329
layered security, 64
LDAP (Lightweight Directory Access Protocol), 348
LEAF (Law Enforcement Access Field), 294
least privilege principle, 45
LEDs (light emitting diodes) for fiber-optic cable, 323
legal botnets, 393
legal holds on data, 448
legal issues for cloud, 442–449
legislative compliance, policies for, 125–126
levels
in disaster recovery plans, 166
in training
executives, 156
management, 155
users, 155
libraries, signature, 365
licenses in cloud-based applications, 439
light emitting diodes (LEDs) for fiber-optic cable, 323
Lightweight Directory Access Protocol (LDAP), 348
limitations in incident response policies, 225
links for email, 418
lists in access controls, 67
litigation holds on data, 448
load-balancing clustering, 251
local area networks (LANs), 318, 377
local chapters, 16
local user authentication services, 348–350, 348
Locard, Edmund, 237
Locard’s exchange principle, 237
lockout policies
accounts, 99
passwords, 412–413
log off, automated, 417
logic bombs, 397–398
logical controls
description, 63
overview, 68–69
logins
identification in, 71, 71
session-level access control, 104
logo use, 15
logs and log files
Event Viewer, 495–497, 496–497
networks, 212–213, 342–343
loose coupled clusters, 455
lost devices, 152
M of N control

description, 46–47
keys, 293, 305
MAC limiting, 356
MAC (Media Access Control) addresses
with ARP, 339
filtering, 356
OSI model, 326
MAC (Message Authentication Code), 290
macro viruses, 396
maintaining SSCP certification, 14
maintenance hooks, 201
maintenance in risk assessment, 201
malicious code and activity domain
add-ons, 409–410
Common Body of Knowledge, 8
cookies and attachments, 402–404, 403
countermeasures, 405–408, 406–407
power supplies, 404
SmartScreen Filter for, 492–493, 493
sources, 390–392, 391
spam management, 401–402
terms and concepts, 393–401
user threats, 410–415, 412
malware
description, 394
training for, 150–151
man in the middle attacks, 394
managed file transfer (MFT), 440–441
management, training, 155–156
management information bases (MIBs) in
SNMP, 212
managerial certifications, 11
managers in SNMP, 212
mandate statements in security policies, 131–132
mandatory access control
account-level. See account-level access control
administering, 89–90
architecture models, 91–94
assurance of accountability, 107–108
cloud-based security, 111–113
data access control, 105–106
data protection, 207
data sharing, 205–207
data sources, 390–392, 391
data transfer, 105–106
database migration, 487–490
database reconstruction, 490–491
database-related data, 108
夫妇 data and printed media, 106–107
view-based, 104–105
mandatory security training, 52
mandatory vacations, 46
MANs (metropolitan area networks), 376
MapReduce framework, 450
master keys, 304
maximum tolerable downtime (MTD), 164,
241–242, 242
maximum tolerable period of disruption
(MTPoD), 241
MBSA (Microsoft Baseline Security Analyzer),
407, 407, 488–491, 489–490
MD4 and MD5 hashing algorithms, 86
MD5 (Message Digest 5), 289
MDM (Mobile Device Management), 426–427
measured service in cloud, 433–434
mechanical standards, 36
Media Access Control (MAC) addresses
with ARP, 339
filtering, 356
OSI model, 326
media access models, 335
media communication for incident response
plans, 230–231
media destruction policy for external data, 106
Melissa virus, 404
member numbers, 25
Merkle, Ralph, 284
mesh topology, 332, 333, 377
Message Authentication Code
(MAC), 290
Message Digest 5 (MD5), 289
metrics in monitoring, 212–213
metropolitan area networks (MANs), 376
MFT (managed file transfer), 440–441
MIBs (management information bases) in
SNMP, 212
Microsoft Baseline Security Analyzer (MBSA),
407, 407, 488–491, 489–490
Microsoft Office 365, 424
Microsoft Password Checker, 75, 491, 492
Microsoft SharePoint, 86–87
Miller, Victor, 285
MIME type, 404
mirrored backups, 248
mirroring, RAID, 251
miscellaneous events, business continuity plans for, 159
mistaken access, training for, 152
mitigation of risk, 185
Mobile Device Management (MDM), 426–427
mobile devices, 130, 150, 426–428
mobile sites, 246
monitoring and analysis domain
Common Body of Knowledge, 7
IDFs and IPSs, 365
networks, 341–343
privileged accounts, 96–97
results, 215
analytics, metrics, and trends, 212–213
communicating, 215–216
event data, 213–214
networks, 211–212
visualization, 214
risk management, 208–209
Moore's law, 263, 291
moving cloud data, 440–441
MTD (maximum tolerable downtime), 164, 241–242, 242
MTPoD (maximum tolerable period of disruption), 241
multi network controllers, 366
multifactor authentication, 84–85
multimode fiber-optic cable, 323
multipartite viruses, 397
multiple logon control, 104
mutual sites, 246

National Institute of Standards and Technology (NIST)
800 series of Special Publications, 124–125
cloud, 432
data sanitization, 421
description, 36–37
DoD directives, 4
National Security Agency (NSA), 291, 294, 403
natural events, business continuity plans for, 158
NDAs (nondisclosure agreements), 22
NDP (Network Discovery Protocol), 327
need to know classifications, 89
Nessus scanner, 407
network access control (NAC)
BYOD requirements, 51
endpoint health compliance, 148–149
overview, 368–369
network address translation (NAT), 326–327, 354–355
network administrators, communicating monitoring results with, 216
Network Discovery Protocol (NDP), 327
network interface cards (NICs), 358
network intrusion detection systems (NIDSs), 364
Network layer in OSI model, 326–327
network locks, 356
network management system (NMS), 212
networks and communications domain
access policies, 129
cellular technologies, 369–373, 375, 376
Common Body of Knowledge, 7–8
connection models, 334
converged communications, 340
device security, 355–356
exam essentials, 383–384
firewalls, 357–360
invasion detection and prevention devices, 363–368, 364
invasion prevention systems, 206–207
local user authentication services, 348–350, 348
media access models, 335
models, 318
monitoring, 341–343
monitoring results, 211–212
OSI model. See Open Systems Interconnection (OSI) model
policies, 130
ports, 336–338
NAC (network access control)
BYOD requirements, 51
device health compliance, 148–149
overview, 368–369
names and item synonyms, 33–34
NAT (network address translation), 326–327, 354–355
nation states, 392
National Bureau of Standards, 192
National Initiative for Cybersecurity Education (NICE) standard, 4
NDAs (non-disclosure agreements), 22
NDP (Network Discovery Protocol), 327
need to know classifications, 89
Nessus scanner, 407
network access control (NAC)
BYOD requirements, 51
device health compliance, 148–149
overview, 368–369
network address translation (NAT), 326–327, 354–355
network administrators, communicating monitoring results with, 216
Network Discovery Protocol (NDP), 327
network interface cards (NICs), 358
network intrusion detection systems (NIDSs), 364
Network layer in OSI model, 326–327
network locks, 356
network management system (NMS), 212
networks and communications domain
access policies, 129
cellular technologies, 369–373, 375, 376
Common Body of Knowledge, 7–8
connection models, 334
converged communications, 340
device security, 355–356
exam essentials, 383–384
firewalls, 357–360
invasion detection and prevention devices, 363–368, 364
invasion prevention systems, 206–207
local user authentication services, 348–350, 348
media access models, 335
models, 318
monitoring, 341–343
monitoring results, 211–212
OSI model. See Open Systems Interconnection (OSI) model
policies, 130
ports, 336–338
protocols, 338–340
quality of service, 381–382
remote access, 343–346, 344–346, 368–369
remote user authentication services, 346–347
review questions, 385–388
routers, 361–363
security state, 356–357
segmentation, 351–355, 352, 354
software-defined, 451–455
summary, 382–383
switches, 363
topology models, 330–334, 331–333
traffic shaping, 381
wireless. See wireless networks
written lab, 384
new hire orientation, 52
New Technology File System (NTFS), 398, 419
NICE (National Initiative for Cybersecurity Education) standard, 4
NICs (network interface cards), 358
NIDSs (network intrusion detection systems), 364
NIST. See National Institute of Standards and Technology (NIST)
“NIST Definition of Cloud Computing,” 432
NIST Special Publication 800-30 Revision 1, 199–200, 200, 391, 391
NIST Special Publication 800-37 Revision 1, 192–194, 193
NIST Special Publication 800-39, 194
NIST Special Publication 800-145, 432, 436
Nmap scanner, 406–407
NMS (network management system), 212
non-key-based asymmetric cryptography, 284
nonces, 276
nondisclosure agreements (NDAs), 22
nondiscretionary access controls, 87
nonrepudiation, 42, 269, 291–292
normal alert level in incident response plans, 229
North/South data path, 452
Northbound APIs, 453
Notice principle in European Convention on Human Rights, 129
notice severity level for syslogs, 213
NSA (National Security Agency), 291, 294, 403
NTFS (New Technology File System), 398, 419
object classification, 145
objectives in incident response policies, 225
objects in access controls, 66–67, 66
OCSP (Online Certificate Status Protocol), 302
OECD (Organization for Economic Cooperation and Development), 444–445
OFB (output feedback) mode, 275, 275
off-site storage, 106, 250
omnidirectional antennas, 380
on-demand scans for anti-malware, 405
on-demand self-service in cloud, 432–433
on-demand software in Software as a Service, 436–437
one-time pads, 85–86, 270
One-Time Passwords in Everything (OPIE), 86
one-to-one searches in biometrics, 81
one-way trust relationships, 109
Online Certificate Status Protocol (OCSP), 302
online posts, 151
onsite interviews in information gathering, 198–199
open data programs, 145
Open Systems Interconnection (OSI) model, 319
  Application layer, 329
  Data Link layer, 326
  Network layer, 326–327
  overview, 320–321, 320
  Physical layer, 322–326, 325
  Presentation layer, 329
  Session layer, 328–329
  vs. TCP/IP, 321, 322
  Transport layer, 328, 328
operating systems for mobile devices, 427
operational policies, 128
OPIE (One-Time Passwords in Everything), 86
opportunities and problems, 29–31, 31
Organization for Economic Cooperation and Development (OECD), 444–445
organizational policies, 127
origination location in session-level access control, 104
orphan accounts, 52
OSI model. See Open Systems Interconnection (OSI) model
out-of-band key exchange, 270, 303, 346
out-of-band transmissions, 396
output feedback (OFB) mode, 275, 275
outsourced incident response teams, 232
outsourcing policy, 130

P

PaaS (Platform as a Service), 112, 437
packet filter firewalls, 357–358
packet loops, 362
packet sniffers, 405–406
packet-switched networks, 334
Padding Oracle On Downgraded Legacy Encryption (POODLE), 309
palm geometry, 80
palm scans, 80
parallel tests, 170–171, 253
parity, RAID, 251
parking lot attacks, 378
partnership/cooperative sites, 173
passing score for exam, 17
passive monitoring in risk management, 208
passwords
  in authentication, 72
  best practices, 412, 412
  default, 74, 149, 362
  email, 418
  escrow, 97
  frequently used, 151–152
  guidelines, 74–75
  lockout policies, 412–413
  managing, 76–77, 77
Microsoft Password Checker, 491, 492
mobile devices, 427
one-time, 85–86, 270
policies, 129
routers, 362
single sign-on, 350
training for, 151
Trusted Platform Module, 420
user accounts, 98
workstations, 411–413, 412
PAT (port address translation), 355
Patch Tuesday, 138
patches
managing, 137–138
workstations, 415
Patriot Act, 447

payloads
  data in transit, 45
  description, 396
  viruses, 396
Payment Card Industry Data Security Standard (PCI DSS), 69, 444
payment for exam, 21
PDF (Portable Document Format), 319
PDIs (data protection impact assessments), 446
Pearson Professional Centers, 23
Pearson VUE professional testing centers, 2
penalties in incident response policies, 225
penetration testing, 146–147
perfect forward secrecy, 296
Performance Monitor, 500–502, 500–502
permanent virtual circuits (PVCs), 334
personal devices, 51
personal identification information (PII), 297–298
personal identification numbers (PINs), 72, 72
personal security questions, 96
personally identifiable information (PII)
  on devices, 425
  workstations, 419
personally owned devices (PODs), 452
pharming attacks, 400
phishing attacks
  description, 398
  email, 418
  SmartScreen Filter for, 492–493, 493
physical controls
  description, 63
  overview, 67–68
  purpose, 189
physical data in mandatory access control, 106–107
physical environment in incident scenes, 236
Physical layer in OSI model, 322–326, 325
physical requirements for BYOD, 51
physical security
  policies, 130
  workstations, 416
piggybacking, 80
PII (personal identification information), 297–298
PII (personally identifiable information)
  on devices, 425
  workstations, 419
PINs (personal identification numbers), 72, 72
PKI (public key infrastructure), 277, 299–300
Places feature, 49
plain old telephone service (POTS), 334
plaintext, 265
Plan-Do-Check-Act cycle, 125
plastic optical fiber, 323
plastic worksheets, 23
Platform as a Service (PaaS), 112, 437
plenum cable, 325
PODs (personally owned devices), 452
point-of-sale terminals, 148
point-to-point protocol (PPP), 344
Point-to-Point Tunneling Protocol (PPTP), 344
pointer overflow attacks, 395
policies and practices, 124
  best practices, 125
  changing and updating, 135
  communication and awareness, 135–136
    corporate, 125–126
    data management, 143–147
    documentation, 134
    endorsements, 128
    endpoint devices, 149–150
    enforcing, 134–135
    enterprise-wide, 129
    event and incident handling, 224–226
    format and design, 131–132
    overview, 126, 126
    privileged accounts, 96
    security alignment, 124–125
    support and execution, 132–134, 134
    supporting, 129–131
    types, 127–128
policy charters for incident response policies, 224
policy detail statements, 132
polymorphic viruses, 397
polyvinyl chloride (PVC) cable, 325
POODLE (Padding Oracle On Downgraded Legacy Encryption), 309
POP (Post Office Protocol), 339
port address translation (PAT), 355
Portable Document Format (PDF), 319
ports
  disabling, 356
  network, 336–338
positioning in physical security, 417
Post Office Protocol (POP), 339
post-processing for cloud-based applications, 439
POTS (plain old telephone service), 334
power-down, automated, 417
power gain
  for antennas, 381
power supplies for malware, 404
PPP (point-to-point protocol), 344
PPTP (Point-to-Point Tunneling Protocol), 344
practitioners, communicating monitoring results
  with, 216
preprocessing cloud-based applications, 439
Presentation layer in OSI model, 329
pretexting provisions, 446
prevention
  in incident response plans, 227
  in security, 39–40
primary version numbers, 139
printed media, access control for, 106–107
privacy
  cloud, 442–449
  cryptography, 298–299
    overview, 49
private clouds, 112, 434–435
private ports, 338
privilege escalation, 394
privilege life cycle, 51–52
privileged accounts, 96–97
privileges
  changes, 98
  overview, 51–52
PRNGs (pseudorandom number generators), 270, 303
procedural standards, 36
procedures
  event and incident handling policy, 225
  privileged accounts, 96
  security policies, 133
processes in business impact analyses, 162
processing cloud-based applications, 439
processing servers in wireless intrusion prevention systems, 366
processing strategies in disaster recovery plans, 245–247
procrastination, 206
proctored examinations, 17
professional association certifications, 10
promiscuous mode, 405
proof of concept, 394
proof of origin in asymmetric cryptography, 282
proofing user accounts, 98
proprietary standards, 36
protection in incident response plans, 227
protocol analyzers, 405–406
protocols, networks, 338–340
providers in Software as a Service, 437
provisioning
privileged accounts, 96
user accounts, 97–99
proxies, 357–360
proximity keys, 77, 78
prudent man, 44
pseudorandom number generators (PRNGs), 270, 303
public classification, 88
public clouds, 112, 435
public key cryptography, 280–285, 281, 283
public key infrastructure (PKI), 277, 299–300
public keys, 266
pulse pattern recognition, 83
Purpose principle in European Convention on Human Rights, 129
purpose statements in security policies, 131
PVC (polyvinyl chloride) cable, 325
PVCs (permanent virtual circuits), 334

Q
QAT (quality acceptance testing), 141
QoE (quality of experience), 382
QoS (Quality of Service)
networks, 381–382
risk management, 208
qualitative risk analysis, 197
quality acceptance testing (QAT), 141
quality of experience (QoE), 382
Quality of Service (QoS)
networks, 381–382
risk management, 208
quantitative risk analysis, 195–197
quantum cryptography, 285
Quantumcookies, 403
questionnaires in information gathering, 198
questions
exam, 17, 24
personal security, 96
quick fixes for software, 139

R
radio frequency modulation techniques, 322
RADIUS (Remote Authentication Dial-In User Service) protocol, 347
RAID (Redundant Array of Independent Disks), 251–252
rainbow tables, 272, 296
random number generators, 270, 303
ranking
assets, 186
disaster types, 243, 243
ransomware, 395–396, 400
RAs (registration authorities), 268, 301–302
rate limiting, 381
RBAC (role-based access control), 101–103, 102–103
RC4 algorithm, 279
RC5 algorithm, 279
reading techniques for exam, 18–20, 18–19
real-time anti-malware scans, 405
real-time monitoring, 208–209
recertification, 9–10
reciprocal sites, 173
recovery
devices, 424
plans. See disaster recovery plans (DRPs) in security, 40
recovery point objective (RPO), 164, 165, 241–242, 242
recovery time objective (RTO), 164, 241–242, 242
reducing risk, 185, 203
Redundant Array of Independent Disks (RAID), 251–252
reference monitors, 90, 91
reference templates, 79
regional regulations for cloud, 444
registered ports, 338
registers, risk, 205–207
registration authorities (RAs), 268, 301–302
registration of devices, 424
regression analysis, 356–357
regulations
cloud, 113, 444–445
cryptography, 297–299
regulatory agency standards, 36
regulatory compliance, policies for, 125–126
release management for software, 141
reminder memos in management training, 156
remote access policy, 130
remote authentication, 109
Remote Authentication Dial-In User Service (RADIUS) protocol, 347
remote journaling, 250–251
remote network access control, 343–346, 344–346, 368–369
remote user authentication services, 346–347
replay attacks, 372
repositories, 448
reputation risk category, 185
request to reset lockout policy, 99
requirements, cryptography, 298–299
rescheduling exam, 21–22
reservations in host clustering, 454
Reset Account Lockout Counter After setting, 413
reset interval in lockout policy, 99
residual risk, 203
resolution in incident response plans, 228
resources
   in alternate sites, 173
   pooling
   cloud, 432–434
   virtualization, 456
   security basics, 44–45
response in incident response plans, 228
responsibilities in incident response policies, 225
restoration
   disaster recovery plans, 244, 247
   incident response, 233–234
resumes, 9, 13–14
retention policy, 130
retina scans, 79–81, 79
retinography, 80
Retina scanner, 407
retrieval of keys, 304–305
retroviruses, 397
reverse authentication, 95–96
reverse engineering, 395
revocation of certificates, 302, 302
right to be forgotten, 445
right to erasure, 445
rights in privilege management, 52
Rijndael cipher, 278–279
ring topology, 331, 332
risk management framework (RMF), 192–193
risk, response, and recovery domain, 182–183
   analysis, 190, 194–199
   assessments, 199–201, 200
   assets, 185–186
   Common Body of Knowledge, 7
   controls, 189–190
   defining, 183
   description, 123
   enterprise risk management, 207–208
   exam essentials, 217–218
   exposure, 190
   impact, 190–191
   ISO/IEC 27000 series, 191
   monitoring, 208–209
   monitoring results
      analytics, metrics, and trends, 212–213
      communicating, 215–216
      event data, 213–214
      networks, 211–212
      visualization, 214, 215
   NIST Special Publication 800-37 Revision 1, 192–194, 193
   NIST Special Publication 800-39, 194
   overview, 42–43
   process, 184–185, 184
   registers, 205–207
   review questions, 219–222
   security operations center, 209–210, 210
   summary, 216–217
   threat intelligence, 210–211
   threats, 186–188
   treatment, 202–203
   treatment plans, 202
   treatment schedules, 203–205, 204
   vulnerabilities, 188–189
   written lab, 218
Rivest, Ronald, 279, 283
Rivest, Shamir, and Adleman (RSA) cryptosystem, 283–284
RMF (risk management framework), 192–193
rogue access points, 379
rogue software, 400
rogue virtual machines, 456
role-based access control (RBAC), 101–103, 102–103
roll forward, 144
rollbacks, 105, 144, 456
root certificate authorities, 301
rootkits, 394
rounds in cryptography, 268
routers, 73, 361–363
routing databases, 362
routing tables, 361
RPO (recovery point objective), 164, 165, 241–242, 242
RSA (Rivest, Shamir, and Adleman) cryptosystem, 283–284
RTO (recovery time objective), 164, 241–242, 242
rules
  firewalls, 359–360
  incident response policies, 225

S
S/FTP cable, 324
S/KEY password system, 86
SaaS (Software as a Service), 112, 424, 436–437
Safe and Secure Online Program, 16
Safe Harbor Privacy Principles, 446
safe harbor regulations, 298
safeguards, 189
Safeguards Rule, 446
salt process in cryptography, 271
SAM (Security Accounts Manager) database, 411
sandbox testing, 140
sandboxes, 409–410
SANS Institute, 37
SAPs (special access programs), 89
Sarbanes-Oxley Act (SOX), 69
SAs (Security Associations), 307, 346
SAS (Serial Attached SCSI) host bus adapters, 454
SCA (Stored Communications Act), 447
scanning tools
  in information gathering, 199
  vulnerability, 406–407, 407
schedules
  anti-malware scans, 405
  risk treatment, 203–205, 204
SCI (sensitive compartmented information), 89
scope in incident response policies, 225
screen shielded twisted-pair cable, 324
screens and desktops for workstations, 416–418
screensavers, 417
script kiddies, 391
Scrum framework, 125
SDL (Security Development Lifecycle), 136–137
SDLC (System Development Lifecycle), 199
SDNs (software-defined networks), 451–455
search and seizure
  during investigations, 232
  training for, 425
searches in biometrics, 81
SEC (Security and Exchange Commission), 69
secondary authentication questions, 75, 76
secret classification, 88, 145
secret keys, 266
Secure Hash Algorithm (SHA-2) hash function, 289
secure protocols, 306–308
Secure Shell (SSH), 344–345
Secure Sockets Layer (SSL), 309, 340
Security Accounts Manager (SAM) database, 411
Security and Exchange Commission (SEC), 69
Security Associations (SAs), 307, 346
security awareness education programs, 52–53
security basics, 28
  AAA, 45, 46
  access control, 40–41
  Bring Your Own Device (BYOD) requirements, 51
  categories, 39–40
  CIA triad, 38–39, 38
  evolution, 31–33
  exam essentials, 55
  external users, 54
  geographic access control, 48
  human resources and stakeholders, 53
  implicit denies, 50
  job rotation policies, 48, 48
  M of N requirement, 46–47
  mandatory vacations, 46
  nonrepudiation, 42
  privacy, 49
  privileges, 51–52
  problems and opportunities, 29–31, 31
  prudent man, due diligence, and due care, 44
  review questions, 57–60
  risk, 42–43
  security awareness education programs, 52–53
  senior executives, 53
  separation of duties, 46
  standards, 34–37, 35
summary, 54–55
  techniques, 28–29
  terms and concepts, 29–37, 31, 35
  time of day control, 48
  transparency, 49–50
  two-man rule, 47
  user security management, 44–45
  written lab, 56
  security clearances, 88
  Security Development Lifecycle (SDL), 136–137
  security equation, 123
  security event information in incident response plans, 233
  Security Information and Event Management (SIEM) systems, 209, 233
  security kernels, 91
  security logs, 342
  security management software, 149
  security operations and administration domain, 121–122
    asset management, 142–143
    automated configuration management, 137–140
    business continuity plans. See business continuity plans (BCPs)
    change management, 142
    Common Body of Knowledge, 6–7
    concepts and principles, 122–123
    data management policies, 143–147
    disaster recovery plans. See disaster recovery plans (DRPs)
    education and awareness training, 150–157
    endpoint device management, 148–150
    exam essentials, 174–175
    implementation and release management, 141
    policies. See policies and practices review questions, 176–180
    SDL, 136–137
    security equation, 123
    summary, 173–174
    validating security controls, 143
    written lab, 175
  security operations center (SOC), 209–210, 210
  Security Parameter Index (SPI), 307
  security patches, 138
  Security principle in European Convention on Human Rights, 129
  segmentation, network, 351–355, 352, 354
  segregation of duties, 305
  senior executives, working with, 53
  sensitive compartmented information (SCI), 89
  sensors in wireless intrusion prevention systems, 366
  separate machines, privileged accounts for, 97
  separation of duties, 46, 94, 305
  Serial Attached SCSI (SAS) host bus adapters, 454
  server administrators, communicating monitoring results with, 216
  service packs, 139
  service set identifiers (SSIDs), 381
  session keys in cryptography, 269
  Session layer in OSI model, 328–329
  session-level access control, 104
  session tickets, 350
  severity levels
    incident response plans, 229
    syslog, 213
    SIEM (Security Information and Event Management) systems, 209, 233
  signal strength, 380
  signature-based detection, 365, 413
  signature dynamics, 82
  signature libraries, 365
  signatures
    asymmetric cryptography, 282, 283
    typing, 83
    viruses, 396
    simple integrity axiom (no read down), 92
    Simple Mail Transfer Protocol (SMTP), 338
    Simple Network Management Protocol (SNMP), 211–212, 339
    simple security property rule (no read up), 92–93
    simple trust relationships, 108–109
    simulation tests, 170, 253
    single-factor authentication, 84
    single loss expectancy (SLE), 196
    single-mode fiber-optic cable, 322
    single sign-on (SSO)
      description, 110
      overview, 350–351, 351
      terms and concepts, 32–33
    Six Sigma, 125
    skipjack algorithm, 294
    SLE (single loss expectancy), 196
slowing down attackers, 65
smart cards, 78
smart meters, 148
SmartScreen Filter, 492–493, 493
SMEs (subject matter experts), 198
SMTP (Simple Mail Transfer Protocol), 338
snapshots, 453, 456
SNMP (Simple Network Management Protocol), 211–212, 339
Snowden, Edward, 159
SOC (security operations center), 209–210, 210
social media platforms, training for, 151
Software as a Service (SaaS), 112, 424, 436–437
software-defined networks (SDNs), 451–455
software in trusted systems, 90
software key storage, 293
solid-state drives (SSDs), 441
something you are factor, 79–83, 79, 82
something you do factor, 82–83
something you have factor, 77–78, 78
something you know factor, 74–77, 76–77
Southbound APIs, 453
SP (Special Publications), 192–193, 199
spam filters, 368
spam management, 401–402
Spam over Instant Messaging (SPIM), 401
Spam over Internet Telephony (SPIT), 401
spear phishing attacks, 398–399
special access programs (SAPs), 89
Special Publication 800-88 revision 1, 421
Special Publications (SP), 192–193, 199
specialty certifications, 11
specialty security training, 53
speech recognition, 83
SPI (Security Parameter Index), 307
SPI (stateful packet inspection) firewalls, 358–359
SPIM (Spam over Instant Messaging), 401
SPIT (Spam over Internet Telephony), 401
split knowledge, 94, 305
spoliation of evidence, 448
spyware, 393
SQL injection, 396
SQL (Structured Query Language), 396
SSCP. See Systems Security Certified Practitioner (SSCP) certification
SSCP Applicant Endorsement Assistance Form, 9
SSDs (solid-state drives), 441
SSH (Secure Shell), 344–345
SSID (service set identifiers), 381
SSL (Secure Sockets Layer), 309, 340
SSO (single sign-on)
  description, 110
  overview, 350–351, 351
  terms and concepts, 32–33
stakeholders, working with, 53
standards
  event and incident handling policy, 225
  incident response policies, 225
ISO, 124–125, 191
  organizations, 36
  overview, 34–37, 35
  security policies, 131
star integrity axiom (no write up), 92–93
star property rule (no write down), 92
star topology, 332, 333
stateful packet inspection (SPI) firewalls, 358–359
stateless firewalls, 359
states
  data, 144
  security, 356–357
static routes, 362
stealth viruses, 397
steganography, 286, 287
stolen devices, 424–425
storage
  clusters in SDNs, 454–455
  keys, 305–306
storage-level encryption for cloud data, 442
Stored Communications Act (SCA), 447
STP (shielded twisted-pair cable) cable, 324
stream algorithms in cryptography, 271–272
stress techniques for exam, 24
striping, RAID, 251
strong passwords, 75
strong star rule, 92–93
Structured Query Language (SQL), 396
structured walk-through tests, 252–253
study time for exam, 18–20, 18–19
Stuxnet virus, 400–401
subject labeling, 145
subject matter experts (SMEs), 198
subjects in access controls, 66–67, 66
subnet masks, 353
subnetting, 352–353, 352
substantial alert level in incident response plans, 229
substitution in cryptography, 270
succession planning, 171–172
supply chain events, business continuity plans
for, 158
supporting security policies, 129–131
survival factors in business impact analyses, 162–163
switched virtual circuits (SVCs), 334
switches
in authentication, 73
networks, 363
OSI model, 326
symmetric cryptography, 32, 32, 266–267, 276–280, 277
synchronized one-time passwords, 85
synonyms for items, 33–34
Syskey (system key utility), 411
syslogs, 212–213
System Development Lifecycle (SDLC), 199
system key utility (Syskey), 411
system-level access controls, 86
systems security
data warehouse and big data environments, 449–451
exam essentials, 458
review questions, 460–463
software-defined networks, 451–455
summary, 457
virtualization, 455–457
written lab, 459
Systems Security Certified Practitioner (SSCP), 2, 4
Systems Security Certified Practitioner (SSCP) certification, 12
for advancement, 13
endorsement steps, 13–14
exam. See exam
information requirements, 13
on-the-job use of, 15–16, 16
maintaining, 14
objective, 12
positions, 12–13
as stepping stone, 14–15
tangible assets, 142, 185–186
Tavares, Stafford, 279
TCB (trusted computer base), 90–91
TCP (Transmission Control Protocol), 328, 328, 336–337
TCP/IP model vs. OSI, 321, 322
teams for incident response, 231–232
technical certifications, 11
technical controls, 189
telecommunications, remote access for, 368–369
Telecommunications Industry Association (TIA), 37
Telnet protocol, 339
temporal access control, 48
Temporal Key Integrity Protocol (TKIP), 372
Terminal Access Controller Access Control System (TACACS) environment, 347
terms and concepts
attacks, 393–401
business continuity plans, 241–242
cryptography, 263–272
incident response, 225
malicious code, 393–401
security basics, 29–37, 31, 35
single sign-on, 32–33
terrorism, business continuity plans for, 158–159
Tesla, Nikola, 35
testing DRPs and BCPs, 169–171, 252–253
testing exam engine, 24
TGC (Trusted Computing Group), 420
TGSs (ticket-granting servers), 292, 349
TGTs (ticket-granting tickets), 110, 303, 349–350
The Onion Router (TOR) network, 403, 444
theft in virtualization, 456
third-party connection policy, 130
threat analysis appliances, 409
threat intelligence, 210–211
threat vectors, 42–43
threats
actions, 392
risk, 42, 186–188
three-way handshakes, 328, 328
threshold of entry attempts setting in lockout policy, 99
throughput time in biometrics, 81
TIA (Telecommunications Industry Association), 37
ticket-granting servers (TGSs), 292, 349
ticket-granting tickets (TGTs), 110, 303, 349–350

T

 tabletop tests, 170
TACACS (Terminal Access Controller Access Control System) environment, 347
tight coupled clusters, 455

time limits in session-level access control, 104
time of day control, 48, 102
timelines in business impact analyses, 163, 164
TKIP (Temporal Key Integrity Protocol), 372
TLS (Transport Layer Security), 279, 309, 340
TLS Cipher Suite Registry, 295
token-based access control, 85–86, 85
token workstation access, 417
toll authority RFID devices, 77, 78
top secret classification, 87–89
topology models for networks, 330–334, 331–333
TOR (The Onion Router) network, 403, 444
total internal reflection in fiber-optic cable, 323
TP (twisted-pair) cable, 323–324, 325
TPM (Trusted Platform Module), 420–421
traffic patterns, 452
traffic shaping, 381

training
employees, 153–157
executives, 53, 156–157
management, 155–156
overview, 150–153
privacy, 299

privately owned devices, 424
security awareness programs, 52–53
transborder information flow in cloud, 444
transference in risk treatment, 203
transitive trust relationships, 109
Transmission Control Protocol (TCP), 328, 328, 336–337

transmission methods
backups, 250
OSI model, 325–326
transmitting cloud data, 440–441

transparency, 49–50

transport encryption, 271
Transport layer in OSI model, 328, 328
Transport Layer Security (TLS), 279, 309, 340
transport mode in IPsec, 307

transposition in cryptography, 269
transversal, directory, 395
travel devices, 425
treatment and treatment plans in risk management, 202–203
tree topology, 330, 331
trends in monitoring, 212–213

triage, event, 187

Triple Data Encryption (3DES), 32, 278
Trojan malware, 400
trust architectures, 108–111
trust levels in virtualization, 456
trusted computer base (TCB), 90–91
Trusted Computing Group (TGC), 420
trusted domains, 108
Trusted Platform Module (TPM), 420–421
trusted systems, 90–91, 91
tuning in incident response plans, 227
tunnel mode in IPsec, 307
tunneling protocols, 344–345
twisted-pair (TP) cable, 323–324, 325
Twitter feeds, 151
two-man rule, 47, 305
two-way algorithms in cryptography, 264
two-way trust relationships, 109

Twofish algorithm, 279
Type I errors in biometrics, 81
Type II errors in biometrics, 81
typing signatures, 83

U

UAT (user acceptance testing), 141
UDP (User Datagram Protocol), 328, 336–337
UMBRA compartment, 89
unclassified classification, 88
Unicode Consortium, 37
unintentional vulnerabilities, 188–189
United States military classification, 298
unofficial patches, 138
unshielded twisted-pair (UTP) cable, 324
updates
security policies, 135
software, 139
workstations, 415
upgrades, software, 139
user acceptance testing (UAT), 141
user accounts, 97–99
User Datagram Protocol (UDP), 328, 336–337
user entitlement, 97
user inactivity in session-level access control, 104
user threats
overview, 410–411
workstations, 411–415, 412
users
  authentication services, 348–350, 348
  security management, 44–45
  training, 154–155
utility events
  business continuity plans for, 158
  risk category, 185
UTP (unshielded twisted-pair) cable, 324

V

vacations, mandatory, 46
validating security controls, 143
VDI (virtual desktop infrastructure), 455–456
vectors, threat, 42–43, 187, 392
vendor-neutral certifications, 10
vendors
  certifications, 10
  cloud-based security, 112
  policies, 131
  working with, 54
version numbering for software, 139
VHS videotape recording standard, 35
videotape recording standards, 35
view-based access control, 104–105
violation warning screen, 100, 100
virtual appliances, 453
virtual circuit networks, 334
virtual desktop infrastructure (VDI), 455–456
virtual desktops, 423–424
virtual local area networks (VLANs), 353, 363
virtual private networks (VPNs), 130, 150,
  343–345, 344
virtual sites, 172
virtualization
  benefits, 455
  challenges, 456–457
  in cloud, 449
viruses, 73, 396–397
vishing attacks, 399
visual security filters, 417
visualization in monitoring, 214, 215
VLANs (virtual local area networks), 353, 363
VM escape attacks, 398
Voice over Internet Protocol (VoIP), 340
voice pattern recognition, 82–83
voicemail, 448

VoIP (Voice over Internet Protocol), 340
volatility of evidence, 237
volume storage encryption for cloud data, 442
VPNs (virtual private networks), 130, 150,
  343–345, 344
vulnerabilities in risk, 43, 188–189
vulnerability scanners, 406–407, 407

W

W3C (World Wide Web Consortium), 37
WAFs (web application firewalls), 359
wait period for lockout policy, 99
walk-through tests, 252–253
WAP (Wireless Application Protocol), 371
WAPs. See wireless access points (WAPs)
war, business continuity plans for, 158
wardalking, 378
wardriving, 378
warm sites, 172, 246
warnings
  incident response plans, 227
  syslog, 213
Warnock, John, 319
waterfall development process, 141
watermarks, 287
wearable devices, 431
weather events
  business continuity plans for, 158
  risk category, 185
web application firewalls (WAFs), 359
weight recognition, 80
well-known ports, 336–338
WEP (Wired Equivalent Privacy), 49–50, 371–372
whaling attacks, 398–399
what procedures in security policies, 133
when procedures in security policies, 133
where procedures in security policies, 133
white lists, 67, 360
who procedures in security policies, 133
Wi-Fi Alliance, 370
Wi-Fi Protected Access (WPA), 50, 371–373
wide area networks, 377
WiMAX Forum, 375–376
Windows Certificate Manager, 497–499, 499
Windows Performance Monitor, 500–502,
Windows XP operating system, 138
wiping process, 424
WIPSs (wireless intrusion prevention systems), 365–366
Wired Equivalent Privacy (WEP), 49–50, 371–372
wireless access points (WAPs)
  antenna placement, 379
  antenna types, 380–381
  IEEE standard, 373, 374
  OSI model, 322
  overview, 378–379
Wireless Application Protocol (WAP), 371
wireless intrusion prevention systems (WIPSs), 365–366
wireless LANs (WLANs), 377
wireless MANs (WMANs), 376
wireless networks
  attacks, 378
  technologies, 369–373
  types, 373–377, 374–375
  wireless access points, 378–381
wireless policy, 130
wireless radio transmissions, 322
wireless wide area networks (WWANs), 377
Wireshark packet sniffer, 405–406, 406
WLANs (wireless LANs), 377
WMANs (wireless MANs), 376
Work Factor in cryptography, 264, 372
worksheets, 23
workstations
  anonymous access, 414–415
  backups, 414
  email, 418–419
  encryption, 419–420
  hardening, 425
host-based firewalls, 419
malware protection, 413–414
passwords, 411–413, 412
patches and updates, 415
physical security, 416
screen and desktop, 416–418
  Trusted Platform Module, 420–421
World Wide Web Consortium (W3C), 37
worms, 393
WPA (Wi-Fi Protected Access), 50, 371–373
WPA2, 371–373
WWANs (wireless wide area networks), 377

X

X.509 version 3 format, 300
XOR (exclusive or) function in cryptography, 268–269, 271–272
XSS (Cross Site Scripting), 359, 395
XTACACS (extended TACACS), 347

Y

yagi antennas, 380
Yankee White program, 89

Z

zero-day attacks, 138, 401
zeroisation, 306
zombies, 393