

Enhanced Interior Gateway Routing
Protocol (EIGRP), 536
Enhanced Performance
Architecture (EPA), 627
Enigma machine, 320
ENISA (European Union Agency for
Cybersecurity), 106

enrollment in biometric authentication, 725
enterprise architecture frameworks
military-oriented, 195–196
models, 172–173
need for, 191–192
overview, 189–191
The Open Group Architecture Framework,
194–195
Zachman Framework, 192–194
enterprise security architecture
description, 13
vs. ISMS, 26
enterprise security program in business
continuity management, 106–108
entry points in physical security, 439–441
enumeration step in penetration testing, 824
environmental issues
business continuity planning, 1071
CPTED, 427–433
digital asset management, 262
disaster recovery, 1059
site and facilities, 461
Environmental Protection Agency (EPA), 434
EOL (end-of-life) of assets, 229
EOS (end-of-support) of assets, 229
EPA (Enhanced Performance
Architecture), 627
EPA (Environmental Protection Agency), 434
ephemeral keys in TLS, 604
ephemeral ports, 507
equipment malfunction in risk
management, 54
equipment warranty, 672
erasing media, 259
escrow, software, 1070, 1143
ESI (electronically stored information),
236–237
ESMTP (Extended SMTP), 622
ESP (Encapsulating Security
Payload), 608
ESTABLISHED state in TCP
connections, 951
Ethernet
data link layer, 481–482
layer 2 protocol, 494–495
local area networks, 499

Metro Ethernet, 539–540
Token Ring, 495–496

▲CISSP All-in-One Exam Guide

1274
ethics
professional, 44–46
vulnerability disclosures, 872
EULA (End User License Agreement), 153
European Union Agency for Cybersecurity (ENISA), 106
European Union Laws, 142–144
Evaluate, Direct and Monitor (EDM) domain in COBIT 2019, 189
evaluation
business impact analysis, 110–112
change management procedure, 891
framework steps, 201
program effectiveness, 43–44
Everything as a Service (XaaS), 304–305
evidence
acquiring, 1012
admissibility, 1013–1014
collecting, 1008–1012
identification guidelines, 1009–1010
incident investigations, 1006–1007
order of volatility, 1016
preserving, 1013
storage, 447–448
evolution of attacks, 134–138
evolutionary prototypes in software development, 1096
examination stage in forensics investigations, 1016–1017
exception handling, 871
executive succession planning, 1043
executive summaries in reports, 872–875
executives
incident notifications for, 1004
risk reporting for, 94–95
roles, 19–22
exercises for disaster recovery plans, 1061–1062
exigent circumstances, 1011
exploitation
Cyber Kill Chain model, 388, 994
penetration testing, 824
exploratory methodology in software development, 1104
exposure, defined, 9
exposure factor (EF), 74
extended detection and response (XDR) platforms, 968

- Extended SMTP (ESMTP), 622
- Extended TACACS (XTACACS), 790–791
- extended teams in incident response plans, 1000–1001
- Extensible Access Control Markup Language (XACML), 781
- Extensible Authentication Protocol (EAP) VPNs, 699
- WPA Enterprise, 577
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework, 501
- Extensible Markup Language (XML), 615, 777
- exterior lighting, 911–912
- exterior routing protocols, 536–537
- external audits, 842–843
- external labeling in digital asset management, 263
- external parties issues in data loss prevention, 267
- external perimeter security
 - bollards, 910–911
 - fencing, 908–910
 - lighting, 911–912
 - overview, 906–908
 - surveillance devices, 913
 - visual recording devices, 913–916
- extranets, 537–538
- Extreme Programming (XP), 1102

F

- Facebook breach, 20
- facial scans, 728
- Facilitated Risk Analysis Process (FRAP), 68
- facilities. See site and facility security
- facility safety officers, 434
- Factor Analysis of Information Risk (FAIR) framework, 172, 179
- factors in ISO/IEC 27004, defined, 852
- fail-safe devices, 931
- fail safe systems for locks, 921
- failed logon attempts, 721–723
- failing securely
 - network security, 598
 - secure design, 396–397
 - site and facility security, 422
 - third-party connectivity, 706
 - web services, 612

▲Index

failover capability in quality of service, 1051
Failure Modes and Effect Analysis (FMEA),
69–71
FAIR (Factor Analysis of Information Risk)
framework, 172, 179
fairness issue in forensics investigation
interviews, 1019
false acceptance rate (FAR) in biometric
authentication, 724–725
false negatives in anomaly-based IDS/IPS, 967
false positives in anomaly-based IDS/IPS, 967
false rejection rate (FRR) in biometric
authentication, 724–725
FAR (false acceptance rate) in biometric
authentication, 724–725
FAST (Federation Against Software Theft), 154
fault generation attacks on smart cards, 734
fault injection attacks in cryptography, 372
fault tolerance in availability, 1051
fault tree analysis in risk assessment, 71–72
FCoE (Fibre Channel over Ethernet) protocol,
628–629
FCS (frame check sequence) numbers in
WANs, 546
FDDI (Fiber Distributed Data Interface)
technology, 496–499
FDDI rings in MANs, 538
FDE (full-disk encryption), 407
FDM (frequency-division multiplexing), 544
FDMA (frequency division multiple
access), 584
Federal Copyright Act, 149–150
Federal Emergency Management Agency
(FEMA), 1054
Federal Information Processing Standard
(FIPS) 140-2, 406–407
Federal Risk and Authorization Management
Program (FedRAMP), 156, 1146
Federal Rules of Evidence (FRE), 1014
federated identity management (FIM) systems
overview, 752–754
with third-party service, 754–756
Federation Against Software Theft (FAST), 154
FedRAMP (Federal Risk and Authorization
Management Program), 156, 1146
Feistel, Horst, 332
FEMA (Federal Emergency Management
Agency), 1054

fencing, 908–910
FHSS (frequency hopping spread spectrum),
561–563
Fiber Distributed Data Interface (FDDI)
technology, 496–499

- fiber-optic cable, 650-651
- Fibre Channel over Ethernet (FCoE) protocol, 628-629
- field kits for digital forensics, 1015
- field of view in CCTV systems, 913, 915
- fifth-generation (5G) mobile wireless, 586-587
- fifth-generation programming languages, 1119-1120
- file descriptor attacks, 821
- file permissions, 821
- File Transfer Protocol (FTP)
 - application-level proxies, 954
 - sessions, 951
- filters
 - DNS, 621
- firewalls. See firewalls
- QKD, 344-345
- FIM (federated identity management)
 - systems
 - overview, 752-754
 - with third-party service, 754-756
- FIN-WAIT-1 state in TCP connections, 951
- FIN-WAIT-2 state in TCP connections, 951
- findings in reports, 873
- finances for executive management, 20
- fingerprint detection in antimalware software, 969
- fingerprints, 726
- FIPS (Federal Information Processing Standard) 140-2, 406-407
- fire codes for door placement, 440
- fire detection considerations, 438
- fire extinguishers, 455
- fire prevention, 454
- fire rating for cabling, 653
- fire resistance ratings, 456
- fire-resistant material, 439
- fire safety
 - detection, 454-457
 - overview, 454

▲CISSP All-in-One Exam Guide

- 1276
- fire sensors, 445
- fire suppression
 - considerations, 438
- fire types, 458-459
- heat-activated, 456-457
- overview, 454, 457-459
- smoke activated, 456

- water sprinklers, 459–460
- firewalls
 - appliances, 958
 - architecture, 959–965
 - bastion hosts, 965
 - comparisons, 958
 - configuring, 965–966
 - demilitarized zones, 945–946
 - dual-homed, 959
 - next-generation, 957–958
 - overview, 945–946
 - packet-filtering, 946–949
 - proxy, 952–957
 - screened host, 959–960
 - screened subnet, 960–962
 - stateful, 949–952
 - virtual, 964
- first-generation (1G) mobile wireless, 585–586
- first-generation programming languages, 1118
- five nines availability, 1050
- fixed focal length in CCTV systems, 914–915
- fixed mounting cameras in CCTV systems, 916
- floods, SYN, 508
- flooring considerations, 438
- fluorescent lighting interference, 450
- FMEA (Failure Modes and Effect Analysis), 69–71
- foams for fire suppression, 459
- focal length in CCTV systems, 914–915
- foot-candles
 - CCTV systems, 916
 - lighting, 911
- footprints of satellites, 589
- forensics. See digital forensics
- Forrester report, 1134
- forward secrecy in TLS, 604
- forwarding planes in SDNs, 633–634
- forwarding proxies, 663–664
- forwarding tables for bridges, 656–657
- Foundational controls, 187
- Fourth Amendment issues, 1011
- fourth-generation (4G) mobile wireless, 586–587
- fourth-generation programming languages, 1119–1120
- fractional T lines, 542
- fragmentation in firewalls, 948, 965–966
- frame check sequence (FCS) numbers in WANs, 546
- frame relay for WANs, 547–548, 552
- frames

- description, 483
- packets, 509
- TCP, 509
- Framework Core, 182–183
- Framework Profile in Cybersecurity
- Framework, 182
- frameworks
 - chapter questions, 205–209
 - chapter review, 203–205
- CIS controls, 185–187
- CMM, 197–199
- COBIT 2019, 187–189
- description, 15
- enterprise architecture, 189–196
- information security, 179–189
- ITIL, 196–197
- overview, 171–173
- process steps, 199–203
- risk, 172–179
- security controls, 183–189
- security programs, 180–183
- Six Sigma, 197
- framing risk, 57
- Franklin, Benjamin, 317
- FRAP (Facilitated Risk Analysis Process), 68
- fraud
- IP telephony, 692
- PBX systems, 666
- FRE (Federal Rules of Evidence), 1014
- free space transmission media, 644
- freeware, 153
- frequency analysis attacks in
 - cryptography, 370
- frequency division multiple
 - access (FDMA), 584
- frequency-division multiplexing (FDM), 544

▲Index

- 1277
- frequency hopping spread spectrum (FHSS),
561–563
- frequency in wireless signals, 559
- FRR (false rejection rate) in biometric
authentication, 724–725
- FTP (File Transfer Protocol)
 - application-level proxies, 954
 - sessions, 951
- full backups, 1035–1036
- full-disk encryption (FDE), 407
- full-duplex
- session layer, 478
- TCP, 508
- full-interruption tests in disaster recovery

- plans, 1064
- full knowledge in penetration testing, 825
- full RBAC, 773
- full tunnels in VPNs, 697
- functional analysis in BIA, 109
- functional model in software development design, 1084
- functional policies, 28
- functional requirements in software development, 1083
- fuzzing in application security testing, 1139-1140

G

- G.fast standard, 684
- gamification, 42-43
- garbage collectors in programming languages, 1122
- gas lines, 438
- gatekeepers in H.323, 689
- gates, 910
- gateways
 - characteristics, 665
- H.323, 689
- gauge for fencing, 909
- General Data Protection Regulation (GDPR)
 - compliance monitoring, 93
- entities, 143-144
- FIM systems, 754
- legal systems, 126
- privacy issues, 147, 158, 397
- general hierarchies in RBAC, 772
- General Personal Data Protection Law, 144
- Generalized Markup Language (GML), 776

- generators, 449-450
- Generic Routing Encapsulation (GRE), 606
- Geneva, Switzerland, QKD in, 346
- geosynchronous satellites, 588-590
- GET methods in HTTP, 614
- Get Out of Jail Free Cards, 824
- glare protection, 912
- glass in data processing facilities, 446
- Glenny, Misha, 939
- Global System for Mobile Communication (GSM), 584
- GML (Generalized Markup Language), 776
- goals
 - audits, 839
- disaster recovery, 1053-1054
- GOC domain in DNS, 527
- Gold Masters, 225
- Good Practice Guidelines (GPG), 105-106

- Goodman, Marc, 597
- Google trademark case, 150
- governance committees, 18
- Governance function in SAMM, 1109
- governance objectives in COBIT 2019, 189
- governance, risk, and compliance (GRC) programs, 155
- GPG (Good Practice Guidelines), 105–106
- grades of locks, 923
- Graham-Denning model, 402–403
- Gramm-Leach-Bliley Act, 141, 147
- gray box testing, 826
- GRC (governance, risk, and compliance) programs, 155
- GRE (Generic Routing Encapsulation), 606
- Gretzky, Wayne, 997
- groups for separation of duties, 394
- GSM (Global System for Mobile Communication), 584
- guaranteed service in QoS, 551
- Guaranteed Time Slot (GTS) reservations in WPANs, 570
- guards, 928–929
- guests in virtualized systems, 296
- guidelines
 - coding, 1136
 - overview, 32
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 142–144

▲CISSP All-in-One Exam Guide

- 1278
- H
- H.323 standard, 689
- HA (high availability), 1050–1053
- HaaS (Hacking as a Service), 135
- hacking mobile phones, 588
- hacktivists, 61
- Hadnagy, Chris, 902
- HAIPE (High Assurance Internet Protocol Encryptor), 609
- half-duplex mode in session layer, 478
- hand geometry, 727
- hand topography, 728–729
- handling evidence, 1008–1015
- handoffs in 802.11f standard, 574
- handouts for information access control, 801
- handshakes
- RADIUS, 789
- session keys, 350
- SIP, 689–690
- SSH, 700–701
- TCP, 508, 949–951

- TLS, 603
- hardware
 - backups in business continuity planning, 1069–1070
 - cryptography systems, 602
 - electrical power, 670–672
 - operation, 670–672
 - supply chain risk management, 98
 - tracking, 224
 - hardware guard in MAC, 770
 - hardware reverse engineering in cryptography, 371
 - hardware security modules (HSMs), 406–407
- Harrison-Ruzzo-Ullman (HRU) model, 402–404
- hash chaining, 831
- hash MAC (HMAC), 355, 358
- hashing functions
 - algorithms, 351–352
 - attacks against, 353
 - overview, 351
- passwords, 722
- HDLC (High-level Data Link Control)
 - frames, 550
- headers
 - IPv6, 513–514
 - TCP, 950–951

- Health Information Technology for Economic and Clinical Health (HI-TECH) Act, 141
- Health Insurance Portability and Accountability Act (HIPAA), 147
- hearsay evidence, 1014
- Heartbleed security bug, 257, 370
- heat-activated fire suppression, 456–457
- heating, ventilation, and air conditioning (HVAC)
 - considerations, 438
 - data processing facilities, 446
 - fire suppression, 459
 - overview, 453–454
- heavy timber construction material, 439
- heavyweight methods in software development, 1101
- Hellman, Martin, 337–340
- Hello messages in TLS, 603
- help desk tasks and responsibilities, 886
- heuristic detection in antimalware software, 969, 971
- hexadecimal values, 1121
- HI-TECH (Health Information Technology for Economic and Clinical Health) Act, 141
- hiding data in steganography, 264–265
- HIDSs (host-based intrusion detection

- systems), 967
- hierarchical RBAC, 772–773
- hierarchical storage management (HSM) for backups, 898–899
- High Assurance Internet Protocol Encryptor (HAIPE), 609
- high availability (HA), 1050–1053
- high coupling in software, 1131–1132
- High-level Data Link Control (HDLC) frames, 550
- high-level languages, 1118–1121
- high-performance computing (HPC) systems, 288–289
- high privacy risk in software development, 1082
- High-Speed Serial Interface (HSSI), 552
- Hinckley, Gordon B., 171
- hints for passwords, 720
- HIPAA (Health Insurance Portability and Accountability Act), 147
- hiring candidates, 35–36
- history of changes, documenting, 262

▲Index

1279

- HMAC (hash MAC), 355, 358
- HMI (human-machine interface), 291–294
- holistic risk management, 54–55
- hollow-core doors, 440
- home IP address in mobile IP, 793
- homomorphic encryption, 258
- honeyclients, 975
- honeynets, 975
- honeypots, 974–976
- hop devices, 601
- hop sequences in FHSS, 561–563
- Hopper, Grace, 851
- hopping attacks in VLANs, 632
- horizontal enactment for privacy, 147
- host addresses in IP addresses, 510
- host-based intrusion detection systems (HIDSs), 967
- hostage alarm feature for combination locks, 920
- HOSTS file in DNS, 528, 530
- hosts in virtualized systems, 296
- hot sites
 - disaster recovery, 1044–1046
 - vs. redundant sites, 1049
- hot washes
 - event debriefing, 869
 - lessons learned, 1061
- hotel key cards, 921

HPC (high-performance computing)
systems, 288–289
HR (human resources)
disasters, 1042–1043
proofing of identity, 739
HRU (Harrison-Ruzzo-Ullman) model,
402–404
HSM (hierarchical storage management)
for backups, 898–899
HSMs (hardware security modules), 406–407
HSSI (High-Speed Serial Interface), 552
HTML (Hypertext Markup Language),
776–777
HTTP (hypertext transfer protocol),
613–614
HTTPS (Hypertext Transfer Protocol
Secure), 614
hubs, 655–656
human interaction in risk management, 54
human-machine interface (HMI), 291–294

human resource managers on incident
response teams, 1001
human resources (HR)
disasters, 1042–1043
proofing of identity, 739
human sensors for incident detection, 995
human vulnerabilities, 902–903
humidity
data processing facilities, 446
HVAC systems, 453
hygrometers, 461
HVAC. See heating, ventilation, and air
conditioning (HVAC)
hybrid clouds, 305
hybrid controls in Risk Management
Framework, 175
hybrid data loss prevention, 274
hybrid encryption methods, 346
asymmetric and symmetric together,
346–349
session keys, 349–350
hybrid FIM systems, 756
hybrid flow in OIDS, 784
hybrid RBAC, 773
hybrid smart cards, 734
hybrid teams for incident response, 991
hygrometers, 461
Hypertext Markup Language (HTML),
776–777
hypertext transfer protocol (HTTP), 613–614
Hypertext Transfer Protocol
Secure (HTTPS), 614
hypervisors in virtual machines, 296–298

I

- IaaS (Infrastructure as a Service), 228, 302, 304
- IAM (identity and access management), 745
- ICMP. See Internet Control Message Protocol (ICMP)
- ICSs. See industrial control systems (ICSs)
- ICVs (Integrity Check Values), 501, 575–576
- IDaaS (Identity as a Service), 754
- IDC (International Data Corporation), 154
- identification, 214
 - authentication. See authentication
 - credential management, 736–745
 - crime scenes, 1009–1010

▲CISSP All-in-One Exam Guide

1280

- identification (cont.)
 - description, 716
 - directory services, 747–750
 - FIM systems, 752–754
 - forensics investigations, 1016–1017
 - identity management, 745–754
 - life cycle of assets, 222–223
 - proofing, 738–740
 - single sign-on, 750–752
- identify function in Framework Core, 182
- identities and access fundamentals
 - access control and markup languages, 776–781
- authorization. See authorization
- chapter questions, 759–763
- chapter review, 756–758
- overview, 715–717
- remote access control, 789–795
- identity and access management (IAM), 745
 - attribute-based access control, 774
- authorization. See authorization
 - chapter questions, 805–809
 - chapter review, 804–805
- discretionary access control, 766–768
- life cycle management, 795–800
- mandatory access control, 768–771
- overview, 765
- physical and logical access, 801–803
- provisioning life cycle, 795–800
- risk-based access control, 775–776
- role-based access control, 771–773
- rule-based access control, 774
- Identity as a Service (IDaaS), 754
- identity-based access control, 767
- identity management (IdM)

- directory roles, 748–750
- directory services, 747–748
- federated identity management systems, 752–754
- federated identity with third-party services, 754–756
- overview, 745–747
- single sign-on, 750–752
- identity providers (IdPs)
 - OpenID Connect, 783
 - SAML, 780
- identity repositories, 739
- identity stores, 748

- IDEs (integrated development environments)
 - in software development, 1137
- iDevIDs (initial device identities), 501
- IDFs (intermediate distribution facilities), 446–447
- IdPs (identity providers)
 - OpenID Connect, 783
 - SAML, 780
- IDSs. See intrusion detection systems (IDSs)
- IEC (International Electrotechnical Commission) 27000 Series, 180–182
- IETF (Internet Engineering Task Force) RFC 4987, SYN flood attacks, 508
- if this, then that (IFTTT) programming rules, 774
- IGMP (Internet Group Management Protocol), 500
- IGP (Interior Gateway Protocol), 533
- IGRP (Interior Gateway Routing Protocol), 536
- IGs (implementation groups) in CIS controls, 187
- IIoT (Industrial Internet of Things) devices, 570
- IKE (Internet Key Exchange), 608
- illogical processing, 62
- illumination in CCTV systems, 913, 916
- images
 - evidence, 1012–1013
 - system, 896
- IMAP (Internet Message Access Protocol), 623–624
- impact in incidents classification, 1002
- implementation
 - change management, 892
 - cybersecurity governance, 32–33
 - data loss prevention, 270–271
 - disaster recovery goals, 1054
 - frameworks, 200
 - Good Practice Guidelines, 106
 - Risk Management Framework, 175–176

- SAMM, 1109
- software, 1133
- implementation attacks in cryptography, 370–372
- implementation groups (IGs) in CIS controls, 187
- Implementation Tiers in Cybersecurity Framework, 182

▲Index

- 1281
- implicit denies in firewalls, 965
- implicit flow in OIDC, 784
- import/export controls for data breaches, 145–146
- IMPs (incident management policies), 990, 1000
- IMSI (International Mobile Subscriber Identity) catchers, 588
- in-rush current for electric power, 451
- inactivity, session termination from, 741
- incident assessment in site planning, 424
- incident investigations
 - chapter questions, 1024–1027
 - chapter review, 1022–1024
 - digital forensics, 1015–1022
 - evidence collection and handling, 1008–1015
 - law enforcement involvement, 1007
 - motive, opportunity, and means, 1007–1008
 - overview, 1006–1007
 - privacy issues, 1014
- incident management in business continuity, 1066
- incident management policies (IMPs), 990, 1000
- incident responders, tasks and responsibilities, 886
- incident response plans (IRPs)
 - classifications, 1002–1003
 - notifications, 1003–1004
 - operational tasks, 1004–1005
 - overview, 1000
 - roles and responsibilities, 1000–1002
 - runbooks, 1006
- incidents
 - classification, 1002–1003
 - Cyber Kill Chain framework, 994–995
 - detection, 995–996
 - investigations. See incident investigations
 - lessons learned, 999–1000
 - management overview, 989–994

- mitigating, 996–997
- notifications, 1003–1004
- operational tasks, 1004–1005
- overview, 989
- recovery, 998
- remediating, 999

- reporting, 997–998
- response plans, 1000–1006
- response teams, 991
- responses, 996
- runbooks, 1006
- supply chain risk management, 100
- incombustible material, 439
- income approach for executive summaries, 874
- incomplete level in CMMI, 1107
- incremental backups, 1036–1037
- Incremental software development, 1096–1097
- incremental testing for federated identity, 755
- indexing for data retention, 236
- indicators in ISO/IEC 27004, 852
- indicators of attack (IOAs), 999
- indicators of compromise (IOCs)
- incident remediation, 999
- threat data sources, 942
- Individual Participation Principle in OECD, 142
- industrial control systems (ICSs)
 - devices, 291–293
 - distributed control systems, 293
 - overview, 289–290
 - SCADA systems, 294
 - security, 294–295
- Industrial Internet of Things (IIoT)
 - devices, 570
 - industrial, scientific, and medical (ISM) bands, 565–566
 - industry standards, compliance with, 156–158
 - inference in database systems, 287
 - information disclosure category in STRIDE model, 388
- information security
 - access control, 801
 - bus encryption, 407–408
 - classification, 215–219
 - frameworks, 179–189
 - hardware security modules, 406–407
 - identification, 215–219
 - overview, 214, 404
 - secure processing, 408
 - self-encrypting drives, 407
 - trusted execution environments, 408–410
 - Trusted Platform Modules, 404–406

vulnerabilities, 59

▲CISSP All-in-One Exam Guide

1282

Information Security Continuous Monitoring (ISCM), 981–982

information security management systems (ISMSs)

commercial software certifications, 1146

description, 12

vs. enterprise security architecture, 26

ISO/IEC 27000 series, 180

security operations centers, 939

Information Systems Audit and Control

Association (ISACA), 187

information systems availability in business continuity planning, 1067–1070

information systems risk management (ISRM)

policies, 56

information systems view (Tier 3) in risk management, 55

Information Technology Infrastructure

Library (ITIL), 196–197

informational model in software development design, 1084

informative policies, 30

Infrastructure as a Service (IaaS),

228, 302, 304

infrastructure WLANs, 565

ingress filtering, 948

initial level in CMMI, 1107

initial device identities (iDevIDs), 501

initialization vectors (IVs)

802.11 standard, 575–576

symmetric key cryptography,
334–335

inputs, reviewing, 876–877

inside attacks in risk management, 54

installation stage in Cyber Kill Chain model,
388, 994

instantiation in object-oriented

programming, 1125

INT domain in DNS, 527

integrated development environments (IDEs)

in software development, 1137

integrated product teams (IPTs), 1105

Integrated Services Digital Network (ISDN),
685–686

integration issues in federated identity,
754–755

integration testing in software
development, 1091

- integrity
 - Biba model, 399
 - CIA triad, 8
 - in cryptography, hashing functions, 351–354
 - in cryptography, message verification, 354–358
 - in cryptography, overview, 351
 - cryptosystems, 323
 - overview, 5–6
 - Integrity Check Values (ICVs), 501, 575–576
 - integrity verification procedures (IVPs) in Clark-Wilson model, 400
 - Intel trade secrets theft, 149
 - intellectual property (IP)
 - data breaches, 139
 - internal protection, 152–153
 - requirements. See licensing and intellectual property requirements
 - intelligence cycle in threat intelligence, 941–942
 - intentional category in civil law, 127
 - interface testing, 837
 - interference
 - coaxial cable, 649
 - electric power, 450–451
 - twisted-pair cabling, 649–650
 - Interior Gateway Protocol (IGP), 533
 - Interior Gateway Routing Protocol (IGRP), 536
 - interior routing protocols, 535–536
 - intermediate distribution facilities (IDFs), 446–447
 - Intermediate System to Intermediate System (IS-IS), 536
 - internal actors, 61–62
 - internal audits, 840–842
 - internal labeling in digital asset management, 263
 - internal partitions, 442
 - internal protection of intellectual property, 152–153
 - internal security controls, 924
 - internal sources of threat data, 942–943
 - International Data Corporation (IDC), 154
 - International Electrotechnical Commission (IEC) 27000 Series, 180–182
 - international issues in cybercrimes, 138–139

▲Index

1283

- International Mobile Subscriber Identity (IMSI) catchers, 588

- International Organization for Standardization (ISO)
 - ISO 7498-1, 472
 - ISO 22301:2019, 105–106
 - ISO 28000:2007, 224
 - ISO/IEC 14443, 735
 - ISO/IEC 27000 series, 172, 180–182
 - ISO/IEC 27001, 1146
 - ISO/IEC 27004, 852
 - ISO/IEC 27005, 177–179
 - ISO/IEC 27031:2011, 105–106
 - ISO/IEC 27034, 1146
 - ISO/IEC 27037, 1009
- network reference model, 470
- Internet Control Message Protocol (ICMP)
 - attacks using, 520–522, 537
 - message types, 520–521
 - overview, 520
 - stateful firewalls, 952
- Internet Engineering Task Force (IETF) RFC 4987, SYN flood attacks, 508
- Internet Group Management Protocol (IGMP), 500
- Internet growth, increase of attacks from, 134
- Internet Key Exchange (IKE), 608
- Internet Message Access Protocol (IMAP), 623–624
- Internet of Things (IoT)
 - devices, 570
 - issues, 306–307
- Internet Protocol (IP)
 - addresses. See IP addresses
 - L2TP, 606–607
- Internet protocol networking
 - ARP, 515–517
 - DHCP, 517–519
 - DNS, 524–531
 - ICMP, 520–522
 - IP addresses, 510–515
 - NAT, 531–533
 - overview, 502–503
 - routing protocols, 533–537
 - SNMP, 522–524
 - TCP, 503–509
- Internet Protocol Security (IPSec)
 - transport adjacency, 609
 - VPNs, 607–609
- Internet Protocol telephony, 687–688
 - H.323, 689
 - issues, 692
 - SIP, 689–691
- Internet Security Association and Key Management Protocol (ISAKMP), 608

- Internet Small Computer Systems
- Interface (iSCSI), 629
- internetworks, 657
- interoperability
- data loss prevention, 270
- ISO/IEC 14443, 735
- interpreters, 1119–1122
- interviews in forensics investigations, 1018–1019
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 514
- intranets, 537–538
- intraorganizational configuration
- in SIP, 691
- intrasite tunneling mechanisms, 514
- intrusion detection systems (IDSs)
 - anomaly-based, 967–968
- audits, 743
- characteristics, 928
- dogs, 929
- overview, 925–928, 967
- patrol forces and guards, 928–929
- physical security, 908
- rule-based, 967
- whitelisting and blacklisting, 968–969
- intrusion prevention systems (IPSs)
 - anomaly-based, 967–968
 - overview, 967
 - rule-based, 967
 - whitelisting and blacklisting, 968–969
- inventories
 - data loss prevention, 267–268
 - digital asset management, 262
 - hardware, 224
 - software, 224–227
- investigations
- incidents. *See* incident investigations
- requirements, 161–162
- INVITE messages in SIP, 689–690
- invocation property in Biba model, 399
- IOAs (indicators of attack), 999

▲CISSP All-in-One Exam Guide

- 1284
- IOCs (indicators of compromise)
- incident remediation, 999
- threat data sources, 942
- IoT (Internet of Things)
 - devices, 570
 - issues, 306–307
- IP addresses

- DHCP, 501
- DNS, 524–531
- multicasting, 500
- NAT, 531–533
- overview, 510–512
- packet-filtering firewalls, 948
- three-way-handshake process, 951
- IP convergence, 628
- IP (intellectual property)
 - data breaches, 139
 - internal protection, 152–153
 - requirements. See licensing and intellectual property requirements
- IP (Internet Protocol)
 - addresses. See IP addresses
- L2TP, 606–607
- networking, 502–503
- IP version 4 (IPv4), 510
- IP version 6 (IPv6), 510, 512–514
- IPSec (Internet Protocol Security)
 - transport adjacency, 609
- VPNs, 607–609
- IPTs (integrated product teams), 1105
- IPv4 (IP version 4), 510
- IPv6 (IP version 6), 510, 512–514
- iris lenses in CCTV systems, 915–916
- iris scans, 727
- IRPs. See incident response plans (IRPs)
- IS-IS (Intermediate System to Intermediate System), 536
- ISACA (Information Systems Audit and Control Association), 187
- ISAKMP (Internet Security Association and Key Management Protocol), 608
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 514
- (ISC)2 Code of Ethics, 44–45
- ISCM (Information Security Continuous Monitoring), 981–982
- iSCSI (Internet Small Computer Systems Interface), 629

- ISDN (Integrated Services Digital Network), 685–686
- island-hopping attacks, 133
- ISM (industrial, scientific, and medical) bands, 565–566
- ISMSs. See information security management systems (ISMSs)
- ISO. See International Organization for Standardization (ISO)
- isochronous networks, 687
- isolation in ACID properties, 286
- ISRM (information systems risk management)

- policies, 56
- issue-specific policies, 28
- IT engineers, tasks and responsibilities, 886
- IT Governance Institute (ITGI), 187
- IT support specialists on incident response teams, 1001
- iterated tunneling in IPSec, 609
- ITGI (IT Governance Institute), 187
- ITIL (Information Technology Infrastructure Library), 196–197
- IVPs (integrity verification procedures) in Clark-Wilson model, 400
- IVs (initialization vectors)
 - 802.11 standard, 575–576
 - symmetric key cryptography, 334–335

J

- JAD (Joint Application Development), 1104–1105
- Java programming language, 1121–1122
 - bytecode, 1122–1123
 - protection mechanisms, 1123–1124
- Java Virtual Machine (JVM), 1122–1123
- JavaScript Object Notation (JSON), 615
- JavaScript programming language, 1121
- Jigsaw ransomware, 604
- JIT (just-in-time) access, 738
- jitter in IP telephony, 687–688
- job rotation, 34, 889–890
- Joint Application Development (JAD), 1104–1105
- journaling, remote, 1039
- JSON (JavaScript Object Notation), 615
- jumbograms in IPv6, 514
- jump boxes, 700

▲Index

- 1285
- jurisdiction in incident response, 993
- just-in-time (JIT) access, 738
- JVM (Java Virtual Machine), 1122–1123

K

- k-means clustering, 978
- k-nearest neighbors (KNN), 977
- Kanban development methodology, 1102–1103
- KBA (knowledge-based authentication)
 - description, 718
 - passwords, 720–723
- KDCs (Key Distribution Centers)
- Kerberos, 785–788

- PKI, 365
- Kelling, George L., 433
- Kerberos protocol
 - authentication process, 785–788
 - components, 785
 - key management, 365
 - overview, 784–785
 - passwords, 789
 - weaknesses, 788–789
- Kerckhoffs, Auguste, 324–325
- Kerckhoffs’ principle, 324–325
- kernel flaws in cryptography, 819
- key distillation in quantum cryptography, 344
- Key Distribution Centers (KDCs)
- Kerberos, 785–788
- PKI, 365
- key escrow in PKI, 366
- key exchange protocol in RSA, 340
- key management in PKI, 364–367
- key override feature for combination locks, 920
- key performance indicators (KPIs), 155, 856–857
- key risk indicators (KRIs), 855–857
- keycard entry systems, 442
- keys
 - asymmetric key cryptography, 335
 - cryptography, 322–323, 367–370
 - Diffie-Hellman algorithm, 337–338
 - hybrid methods, 347–348
 - RSA, 340–341
 - session, 349–350
 - symmetric key cryptography, 329
- TLS, 604
- ZigBee, 572
- keyspaces for cryptology, 322
- keystream generators in symmetric key cryptography, 333
- keystroke dynamics, 728
- kill chains in threat modeling, 386
- kill switches in VPNs, 697
- knowledge-based authentication (KBA)
 - description, 718
 - passwords, 720–723
- known-plaintext attacks in cryptography, 368
- Koolhaas, Rem, 417
- KPIs (key performance indicators), 155, 856–857
- KRIs (key risk indicators), 855–857

L

- L2F (Layer 2 Forwarding) protocol, 606

- L2TP (Layer 2 Tunneling Protocol), 606–607
- labels
 - digital asset management, 263
 - evidence, 1010
- IPv6, 514
- MAC, 768–769
- laminated windows, 441
- landscaping, 908
- language in reports, 871
- LANs. See local area networks (LANs)
- LAST-ACK state in TCP connections, 951
- last full backups, 1035–1036
- latency in cabling, 654
- law enforcement involvement in incident investigations, 1007
- laws and regulations
 - data breaches, European Union, 142–144
 - data breaches, U.S., 141–142
 - legal systems, 126–130
 - overview, 125–126
 - security programs, 434
- layer 2
 - local area networks, 494–499
 - security standards, 500–502
- Layer 2 Forwarding (L2F) protocol, 606
- Layer 2 Tunneling Protocol (L2TP), 606–607
- layer 3 and 4 switches, 659

▲CISSP All-in-One Exam Guide

- 1286
- layers
 - encryption, 600–601
- OSI reference model. See Open Systems Interconnection (OSI) reference model
- LDAP (Lightweight Directory Access Protocol), 747, 749
- LEAP (Lightweight Extensible Authentication Protocol), 580
- leased lines for WANs, 541–543
- least privilege principle
 - configuration management, 799
 - description, 888
- endpoint security, 673
- network security, 598
- overview, 394–395
- privileged accounts, 889
- site and facility security, 421
- software tracking, 225
- third parties, 705–706
- web services, 611
- least significant bits (LSBs) in

- steganography, 265
- LEDs (light-emitting diodes) in fiber-optic cable, 651
- legacy systems for federated identity, 755
- legal counsels in incident response teams, 1001
- legal departments, advice from, 157
- legal requirements
 - compliance, 156–158
- physical security programs, 434
- site planning, 427
- legal systems
 - civil law, 126, 129
 - common law, 126–130
 - customary law system, 128
 - mixed law system, 128–129
 - religious law system, 128
- legality issues in evidence admissibility, 1013–1014
- legally recognized obligations, 161
- Lei Geral de Proteção de Dados (LGPD), 144
- length of passwords, 720
- lenses in CCTV systems, 915–916
- LEO (low Earth orbit) satellites, 588–590
- lessons learned
 - disaster recovery plans, 1061
- incidents, 999–1000
- levels
 - classification, 216–219
- CMMI, 1107–1108
- programming languages, 1120
- LGPD (Lei Geral de Proteção de Dados), 144
- Li-Fi standard, 568
- liability
 - civil law, 129
 - compliance, 158–161
 - outsourced security services, 974
- libraries
 - object-oriented programming, 1129–1130
 - software, 1132–1133
- licensing and intellectual property requirements
 - copyrights, 149–150
- internal protection of intellectual property, 152–153
- overview, 147–148
- patents, 151–152
- software, 225–226
- software piracy, 153–154
- trade secrets, 148–149
- trademarks, 150
- life cycle
 - business continuity planning, 1065–1067

- cryptology, 328
- data. See data life cycle
- life cycle of assets
- decommissioning, 229–230
- inventories, 224–227
- overview, 222–223
- ownership, 223
- provisioning, 227–228
- retention, 228–230
- life safety goals in site planning, 423
- light detectors in fiber-optic cable, 651
- light-emitting diodes (LEDs) in fiber-optic cable, 651
- light frame construction material, 438
- light sources for fiber-optic cable, 651
- lighting
 - CCTV systems, 916
- EMI, 450
- photoelectric IDSs, 926–927
- physical security, 911–912
- Lightweight Directory Access Protocol (LDAP), 747, 749

▲Index

1287

- Lightweight Extensible Authentication Protocol (LEAP), 580
- lightweight methods in software development, 1101
- limited RBAC, 772–773
- Linder, Doug, 1117
- line conditioners for electric power, 451
- line noise
 - cabling, 652
- electric power, 450
- line-of-succession plans, 1043
- linear bus topology, 488
- link encryption vs. end-to-end encryption, 600–602
- link keys in ZigBee, 572
- link-state routing protocols, 535
- LISTEN state in TCP connections, 951
- LLC (Logical Link Control), 481–482
- loads, construction, 436
- local area networks (LANs)
 - Ethernet, 494–495
 - FDDI, 496–498
- medium access control, 489–494
- protocols summary, 498–499
- security standards, 500–502
- Token Ring, 495–496
- topologies, 487–490
- transmission methods, 499–500

- Local Security Authority Subsystem Service (LSASS), 372–374
- Locard, Edmond, 1020
- Locard's exchange principle, 1020–1021
- lock bumping, 924
- Lockheed Martin Cyber Kill Chain, 387–389
- locks
 - administrative responsibilities, 922
 - circumventing, 922–924
 - grades, 923
 - mechanical, 918–922
 - overview, 917–918
- Locky ransomware, 604
- logical access, 717, 801–803
- logical acquisition of evidence, 1012
- Logical Link Control (LLC), 481–482
- logon attempts, failed, 721–723
- logs
 - aggregating for microservices, 299
 - backups, 1039
- evidence, 1014
 - managing, 978–979
 - protecting, 744–745
 - requirements factor, 978–979
 - reviews, 828–831
- SIEM, 744, 979–980
- standards, 979
- tampering, 831
- Long-Term Evolution (LTE), 587
- loose coupling in software, 1131
- loosely coupled microservices, 299
- loss issues in risk management, 54, 63
- low coupling in software, 1131
- low Earth orbit (LEO) satellites, 588–590
- low privacy risk in software development, 1083
- LSASS (Local Security Authority Subsystem Service), 372–374
- LSBs (least significant bits)
 - in steganography, 265
- LTE (Long-Term Evolution), 587
- Lucifer project, 321
- lux values in CCTV systems, 916

M

- m of n control
 - description, 34
- PKI, 366–367
- MAC (mandatory access control) model
 - characteristics, 776
 - overview, 768–771
- MAC Security (MACSec) standard, 500–501
- machine language, 1118, 1121
- machine learning (ML), 977

- MACSec Security Entity (SecY), 501
- Madrid Agreement, 150
- magnetic tapes for backups, 860
- mail transfer agents (MTAs), 622
- mailbox data, backups for, 862
- main distribution facilities (MDFs), 446
- maintenance
 - CPTED, 433
 - data, 238
 - frameworks, 201
 - maintenance hooks in software development, 1091
- malicious code in advanced persistent threats, 136
- malicious insiders, 61

▲CISSP All-in-One Exam Guide

- 1288
- man-in-the-middle (MitM) attacks
 - cryptography, 374–375
 - data in motion, 59, 256
- Diffie-Hellman algorithm, 338–339
- managed level in CMMI, 1107
- managed security services providers (MSSPs), 973–974
- managed service accounts (MSAs), 800
- managed services in software security, 1148
- Management Frame Protection (MFP), 578
- Management Information Base (MIB) in SNMP, 522–524
- management objectives in COBIT 2019, 189
- management review and approval, 875–877
- managers, risk reporting for, 95
- mandatory access control (MAC) model
 - characteristics, 776
 - overview, 768–771
- mandatory vacations, 35, 890
- manmade threats in site planning, 423
- MANs (metropolitan area networks), 538–540
- mantraps, 441
- manual iris lenses in CCTV systems, 915
- manual penetration tests (MPTs), 1140
- manual tests in software development, 1091
- market approach in executive summaries, 874
- markup languages, 776–778
- Mary, Queen of Scots, 319
- masks in IP addresses, 511–512
- masquerading firewalls, 965
- master keying feature for combination locks, 920

- master keys in ZigBee, 572
- matrices
 - access control, 766–767
 - classification, 1002–1003
 - notification, 1003–1004
 - qualitative risk, 76–77
 - role, 799
- Mattermost service, 1057
- maturity models for risk, 96
- maturity software development models
 - CMMI, 1107–1109
 - overview, 1106
 - SAMM, 1109–1110
- MAUs (Multistation Access Units), 495
- maximum tolerable downtime (MTD)
 - BIA, 113–114
 - disaster recovery, 1030–1033
 - spare servers for, 672
- maximum tolerable period of disruption (MTPD), 113
- maximum transmission units (MTUs)
- MAC mechanisms, 489–494
 - routers, 661
- “McAfee 2019 Cloud Adoption and Risk Report,” 303
- McNulty, Paul, 125
- MCUs (multipoint control units)
 - in H.323, 689
- MD5 (Message Digest 5)
 - description, 352
 - passwords, 722
- MDFs (main distribution facilities), 446
- MEA (Monitor, Evaluate and Assess) domain
 - in COBIT 2019, 189
- means in criminal investigations, 1008
- measurements in ISO/IEC 27004, 852
- measuring security, 851
 - account management, 858–860
 - backup verification, 860–862
 - chapter questions, 879–881
 - chapter review, 877–879
 - disaster recovery and business continuity, 867–869
 - key performance and risk indicators, 855–857
 - management review and approval, 875–877
 - metrics, 852–855
 - process data overview, 857–858
 - quantifying, 851–853
 - reporting, 869–875
 - training, 863–867
- mechanical locks, 918–922

- Media Access Control (MAC) addresses
 - ARP, 515–517
 - bridges, 656
 - DHCP, 519
 - switches, 658–659
- Media Access Control (MAC) in data link layer, 481–482
- media for storage, 447

▲Index

- 1289
- medium access control (MAC)
 - collision and broadcast domains, 492–494
 - CSMA, 490–491
 - overview, 489–490
 - polling, 494
 - token passing, 491–492
- meeting applications, 694–695
- Meltdown attacks, 257, 372
- members in object-oriented programming, 1125
- memory cards in ownership-based authentication, 732–733
- memory for Trusted Platform Modules, 405–406
- mergers and acquisitions (M&A), 17
- mesh size for fencing, 909
- mesh topology for local area networks, 488–489
- message authentication code (MAC), 355–356, 603–604
- Message Digest 5 (MD5)
 - description, 352
 - passwords, 722
- message digests, 354–355
- messages
 - ICMP, 520–521
 - integrity verification, 354–358
 - object-oriented programming, 1127–1128
 - TCP, 509
- meta-directories, 748
- methodologies
 - description, 15
 - reports, 873
- methods in object-oriented programming, 1127
- Metro Ethernet, 539–540
- metropolitan area networks (MANs), 538–540
- Metropolitan Transit Authority (MTA), 433
- MFA (multifactor authentication)
 - strong authentication, 719

- VPNs, 697
- MFP (Management Frame Protection), 578
- MIB (Management Information Base) in SNMP, 522–524
- micro-segmentation, 629
- microcontrollers in embedded systems, 306

- microprobing attacks on smart cards, 735
- microservices, 299–301
- middle management, awareness
 - programs for, 42
- MIL domain in DNS, 527
- military-oriented architecture frameworks, 195–196
- Miller, Charlie, 627
- MIME (Multipurpose Internet Mail Extensions), 625–626
- MIMO (multiple input, multiple output)
 - standard, 567, 585
- Mirai botnet, 307
- mission/business process view (Tier 2) in risk management, 55
- mission critical data in disaster recovery, 1032
- misuse cases
 - data loss prevention, 271
 - testing, 835–836
- misuse of data in risk management, 54
- Mitchell, Joni, 213
- mitigation
 - incidents, 996–997
 - software security, 1144–1145
- mitigation risk strategy
 - ISO/IEC 27005, 178
- overview, 79
- MitM (man-in-the-middle) attacks
 - cryptography, 374–375
- data in motion, 59, 256
- Diffie-Hellman algorithm, 338–339
- MITRE corporation
 - ATT&CK framework, 389–390
 - Common Weakness Enumeration
 - initiative, 1088
- mixed law systems, 128–129
- ML (machine learning), 977
- MLS (multilevel security) systems
 - Bell-LaPadula, 398
 - description, 769
- MO (modus operandi) in criminal investigations, 1008
- mobile devices and communications
 - disaster recovery plans, 1062
 - endpoint security, 673–674
 - forensics investigations, 1021
 - generations, 585–587

hacking, 588

▲CISSP All-in-One Exam Guide

1290

mobile devices and communications (cont.)

multiple access technologies, 584-585

overview, 582-583

protecting, 220-221

mobile hot sites in disaster recovery, 1049

mobile IP, 793

Modbus system, 627

modems, cable, 686-687

moderate privacy risk in software development, 1082

modularity in object-oriented programming, 1127-1128

modus operandi (MO) in criminal investigations, 1008

MOM (motive, opportunity, and means) in incident investigations, 1007-1008

Monitor, Evaluate and Assess (MEA) domain in COBIT 2019, 189

monitoring

continuous, 981-982

egress, 981

frameworks, 201

ingress, 948

passwords, 721

Risk Management Framework, 176-177

UEBA, 981

monitoring risk

change, 92-93

compliance, 93-94

continuous improvement, 95-96

description, 58

effectiveness, 91-92

maturity models, 96

reporting, 94-95

monitors in Token Ring, 496

monoalphabetic substitution ciphers, 318

monoammonium phosphate for fire suppression, 458

motion detectors, 927

motive, opportunity, and means (MOM) in incident investigations, 1007-1008

MPLS (Multiprotocol Label Switching)

Metro Ethernet, 540

routing tags and labels, 659

MPTs (manual penetration tests), 1140

MSAs (managed service accounts), 800

MSSPs (managed security services providers), 973-974

- MTA (Metropolitan Transit Authority), 433
- MTAs (mail transfer agents), 622
- MTD (maximum tolerable downtime)
- BIA, 113–114
- disaster recovery, 1030–1033
- spare servers for, 672
- MTPD (maximum tolerable period of disruption), 113
- MTUs (maximum transmission units)
- MAC mechanisms, 489–494
- routers, 661
- multi-user MIMO (MU-MIMO) technology, 567–568
- multicast transmission method, 499
- multifactor authentication (MFA)
- strong authentication, 719
- VPNs, 697
- multihomed devices, 959
- multilayer protocols, 626–627
- multilayered switches, 658
- multilevel security (MLS) systems
- Bell-LaPadula, 398
- description, 769
- multimedia collaboration, 693–694
- meeting applications, 694–695
- unified communications, 695–696
- multimode fiber-optic cable, 651
- multiparty key recovery in PKI, 366
- multiple access technologies in mobile communications, 584–585
- multiple input, multiple output (MIMO) standard, 567, 585
- multiple processing sites in disasters recovery, 1049
- multiplexing functionalities, 544
- multipoint control units (MCUs) in H.323, 689
- Multiprotocol Label Switching (MPLS)
- Metro Ethernet, 540
- routing tags and labels, 659
- Multipurpose Internet Mail Extensions (MIME), 625–626
- Multistation Access Units (MAUs), 495
- muscle memory in disaster recovery, 1060
- mutual aid agreements in disasters recovery, 1047
- mutual authentication
- description, 719
- 802.11, 580

▲Index

1291

N

NAC (network access control)

- devices, 667-668
- importance, 697
- namespaces
- directory services, 747
- DNS, 525
- LDAP, 749
- Nappo, Stephane, 989
- NAS (network-attached storage) for backups, 1038
- NAT (network address translation), 512-513, 531-533
- nation-state actors, 60-61
- National Institute of Standards and Technology (NIST) Cybersecurity Framework, 182
- Digital Signature Standard, 357
- enterprise architecture frameworks, 190-191
- passwords, 720-721
- Risk Management Framework, 172-177
- SHA, 352
- SP 800-30, 67-68, 173
- SP 800-34, 104-105, 1059
- SP 800-37, 173
- SP 800-39, 55, 173
- SP 800-53, 172, 175, 183-185
- SP 800-57, 367
- SP 800-60, 174
- SP 800-63B, 720-721
- SP 800-82, 290, 294
- SP 800-88, 240
- SP 800-111, 255
- SP 800-137, 981-982
- SP 800-161, 97
- SP 800-190, 298-299
- National Security Agency (NSA) DES standard, 321
- HAIPE, 609
- natural access control in CPTED, 428-431
- natural environmental threats in site planning, 423
- natural languages, 1119-1120
- natural surveillance in CPTED, 431-432
- natural threats, 62
- naturalness in object-oriented programming, 1127
- NDA (nondisclosure agreements)
- incident response teams, 1001
- trade secrets, 148
- NDLP (network DLP), 272-273
- NDR (network detection and response)
- products
- forensics investigations, 1021

- HIDSs, 968
- security operations centers, 940
- Near Field Communication (NFC) with smart cards, 735
- near-line devices for backups, 898–899
- need-to-know principle
 - description, 394
 - overview, 888
- negligence
 - breaches from, 266
 - civil law category, 127
- negligent insiders, 61
- NET domain in DNS, 527
- network access control (NAC)
 - devices, 667–668
 - importance, 697
- network address translation (NAT), 512–513, 531–533
- network administrators, tasks and responsibilities, 886
- network-attached storage (NAS) for backups, 1038
- network-based intrusion detection systems (NIDSs), 967
- network components, 643
- CDNs, 674
- chapter questions, 677–679
- chapter review, 674–676
- devices. See network devices
- endpoint security, 673–674
- transmission media, 643–655
- network detection and response (NDR) products
 - forensics investigations, 1021
- HIDSs, 968
- security operations centers, 940
- network devices
 - bridges, 656–657
 - gateways, 662–663
 - hardware operation, 670–672
 - NACs, 667–668
 - network diagramming, 668–670

▲CISSP All-in-One Exam Guide

1292

- network devices (cont.)
 - overview, 655
- PBXs, 665–667
- proxy servers, 663–664
- repeaters, 655–656
- routers, 660–662
- switches, 657–660
- network DLP (NDLP), 272–273

- network forensics, 1021
- network keys in ZigBee, 572
- network layer
 - functions and protocols, 484
- OSI model, 480
- network reference models, 470–471
- network security
 - chapter questions, 638–641
 - chapter review, 635–638
 - design principles, 597–599
- DNS, 616–621
- e-mail, 621–626
- link encryption vs. end-to-end encryption, 600–602
- multilayer protocols, 626–627
- overview, 597
- protocol overview, 611
- segmentation. See network segmentation
- TLS, 602–605
- VPNs, 605–611
- web services, 611–616
- network segmentation
 - overview, 629
 - risk mitigation, 295
- SD-WANs, 635
- SDNs, 632–635
- VLANs, 630–632
- VxLANs, 632
- network sockets, 703
- Network Time Protocol (NTP), 829–830
- networking fundamentals
 - chapter questions, 555–558
 - chapter review, 552–555
- data communications. See data communications
- Internet protocol networking. See Internet protocol networking
- intranets and extranets, 537–538
- local area networks. See local area networks (LANs)
- networks (LANs)
 - MANs, 538–540
 - overview, 469
 - WANs, 540–552
 - networks
 - diagramming, 668–670
 - testing, 818
 - virtualized, 704–705
- New Zealand, Privacy Act in, 147
- newly observed domains (NODs) as threat data source, 943
- next-generation firewalls (NGFWs), 957–958
- NFC (Near Field Communication) with smart cards, 735

- NGFWs (next-generation firewalls), 957–958
- NIDSs (network-based intrusion detection systems), 967
- NIST. See National Institute of Standards and Technology (NIST)
- NMT (Nordic Mobile Telephone), 584
- NODs (newly observed domains) as threat data source, 943
- noise
 - cabling, 652
 - database systems, 288
 - digital transmission, 645
 - electric power, 450
 - non-symbolic AI approach, 976–978
 - nonces for one-time passwords, 731
- nondisasters
 - availability, 1049–1053
 - description, 1043
- nondisclosure agreements (NDAs)
- incident response teams, 1001
- trade secrets, 148
- nonfunctional requirements in software development, 1083
- noninterference model, 400–401, 403
- nonpersistent VDI, 701
- nonplenum cables, 653
- nonpracticing entities (NPEs), 152
- nonrecursive queries in DNS, 527
- nonrepudiation
 - cryptosystems, 324
 - overview, 6–7
- nonvolatile RAM (NVRAM) in Trusted Platform Modules, 405
- NORAD (North American Aerospace Defense Command), 436

▲Index

- 1293
- Nordic Mobile Telephone (NMT), 584
- normal changes, 892
- normal management in business continuity, 1066
- normalization in data retention, 236
- North American Aerospace Defense Command (NORAD), 436
- notifications for incidents, 1003–1004
- Novell Red color, 150
- NPEs (nonpracticing entities), 152
- NSA (National Security Agency)
- DES standard, 321
- HAIPE, 609
- NTP (Network Time Protocol), 829–830
- nuisance category in civil law, 127

NVRAM (nonvolatile RAM) in Trusted Platform Modules, 405

O

O&M (operation and maintenance) in life cycle of assets, 223

OASIS (Organization for the Advancement of Structured Information Standards), 781

OAuth standard, 782–783

Obama, Barack, 182

object-oriented programming (OOP)

abstraction, 1129

benefits, 1127

classes and objects, 1125–1127

encapsulation, 1130

libraries, 1129–1130

messages, 1127–1128

overview, 1124–1125

vs. procedural programming,
1125–1126

relationships, 1128

objectives in Spiral methodology, 1098

objectivity in forensics investigation
interviews, 1019

objects in ABAC, 774

obligations, legally recognized, 161

occupant emergency plans (OEPs), 931

Occupational Safety and Health
Administration (OSHA), 434

OceanLotus attack, 389–390

OCs (optical carriers) for WANs, 543

OCSP (Online Certificate Status
Protocol), 362

OCTAVE (Operationally Critical Threat,
Asset, and Vulnerability Evaluation)
framework, 68, 172, 178–179

OECD (Organisation for Economic
Co-operation and Development), 142–144

OEMs (original equipment manufacturers), 229

OEPs (occupant emergency plans), 931

OFDM (orthogonal frequency division
multiplexing), 561, 563–564

OFDMA (orthogonal frequency division
multiple access), 585

Office of Management and Budget,
“Safeguarding Against and Responding
to the Breach of Personally Identifiable
Information,” 140

offline media for backups, 1038

offsite backups, 1037

offsite locations in disasters recovery, 1047

OIDC (OpenID Connect), 783–784

on-premise FIM systems, 755–756

- onboarding personnel security, 37-38
- ONC (Open Network Computing), 703
- one-time pads in cryptology, 325-328
- one-time passwords (OTPs), 729-732
- one-to-many identification, 718
- one-to-one identification, 718
- one-way hashing functions, attacks against, 353-354
- one-way RSA functions, 341-342
- ONF (Open Networking Foundation), 634-635
- online backups, 1035
- Online Certificate Status Protocol (OCSP), 362
- online encryption vs. end-to-end encryption, 600-602
- online safety, 866-867
- online UPS systems, 452-453
- onsite backups, 1037
- Ontario Information Commissioner, 397
- OOP. See object-oriented programming (OOP)
- open message format in asymmetric key cryptography, 336
- open network architectures, 472
- Open Network Computing (ONC), 703
- Open Networking Foundation (ONF), 634-635
- open proxies, 663

▲CISSP All-in-One Exam Guide

- 1294
- Open Shortest Path First (OSPF) protocol, 535-536
- open-source intelligence (OSINT)
- social engineering, 903
- threat data sources, 942
- open-source software, securing, 1146-1147
- open system authentication (OSA), 575
- open systems, 474
- Open Systems Interconnection (OSI)
- reference model, 470-471, 648
 - application layer, 474-475
 - attacks, 474
 - data link layer, 480-483
 - functions and protocols, 483-485
 - layers together, 485-487
 - network layer, 480
 - physical layer, 483
 - presentation layer, 475-476
 - protocols, 471-474
 - session layer, 477-478

- transport layer, 479–480
- open trust model in ZigBee, 572
- Open Web Application Security Project (OWASP)
- SAMM, 1109–1110
- Threat Dragon, 1087
- web applications, 1134–1135
- OpenFlow interface, 634–635
- OpenID Connect (OIDC), 783–784
- Openness Principle in OECD, 142
- operate steps in frameworks, 201
- operation and maintenance (O&M) in life cycle of assets, 223
- operational prototypes in software development, 1096
- operational tasks in incident handling, 1004–1005
- operational technology (OT), 290, 292–293, 295
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework, 68, 172, 178–179
- operations and maintenance phase
 - change control, 1092–1094
 - change management, 1092
- SDLC, 1080, 1091–1094

- Operations function in SAMM, 1109
- operations management. See security operations; security operations management
- opportunity in criminal investigations, 1008
- optical carriers (OCs) for WANs, 543
- optical discs for logs, 745
- optical fiber
 - fiber-optic cable, 651
 - transmission media, 643
- optical zoom in CCTV systems, 915
- optimizing level in CMMI, 1108
- orchestration in SOAR, 980
- order of volatility for evidence, 1016
- ORG domain in DNS, 527
- Organisation for Economic Co-operation and Development (OECD), 142–144
- Organization for the Advancement of Structured Information Standards (OASIS), 781
- organization view (Tier 1) in risk management, 55
- organizational change, data loss prevention in, 270
- organizational CIS controls, 187
- organizational code of ethics, 45
- organizational processes, 17–18
- organizational roles and responsibilities, 18–19

- auditors, 25
- change control analysts, 24
- data analysts, 24
- data custodians, 23
- data owners, 22–23
- executive management, 19–22
- security administrators, 24
- system owners, 23–24
- users, 25
- organizational security policies, 27–29
- organizational units (OUs) in LDAP, 749
- organized cybercrime gangs, 134
- organizing steps for frameworks, 200
- original equipment manufacturers (OEMs), 229
- orthogonal frequency division multiple access (OFDMA), 585
- orthogonal frequency division multiplexing (OFDM), 561, 563–564
- OSA (open system authentication), 575
- OSHA (Occupational Safety and Health Administration), 434

▲Index

1295

OSI model. See Open Systems Interconnection (OSI) reference model

OSINT (open-source intelligence)

social engineering, 903

threat data sources, 942

OSPF (Open Shortest Path First) protocol, 535–536

OT (operational technology), 290, 292–293, 295

OTPs (one-time passwords), 729–732

OUs (organizational units) in LDAP, 749

out-of-band method in symmetric key cryptography, 330

outside attacks in risk management, 54

outsourced security services, 973–974

outsourced software, 1147

outsourcing business continuity planning, 1068

overflows

description, 819

software development, 1089–1090

overlays in SDNs, 635

overwriting

data, 243

media, 259–260

OWASP (Open Web Application Security Project)

SAMM, 1109–1110

Threat Dragon, 1087

web applications, 1134–1135

owners

assets, 223

data, 244

OAuth, 782

risk reporting for, 95

ownership-based authentication

cryptographic keys, 732

memory cards, 732–733

one-time passwords, 729–732

overview, 729

smart cards, 733–735

P

PaaS (Platform as a Service), 228, 302–304

PACE (Primary, Alternate, Contingency, and Emergency) communications plans, 1057

package supplies in forensics field kits, 1015

packet-filtering firewalls, 946–949

packet jitter, 681

packet switching in WANs, 546–547

packets

firewalls, 945

TCP, 509

TCP vs. UDP, 506

Padding Oracle On Downgraded Legacy

Encryption (POODLE) attacks, 602

padlocks, 917

pair programming in Extreme

Programming, 1102

palm scans, 727

PAM (privileged account management), 889

pan, tilt, or zoom (PTZ) capabilities in CCTV systems, 916

panic bars, 440

panic buttons, 931

PanOptis lawsuit, 151

PAP (Password Authentication Protocol), 697–698

paper records, protecting, 221

parallel tests in disaster recovery plans, 1064

parameter validations in APIs, 1132

Pareto principle, 179

Paris Convention, 150

partial knowledge in penetration

testing, 825

partitions

database systems, 288

physical security, 442

pass the hash attacks, 372

passive infrared (PIR) IDSs, 927

passive patch management, 904

passive relocking function for safes, 222

- Password Authentication Protocol (PAP), 697–698
- password-guessing attacks, 789
- password managers, 736–737
- passwords
 - checkers, 722
 - cognitive, 723
 - failed logon attempts, 721–723
 - hashing and encrypting, 722
 - Kerberos protocol, 789
 - knowledge-based authentication, 720
 - one-time, 729–732
 - passphrases, 723
- PBX systems, 666

▲CISSP All-in-One Exam Guide

- 1296
- passwords (cont.)
- policies, 720–722
- resets, 737–738
- synchronization, 737
- TACACS, 791
- vulnerabilities, 60
- PAT (port address translation), 532
- patch management, 903
 - centralized, 904–905
 - reverse engineering patches, 905
 - unmanaged patching, 904
- patent trolls, 152
- patents, 151–152
- paths in URLs, 614
- patrol forces, 928–929
- payloads
 - IPv6, 514
 - steganography, 265
- PBXs (Private Branch Exchanges), 665–667
- PCI DSS (Payment Card Industry Data Security Standard), 156
- PCRs (platform configuration registers) in Trusted Platform Modules, 406
- PDC (Personal Digital Cellular), 584
- PDPA (Personal Data Protection Act), 144
- PDU (protocol data units)
 - description, 473
- TCP, 509
- PEAP (Protected EAP), 580
- peer-to-peer systems, 307
- Peltier, Thomas, 68
- penetration tests
 - application security, 1140
 - knowledge of targets, 825–826
 - overview, 822–824
 - process, 824–825

- red team exercises, 902
- software development, 1090
- vs. vulnerability tests, 826–827
- people as vulnerabilities, 60
- perfect forward secrecy in TLS, 604
- performance-based approach in site planning, 424
- performance metrics, 854
- Perimeter Intrusion Detection and Assessment System (PIDAS), 910
- perimeter security, 803
- periodic content reviews, 43

- peripheral switch controls for device locks, 921
- Perl programming language, 1121
- permanent teams for incident response, 991
- permanent virtual circuits (PVCs), 549
- permissions
 - DAC, 767
 - setting, 739
 - testing, 821
- persistent memory in Trusted Platform Modules, 405
- persistent VDI, 701
- Personal Data Protection Act (PDPA), 144
- Personal Digital Cellular (PDC), 584
- personal health information (PHI)
 - breaches, 255
- Personal Information Protection and Electronic Documents Act, 147
- personal liability of executive management, 20
- personally identifiable information (PII)
 - components, 140–141
 - U.S. laws, 141
- personnel
 - disaster recovery plans, 1055–1056
 - testing, 818
 - safety and security
 - access controls, 924–925
 - breaches from, 266
 - candidate screening and hiring, 35–36
 - compliance policies, 39–40
 - duress, 931–932
 - emergency management, 931
 - employment agreements and policies, 36–37
 - incident response, 993
 - onboarding, transfers, and termination processes, 37–38
 - overview, 33–35, 929–930
 - privacy policies, 40
 - threats, 138
 - training and awareness, 930–931

- travel, 930
- vendors, consultants, and contractors, 39
- perturbation in database systems, 288
- pervasive systems
 - embedded, 306
- Internet of Things, 306–307
- overview, 305

▲Index

- 1297
- Petya ransomware, 604
- PGP (Pretty Good Privacy), 367
- PHI (personal health information)
 - breaches, 255
- phishing awareness programs, 42, 864–865
- phone calls in PBXs, 665–667
- photoelectric IDS systems, 926–927
- phreakers, 666
- physical damage in risk management, 54
- physical destruction of data, 244
- physical layer
 - functions and protocols, 485
- OSI model, 483
- physical security and controls
 - auditing, 929
 - data loss prevention, 269
 - devices, 802
 - digital asset management, 261
 - external perimeter, 906–916
 - facilities, 802–803, 916–924
 - information access, 801
 - internal controls, 924
 - intrusion detection systems, 925–929
 - mobile devices, 220–221
 - overview, 220, 801, 906
 - paper records, 221
 - personnel access controls, 924–925
 - risk responses, 83–84, 86–87
 - safes, 221–222
 - physical security programs
 - construction, 436–439
 - design overview, 433–435
 - entry points, 439–441
 - facilities, 435–436
 - physical surveillance in digital forensics, 1019–1020
 - physical testing, 818
 - physiological biometric authentication, 724
- PIDAS (Perimeter Intrusion Detection and Assessment System), 910
- piggybacking, 925
- PII (personally identifiable information)
 - components, 140–141

- U.S. laws, 141
- pin tumbler locks, 918
- PINs
 - memory cards, 732
 - smart cards, 733
- PIR (passive infrared) IDSs, 927
- piracy, software, 153-154
- pirated software, dangers in, 225
- PKCS (Public Key Cryptography Standards), 626
- PKI. See public key infrastructure (PKI)
- plaintext, 321
- Plan-Do-Check-Act loop, 875
- plans
 - audits, 839
 - backups, 863
 - business continuity, 104-105
 - change management, 891
 - forensics investigation interviews, 1019
 - frameworks, 200
 - incident response, 1000-1006
- OEPs, 931
- Plan-Do-Check-Act loop, 875
- Spiral methodology, 1098
- Platform as a Service (PaaS), 228, 302-304
- platform configuration registers (PCRs) in Trusted Platform Modules, 406
- platforms for secure software, 1137-1138
- PLCs (programmable logic controllers), 290-291
- plenum areas
 - cabling, 653
 - fire suppression, 459
- PMs (project managers) in software development, 1080
- point-to-point links in WANs, 541-543
- Point-to-Point Tunneling Protocol (PPTP), 606
- poisoning of ARP cache tables, 516-517
- polarized filters in QKD, 344-345
- policies
 - acceptable use, 226, 664, 858
 - compliance, 39-40
 - data retention, 234-236
 - employment, 36-37
- IMPs, 990, 1000
- passwords, 720-722
- privacy, 40
- security, 27-29
- security operations centers, 940
- types, 30

1298

Policy and Program Management

practice, 105

policy engines for data loss prevention, 270

polling, MAC, 494

polyalphabetic substitution ciphers, 318–320

polyvinyl chloride (PVC) jacket covering, 653

POODLE (Padding Oracle On Downgraded

Legacy Encryption) attacks, 602

POP (Post Office Protocol), 623

port address translation (PAT), 532

portable code, 1122

portable fire extinguishers, 455

portals, TLS, 610

portlets for web portal functions, 753–754

ports

device locks, 921

packet-filtering firewalls, 948

TCP, 504

three-way-handshake process, 951

types, 507

positive drains, 448

POST methods in HTTP, 614

Post Office Protocol (POP), 623

powders for fire suppression, 458

power, electrical. See electric power

power supplies

considerations, 438

data processing facilities, 446

PP (Professional Practices) in Good Practice Guidelines, 105–106

PPTP (Point-to-Point Tunneling Protocol), 606

preaction water sprinkler systems, 460

prediction with artificial intelligence

tools, 977

prefabricated buildings in disasters

recovery, 1049

preparation step

Risk Management Framework, 174

software vulnerability scans, 901

preparedness metrics, 855

presence information in unified

communications, 695

presentation layer

functions and protocols, 483–484

OSI model, 475–476

presentation stage in forensics investigations, 1016–1018

preservation

- evidence, 1013
- forensics investigations, 1016–1017
- preset locks, 917
- presheared keys (PSKs) in 802.11 standard, 575
- pressurized conduits for cabling, 653
- pretexting, 865
- Pretty Good Privacy (PGP), 367
- preventive and detective measures
 - anomaly-based intrusion detection and prevention, 967–968
 - antimalware software, 969–972
 - artificial intelligence tools, 976–978
 - firewalls. See firewalls
 - intrusion detection and prevention systems
 - overview, 967
 - outsourced security services, 973–974
 - process, 944–945
 - vs. recovery strategies, 1033
 - rule-based intrusion detection and prevention, 967
 - sandboxes, 972–973
 - whitelisting and blacklisting, 968–969
- preventive controls
 - business continuity, 104–105
 - risk responses, 85–87
- PRI (Primary Rate Interface) ISDN, 685–686
- Primary, Alternate, Contingency, and Emergency (PACE) communications plans, 1057
- primary category in PACE plans, 1057
- primary images for evidence, 1012
- Primary Rate Interface (PRI) ISDN, 685–686
- principals in KDC, 785
- principle of least privilege. See least privilege
- principle
- principles in SAML, 780
- priorities in disaster recovery goals, 1054
- privacy
 - classification level, 216–217
 - compliance issues, 147
 - control assessments, 90–91
 - data loss prevention, 270
 - incident investigations, 1014
 - policies, 40
 - requirements, 158
 - retina scan issues, 727
 - SDLC assessments, 1082
 - vs. security, 21

▲Index

1299

- privacy by design, 397
- network security, 599

- site and facility security, 423
- third-party connectivity, 706
- web services, 612
- Privacy by Design: Delivering the Promises report, 397
- Private Branch Exchanges (PBXs), 665-667
- private clouds, 301, 305
- private keys
 - asymmetric key cryptography, 335
 - hybrid methods, 347
 - RSA, 340-341
- private portions in objects, 1128
- privilege escalation
 - identity and access, 799-800
 - software development, 1089
- privileged account management (PAM), 889
- PRNGs (pseudorandom number generators), 327, 370
- proactive searching in threat hunting, 943
- probationary periods in employment, 37
- procedural programming vs. object-oriented programming, 1125-1126
- procedures, 32
- process enhancement, 16
- process reengineering, 16
- processes
 - organizational, 17-18
 - race conditions, 717
 - vulnerabilities, 59-60, 902
- processing speed in biometric authentication, 726
- processors
 - data, 244-245
 - security extensions, 410
- professional ethics, 44-46
- Professional Practices for Business Continuity Management, 106
- Professional Practices (PP) in Good Practice Guidelines, 105-106
- profile updates, 740
- program effectiveness evaluation, 43-44
- programmable locks, 920
- programmable logic controllers (PLCs), 290-291
- programming languages and concepts.
 - See also software development
 - assemblers, compilers, and interpreters, 1120-1122
 - levels, 1120
 - object-oriented programming, 1124-1130

- overview, 1117-1120
- runtime environments, 1122-1124
- Project Athena, 784
- project management in SDLC, 1081
- project managers (PMs) in software development, 1080
- project sizing factor in risk assessment, 64
- proofing of identity, 738-740
- protect function in Framework Core, 182
- Protected EAP (PEAP), 580
- protocol data units (PDUs)
 - description, 473
- TCP, 509
- prototypes in software development, 1096
- provisioning
 - assets, 227-228
 - configuration management, 894-895
 - identity and access, 796
 - users, 739
- Provisioning Service Provider (PSP)
 - in SPML, 778
- Provisioning Service Target (PST)
 - in SPML, 778
- proximate causes, 161
- proximity detectors, 927
- proxy firewalls
 - application-level, 954-955, 957
 - circuit-level, 954-956
 - overview, 952-953
- proxy servers
 - characteristics, 665
 - overview, 663-664
- SIP, 690
- pseudorandom number generators (PRNGs), 327, 370
- PSKs (preshared keys) in 802.11
 - standard, 575
- PSP (Provisioning Service Provider)
 - in SPML, 778
- PST (Provisioning Service Target)
 - in SPML, 778

▲CISSP All-in-One Exam Guide

- 1300
- PSTNs (public switched telephone networks), 582-583, 682-683
- PTZ (pan, tilt, or zoom) capabilities in CCTV systems, 916
- public algorithms vs. secret, 369
- public classification level, 216-217
- public clouds, 301, 305
- public disclosure in incident response, 993
- public key cryptography, 328