

# Index

## • A •

- AAA (authentication, authorization, and accountability), 52, 523
- ABCP (Associate Business Continuity Professional), 460
- abstraction, 114, 523
- ACCA (Adaptive Chosen Ciphertext Attack), 207
- access control, 49, 91, 223, 346, 350–352, 523
- Access Control domain
  - concepts of, 46–47
  - data access controls, 78–82
  - defined, 523
  - evaluating, 83–84
  - models, 350–352
  - overview, 19–20, 45–46, 439–440
  - services, 50–51
  - system access controls, 71–78
  - testing, 83–84
  - types of controls, 47–50
- access control list (ACL), 49, 523
- access logs, 332
- Access Matrix model, 82, 351, 523
- access points (APs), 412–413
- accountability, 51, 113, 354, 440, 523
- accreditation, 224, 358–359, 523
- accreditation step, SDLC, 109
- active IDS, 406, 455
- active monitor, 379
- ActiveX, 92–93, 120–121
- ad hoc, 413
- Adaptive Chosen Ciphertext Attack (ACCA), 207
- Adaptive Chosen Plaintext Attack (ACPA), 207
- Address Resolution Protocol (ARP), 380, 387, 523
- address space, 342, 523
- administrative controls, 48–49, 297, 331–332, 523
- administrative law, 248, 447, 524
- administrative management and control, 283–290
- admissibility of evidence, 273
- Advanced Encryption Standard (AES), 49, 190, 524
- Advisory policy, 222, 446
- adware, 524
- agents, 91–92, 406, 440, 524
- aggregation, 97, 440, 524
- aging, password, 56
- AH (Authentication Header) protocol, 204, 411, 525
- alarms, 326
- American Society for Industrial Security (ASIS) International, 457–458
- American Standard Code for Information Interchange (ASCII), 397
- analog signaling, 367
- analytic attack, 206
- annual maintenance fee (AMF), 29
- Annualized Loss Expectancy (ALE), 232, 445, 524
- Annualized Rate of Occurrence (ARO), 233, 524
- anomaly-based IDS, 304
- ANSI (American National Standards Institute), 10, 524
- antennas, wireless, 412–413
- Anti-Phishing Work Group, 126
- antivirus software, 119, 128–130, 524
- applets, 92–94, 120–121, 524
- Application Development Security domain
  - antivirus software, 128–130
  - application security controls, 112–116
  - attack methods, 117–128
  - databases, 96–102
  - distributed applications, 89–94
  - knowledge-based systems, 102–103
  - object-oriented environments, 94–96
  - overview, 20, 440–442
  - perpetrators, 130–131
  - systems development life cycle, 103–112
- Application Layer, 398–400

- application response times, 116
  - application scan, 83, 525
  - application security controls, 112–116
  - application software, 524
  - application-level firewall, 403, 525
  - APs (access points), 412–413
  - archive, 199, 525
  - ARCnet protocol, 379
  - ARO (Annualized Rate of Occurrence), 233, 524
  - ARP (Address Resolution Protocol), 380, 387, 523
  - artificial intelligence, 102–103
  - AS (Authentication Service), KDC, 66
  - AS (autonomous system), 390
  - ASCII (American Standard Code for Information Interchange), 397
  - ASIS (American Society for Industrial Security) International, 457–458
  - assets, 229–231, 332, 525
  - Associate Business Continuity Professional (ABCP), 460
  - Associate of (ISC)<sup>2</sup>, 35
  - asymmetric key cryptography, 192–195, 444, 525
  - asynchronous communication, 387
  - asynchronous dynamic password tokens, 65
  - Asynchronous Transfer Mode (ATM), 384, 525
  - attacks. *See specific attacks by name*
  - attenuation, 373, 376
  - audit logs, 299–302
  - audit trails, 298–302, 332, 525
  - audits, 298, 354, 525
  - Australian Cybercrime Act 2001, 269
  - authentication, 176, 196–199, 440, 525
  - authentication, authorization, and accountability (AAA), 52, 523
  - Authentication Header (AH) protocol, 204, 411, 525
  - Authentication Service (AS), KDC, 66
  - authentication services, 50–51
  - authenticity, guaranteeing message, 193
  - authorization, 51, 440, 525
  - automatic controls, 295, 450, 525
  - autonomous system (AS), 390
  - auto-reply messages, 417
  - auxiliary station systems, 326
  - availability, 186, 215–216, 445, 525
  - awareness programs, security, 236–237
- **B** •
- background checks, 224–225, 284–285, 525
  - backups, 152–153, 291
  - BCP. *See Business Continuity Planning*
  - behavioral biometrics, 58–64
  - behavior-based IDS, 407
  - Bell-La Padula model, 81, 350, 526
  - best evidence, 271, 526
  - best evidence rule, 271–272, 448, 526
  - BGP (Border Gateway Protocol), 390–391
  - BIA (Business Impact Assessment), 140, 143–150, 527
  - Biba integrity model, 81–82, 351, 526
  - biometrics, 52, 58–64, 324, 526
  - Birthday Attacks, 207, 526
  - bit error ratios (BERs), 373
  - black hats, 131
  - black-box testing, 83, 526
  - blackout, 316, 526
  - block cipher, 181–182, 444, 526
  - Blowfish Algorithm, 191
  - bluejacking, 420
  - bluesnarfing, 420
  - book ciphers, 184
  - Border Gateway Protocol (BGP), 390–391
  - bot armies, 122
  - bot herder, 122, 131
  - breaks, during exam, 438
  - bridge, 387, 527
  - Bridge mode, AP, 413
  - Broken Windows theory, 318
  - brownout, 316, 527
  - brute force attack, 75–76, 128, 206, 527
  - buffer overflow attacks, 77, 418, 527
  - burden of proof, 246–247
  - bus (computer architecture), 341, 527
  - bus topology, 371–372, 527
  - business attacks, 252–253
  - Business Continuity and Disaster Recovery Planning domain, 21, 136–141, 442–443. *See also Business Continuity Planning; Disaster Recovery Planning*

- Business Continuity Planning (BCP)
    - Business Impact Assessment, 143–150
    - combining with DRP, 139–141
    - developing plan, 158–161
    - elements of, 150–157
    - implementing plan, 161–162
    - maintaining plan, 162
    - overview, 135
    - project elements, 141–142
    - scope of, 142–143
  - Business Impact Assessment (BIA), 140, 143–150, 527
  - business intelligence, 99
  - business records, 138, 272
- C •
- CA (Certification Authority), 199, 201, 527
  - cables, 372–375
  - California Security Breach Information Act, 262
  - callback method, 408
  - caller ID, 408, 419–420, 527
  - campus area network (CAN), 365, 527
  - Candidate Information Bulletin (CIB), 13
  - CAN-SPAM Act of 2003, 268
  - CAP (Certification and Accreditation Professional), 37, 465
  - CAR (Committed Access Rate), 422
  - carbon dioxide (CO<sub>2</sub>), 330, 452
  - Carnegie Mellon SEI CERT Coordination Center, 469–470
  - Carrier-Sense Multiple Access Collision Detect (CSMA/CD), 378
  - case law, 245–248
  - CBC (Cipher Block Chaining) mode, 187–188, 528
  - CBCP (Certified Business Continuity Professional), 38, 460
  - CBK (Common Body of Knowledge), 3, 19–25, 214. *See also specific domains by name*
  - CBK Review seminars, 14
  - CCA (Chosen Ciphertext Attack), 207
  - CCIE (Cisco Certified Internetworking Expert), 39
  - CCSP (Cisco Certified Security Professional), 39
  - CDI (constrained data item), 82, 352
  - CD-ROM (included with book), 477–478
  - CEH (Certified Ethical Hacker), 39
  - CEI (Computer Ethics Institute), 241
  - Central Processing Unit (CPU), 338, 527
  - central station systems, 326
  - centralized appliance, 124
  - centralized system access controls, 71–74
  - CER (Crossover Error Rate), 59–60, 324, 530
  - CERT (Computer Emergency Response Team), 270, 529
  - certificate programs, 238
  - certification, 36–40, 224, 358–359, 457–467, 527. *See also* CISSP certification
  - Certification and Accreditation Professional (CAP), 37, 465
  - Certification Authority (CA), 199, 201, 527
  - certification step, SDLC, 109
  - Certified Business Continuity Professional (CBCP), 38, 460
  - Certified Ethical Hacker (CEH), 39
  - Certified Functional Continuity Professional (CFCP), 460
  - Certified in the Governance of Enterprise IT (CGEIT), 38, 463
  - Certified Information Security Manager (CISM), 38, 462–463
  - Certified Information Systems Auditor (CISA), 38, 462
  - Certified Information Systems Security Professional certification. *See* CISSP certification
  - Certified Protection Professional (CPP), 38
  - Certified Secure Software Lifecycle Professional (CSSLP), 37, 464–465
  - CEUs (Continuing Education Units), 238
  - CFA (CyberSecurity Forensic Analyst), 39
  - CFB (Cipher Feedback) mode, 187–189, 528
  - chain of custody (chain of evidence), 273–274, 448, 527
  - challenge-response dynamic password tokens, 65
  - Change Control Board, 162
  - change controls, 296–297
  - change management, 109, 296, 441, 528
  - Change Review Board, 109

- CHAP (Challenge Handshake Authentication Protocol), 49, 72, 408, 527
- Check Point certifications, 39, 458
- Chief Information Officers (CIOs), 268
- Child Pornography Prevention Act (CPPA) of 1996, 266
- Chosen Ciphertext Attack (CCA), 207
- Chosen Plaintext Attack (CPA), 207
- Chosen Text Attack (CTA), 188, 207
- C-I-A (Confidentiality, Integrity, and Availability), 444, 528
- CIB (Candidate Information Bulletin), 13
- Cipher Block Chaining (CBC) mode, 187–188, 528
- Cipher Feedback (CFB) mode, 187–189, 528
- ciphers, 180–184, 528
- ciphertext messages, 178, 528
- Ciphertext Only Attack (COA), 207
- circuit switching, 382, 385
- circuit-level gateways, 402–403
- circumstantial evidence, 271, 528
- CIRT (Computer Incident Response Team), 270, 278, 529
- CISA (Certified Information Systems Auditor), 38, 462
- CISC (Complex-Instruction-Set-Computing), 340, 529
- Cisco certifications, 458–459
- Cisco Certified Internetworking Expert (CCIE), 39
- Cisco Certified Security Professional (CCSP), 39
- CISM (Certified Information Security Manager), 38, 462–463
- CISSP (Certified Information Systems Security Professional) certification
  - agents of change, 36
  - examination, 11–18, 429–438
  - maintaining, 29–30
  - overview, 9–10, 27–28
  - promoting, 34–35
  - requirements for, 10–11
  - sample study questions, 479
- CISSP Open Study Guide Web site, 469
- civil law (tort law), 246–249, 447, 528
- civil liability, 236
- civil penalties, 246–247
- cladding, 375
- Clark-Wilson integrity model, 82, 352, 528
- class, 95
- class hierarchy, 95
- Classes of Service (CoS), 205
- classification, 528
- classroom training, 238
- cleaning, 164
- client devices, 412
- Client/TGS Session Key, 67
- clipping levels, 305
- closed systems, 346, 528
- cloud computing, 345
- clustering, 181, 444, 529
- CO<sub>2</sub> (carbon dioxide), 330, 452
- COA (Ciphertext Only Attack), 207
- Code of Ethics, (ISC)<sup>2</sup>, 28–29, 239–240
- code review, SDLC, 107
- codes, 184
- coding, SDLC, 107
- coercion, 273
- cold site, 156, 443, 529
- commercial data classification, 218–220
- Committed Access Rate (CAR), 422
- Common Body of Knowledge (CBK), 3, 19–25, 214. *See also specific domains by name*
- Common Criteria, 357–358, 529
- common law, 245–248
- Common Vulnerabilities and Exposures (CVE), 470
- compensating controls, 47–48, 439, 529
- compensatory damages, 247, 529
- Complex-Instruction-Set-Computing (CISC), 340, 529
- compliance. *See* Legal, Regulations, Investigations, and Compliance domain
- CompTIA (Computing Technology Industry Association), 459
- computer architecture, 337–345
- computer crime, 251–254
- computer crime laws
  - data protection, 256–261
  - disclosure, 261–263
  - information security, 263–269
  - intellectual property, 254–256
  - privacy, 256–261

- Computer Emergency Response Team (CERT), 270, 529
- Computer Ethics Institute (CEI), 241
- computer forensics, 269, 535
- Computer Fraud and Abuse Act of 1986, 248, 263–265
- Computer Incident Response Team (CIRT), 270, 278, 529
- Computer Misuse Act 1990 (U.K.), 269
- Computer Security Act of 1987, 265
- Computing Technology Industry Association (CompTIA), 459
- concealment cipher, 184, 529
- concentrations, CISSP, 37, 465–466
- concentrators, 529
- conceptual definition step, SDLC, 105
- conclusive evidence, 271, 529
- Conficker.B worm, 198
- Confidential information, 219
- confidentiality, 176, 193, 213–215, 444, 529
- Confidentiality, Integrity, and Availability (C-IA), 444, 528
- configuration management, 110, 296, 441, 449, 529
- connection-oriented protocol, 394
- connections, Session Layer, 396
- connectors, 372–374
- constrained data item (CDI), 82, 352
- contention-based network, 378
- Continuing Education Units (CEUs), 238
- Continuing Professional Education (CPE) credits, 18, 30
- Continuity of Operations (COOP), 141
- Continuity Strategy, 158–159
- convergence, 389
- copyright, 256, 529
- corrective controls, 47–48, 295, 439, 450, 529
- corroborative evidence, 271, 530
- CoS (Classes of Service), 205
- Council of Europe’s Convention on Cybercrime (2001), 269
- counter reset, 56
- counter threshold, 56
- covert channels, 348, 354, 453, 530
- CPA (Chosen Plaintext Attack), 207
- CPP (Certified Protection Professional), 38
- CPPA (Child Pornography Prevention Act) of 1996, 266
- CPU (Central Processing Unit), 338, 527
- crackers, 53, 239, 293
- CRC (cyclic redundancy check), 378
- Crime Prevention Through Environmental Design (CPTED), 317, 451
- criminal law, 245–246, 447, 530
- criminal profiles, 251
- critical support areas, 144
- criticality assessment, 144–145, 442, 530
- Crossover Error Rate (CER), 59–60, 324, 530
- crosstalk, 373
- cryptanalysis, 178, 530
- cryptographic algorithm, 180
- cryptography, 530
- Cryptography domain
  - alternatives to, 184–185
  - asymmetric key cryptography, 192–195
  - attack methods, 206–208
  - basics of, 177–181
  - defined, 530
  - e-mail security applications, 201–202
  - Internet security applications, 202–205
  - key escrow, 200–201
  - key management functions, 199–200
  - key recovery, 200–201
  - message authentication, 195–199
  - overview, 21, 175, 443–444
  - Public Key Infrastructure, 199
  - role of, 176–177
  - symmetric key cryptography, 185–191
- cryptology, 178, 530
- cryptosystem, 180–181, 444, 530
- cryptovisible, 180, 530
- CSMA/CD (Carrier-Sense Multiple Access Collision Detect), 378
- CSSLP (Certified Secure Software Lifecycle Professional), 37, 464–465
- CTA (Chosen Text Attack), 188, 207
- culpable negligence, 248, 530
- custodian, 227–228, 530, 536
- customary law system, 250
- cutover test, DRP, 170–171
- CVE (Common Vulnerabilities and Exposures), 470

- cyber attacks, 131
  - Cyber Exchange, (ISC)<sup>2</sup>, 32–33
  - Cybercrime Act 2001 (Australia), 269
  - CyberSecurity Forensic Analyst (CFA), 39
  - cyclic redundancy check (CRC), 378
- D •
- DAC (discretionary access control), 78–79, 353, 532
  - damage assessment, 151, 164
  - data access controls, 51, 78–82, 440
  - Data Accountability and Trust Act (DATA), 262–263
  - data breach, 261
  - data centers, 157
  - data classification, 218–220
  - Data Communications Equipment (DCE), 388, 531
  - data dictionaries, 98, 530
  - data encapsulation, 367
  - Data Encryption Standard (DES), 49, 183, 186–189, 531
  - data hiding, 114, 441
  - data import/export, 80
  - data integrity, 91
  - Data Link Layer, OSI model, 377–388
  - data mining, 99
  - data processing continuity planning, 156–157
  - data protection laws, 256–261
  - data remanence, 353
  - data speeds, 359
  - data storage, 60, 116
  - Data Terminal Equipment (DTE), 388, 532
  - data transmission, LAN, 380
  - data warehouses, 98–99, 531
  - database management system (DBMS), 75, 530
  - databases, 96–102
  - datagram, 385
  - DCE (Data Communications Equipment), 388, 531
  - DCID (Director of Central Intelligence Directive) 6/3, 359
  - Debug mode, 127
  - decentralized system access controls, 74–75
  - deciphering, 178
  - decryption, 178–180, 443, 531
  - Dedicated security mode, 347
  - Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 358–359, 531
  - defense-in-depth, 113, 216, 531
  - Definition phase, DITSCAP, 359
  - delegation, 95
  - deluge system, 330
  - demonstrative evidence, 271, 448, 531
  - Denial of Service (DoS) attack, 57, 121–122, 302, 406, 418, 531
  - DES (Data Encryption Standard), 49, 183, 186–189, 531
  - design review step, SDLC, 106–107
  - design step, SDLC, 106
  - Destination IP Address, 204, 411
  - detective controls, 47–50, 295, 439, 450, 531
  - deterrent controls, 47–48, 439, 450, 531
  - Diameter protocol, 73, 409, 531
  - dictionary attacks, 75, 122, 531
  - Diffie-Hellman key exchange, 194–195, 531
  - digital certificate, 531
  - digital signaling, 367
  - digital signature, 63, 196
  - Digital Signature Standard (DSS), 196, 531
  - Digital Subscriber Line (xDSL), 382–383, 531
  - digital watches, 437–438
  - digital watermarking, 185
  - direct evidence, 270, 447, 532
  - Directive 95/46/EC (1995, EU), 269
  - Director of Central Intelligence Directive (DCID) 6/3, 359
  - Disaster Recovery Institute (DRI) International, 460
  - Disaster Recovery Planning (DRP)
    - combining with BCP, 139–141
    - developing plan, 163–167
    - overview, 21, 135, 162–163, 442–443
    - testing plan, 167–171
  - disastrous events, 136–139
  - disclosure laws, 261–263

- discretionary access control (DAC), 78–79, 353, 532
- discretionary security property, 350
- disk mirroring, 532
- disk striping, 532
- disk striping with parity, 532
- distance-vector protocol, 389
- distributed applications, 89–94, 532
- distributed databases, 101
- distribution, key, 186, 200
- DITSCAP (Defense Information Technology Security Certification and Accreditation Process), 358–359, 531
- documentary evidence, 271, 447, 532
- documentation, 156, 160–161, 355
- domain, 74, 532
- Domain Administrator, Windows Server, 115
- DoS (Denial of Service) attack, 57, 121–122, 302, 406, 418, 531
- DRI (Disaster Recovery Institute) International, 460
- drinks, during exam, 436–437
- DRP. *See* Disaster Recovery Planning
- dry contact switches, 325
- dry-pipe system, 330
- DSS (Digital Signature Standard), 196, 531
- DTE (Data Terminal Equipment), 388, 532
- dual-homed gateways, 404
- due care, 247, 298, 446, 532
- due diligence, 247–248, 447, 532
- dumpster diving, 303, 532
- dynamic packet-filtering firewall, 402
- dynamic password, 64, 532
- dynamic routing protocol, 389
- **E** •
- E&O (Errors and Omissions), 292
- EALs (evaluation assurance levels), 357–358
- EAP (Extensible Authentication Protocol), 72, 205, 408–409, 534
- eavesdropping, 127, 304
- EBCDIC (Extended Binary-Coded Decimal Interchange Code), 397
- EC (elliptic curves), 195
- ECB (Electronic Code Book) mode, 187–188, 532–533
- EC-Council, 461
- ECPA (Electronic Communications Privacy Act) of 1986, 265
- education programs, security, 236–238
- EEA (Economic Espionage Act) of 1996, 253, 266
- EES (Escrowed Encryption Standard), 200, 533
- EF (Exposure Factor), 233, 524
- EGP (Exterior Gateway Protocol), 390
- El Gamal algorithm, 195
- electrical anomalies, 315–316
- electrical noise, 315, 327, 450
- electrical power, 327–328
- Electromagnetic Interference (EMI), 315, 372, 532
- Electronic Code Book (ECB) mode, 187–188, 532–533
- electronic signatures, 63
- electrostatic discharge (ESD), 315, 327
- elliptic curves (EC), 195
- e-mail security, 201–202, 415–417
- emanations, 349
- emergencies, 150–151, 332
- employment agreements, 225
- Encapsulating Security Payload (ESP), 204, 411, 533
- encapsulation, 95
- encryption, 49, 178–180, 443, 533
- encryption keys, 199–201
- end-to-end encryption, 178–179, 533
- Enterprise versions, AV software, 128
- enticement, 273, 533
- entrapment, 273, 448, 533
- environmental safety controls, 326–332
- environmental security. *See* Physical (Environmental) Security domain
- equipment, damage to, 138
- erasers, 437
- Errors and Omissions (E&O), 292
- escalation, 116, 307
- Escrowed Encryption Standard (EES), 200, 533
- ESD (electrostatic discharge), 315, 327
- espionage, 533

Ethernet, 378–379, 533  
 ethics, 28–29, 238–241, 533  
 European Information Technology Security  
 Evaluation Criteria (ITSEC), 356–357,  
 533  
 evacuations, 137  
 evaluation assurance levels (EALs), 357–  
 358  
 evaluation criteria, 352–358  
 evidence, 270–274  
 evidence life cycle, 274–276, 448, 533  
 examination, CISSP, 11–18, 31–32, 429–438  
 excellence, pursuing, 40–41  
 Exclusive Or (XOR) function, 188, 533  
 exigent circumstances, 275, 533  
 expert systems, 102–103, 441, 534  
 Exposure Factor (EF), 233, 524  
 Extended Binary-Coded Decimal  
 Interchange Code (EBCDIC), 397  
 Extensible Authentication Protocol (EAP),  
 72, 205, 408–409, 534  
 Exterior Gateway Protocol (EGP), 390  
 external communications, 154, 166  
 extranet, 366, 534

## • F •

facilities, 306, 317–320  
 fail closed, 215, 534  
 fail open, 215, 534  
 fail-back condition, 215  
 failover, 215, 348, 534  
 fail-safe, 215, 348, 534  
 fail-soft system, 348, 534  
 False Accept Rate (FAR), 59–60, 324, 534  
 False Reject Rate (FRR), 59–60, 324, 534  
 fault, 316, 534  
 fault-tolerant system, 348, 534  
 fax security, 418–419  
 Federal Emergency Management Agency  
 (FEMA), 141  
 Federal Information Processing Standard  
 (FIPS), 187, 200, 535  
 Federal Privacy Act of 1974, 257  
 Federal Sentencing Guidelines of 1991, 266  
 fee, exam, 12  
 felony, 246, 264, 534

fencing, 321, 451  
 Fiber Distributed Data Interface (FDDI),  
 369, 379–380, 534  
 fiber optic cable, 375  
 file transfer protocol (FTP), 55, 398  
 financial attacks, 252  
 financial readiness, DRP, 164–165  
 finger scan systems, 61–62  
 fingerprint recognition, 61  
 fire detection systems, 329, 451–452  
 fire protection, BCP element, 155  
 fire suppression systems, 329–331  
 fire threat, 314  
 firewalls, 301, 401–405, 535  
 firmware, 119, 343, 535  
 flow control, 378, 393  
 focus groups, (ISC)<sup>2</sup>, 33  
 Foreign Intelligence Surveillance Act  
 (FISA), 267  
 foreign key, 101  
 forensics, 269, 535  
 Fraggie attack, 420  
 Frame Relay (FR), 384, 535  
 fraud, 292–293, 535  
 fraud detection system, 293, 449  
 FRR (False Reject Rate), 59–60, 324, 534  
 FTP (file transfer protocol), 55, 398  
 full-duplex mode, 396  
 “fun” attacks, 253–254  
 fuzzy logic, 102, 535

## • G •

gas-discharge system, 330–331  
 gateways, 393, 535  
 GIAC (Global Information Assurance  
 Certification), 38–39, 467  
 GIAC Certified Forensics Analyst (GCFA),  
 38  
 GIAC Certified Incident Handler (GCIH), 38  
 goals, defined, 535  
 governance, 221, 445–446  
 government data classification, 219  
 Gramm-Leach-Bliley Financial Services  
 Modernization Act, 258–259  
 granularity, access control, 97  
 Graphics Interchange Format (GIF), 398

gray-box testing, 84, 535  
 grudge attacks, 253  
 guard dogs, 322  
 guidelines, defined, 535

## • H •

hackers, 53, 130, 239, 293  
 half-duplex mode, 396  
 half-open connections, 421, 455  
 hand geometry systems, 61–62  
 hands-on experience, 13–14  
 hardware, 118–119, 341–343, 535  
 hardware address, 378  
 hardware segmentation, 112–113, 535  
 Hash function, 535  
 hearsay evidence, 448, 536  
 hearsay rule, 272, 536  
 heuristics, 129  
 hidden code, 121, 536  
 hierarchical databases, 99–100  
 Hiers Gamos (HG) Guide to Computers and Law, 470  
 High-level Data Link Control (HDLC), 385  
 High-Speed Serial Interface (HSSI), 536  
 HIPAA (Health Insurance Portability and Accountability Act) 1996, 258, 536  
 hiring practices and procedures, 225–226, 332  
 HMAC (Hashed Message Authentication Code) algorithms, 199  
 hoaxes, 120  
 holddown timers, 390  
 honeypot, 536  
 host scanning, 84  
 host-based intrusion detection (HIDS) system, 92, 304, 406, 455  
 hot site, 157, 536  
 housekeeping, 332  
 hub, 536  
 HVAC (heating, ventilation, and air conditioning), 328–329, 536  
 HyperText Markup Language (HTML), 418  
 HyperText Transfer Protocol (HTTP), 398, 418  
 HyperText Transfer Protocol Secure (HTTPS), 398  
 hypervisor, 119, 344

## • I •

IAB (Internet Architecture Board), 240  
 IANA (Internet Assigned Numbers Authority), 390  
 ICMP (Internet Control Message Protocol), 392, 537  
 ICMP flood, 421  
 IDEA (International Data Encryption Algorithm) Cipher, 191  
 identification, 440, 536  
 identification and authentication (I&A)  
   biometrics, 58–64  
   defined, 354  
   one-time passwords, 64  
   overview, 50, 53  
   passwords, 54–58  
   PINs, 58  
   single sign-on, 65–71  
   tokens, 64–65  
 identity management, 223–224, 536  
 IDSs (intrusion detection systems), 301, 304–305, 325, 406–407, 537  
 IEC (International Electrotechnical Commission), 10, 222  
 IEEE (Institute of Electrical and Electronics Engineers), 380  
 IETF (Internet Engineering Task Force), 64, 201, 536  
 IKE (Internet Key Exchange), 204  
 IMAP (Internet Message Access Protocol), 398–399  
 implementation attack, 206  
 Improved Proposed Encryption Standard (IPES), 191  
 incident handling, 278–279, 306  
 index, relational database, 101  
 indirect damage, 139  
 industrial espionage, 293  
 inert gases, 453  
 inference, 98, 536  
 inference channel, 536  
 inference engine, 536  
 information custodian, 227–228, 530, 536  
 information flow model, 82, 352, 453, 536  
 information owner, 227, 537

- Information Security Governance and Risk Management domain
  - accreditation, 224
  - availability, 215–216
  - awareness programs, 236–237
  - certification, 224
  - confidentiality, 213–215
  - data classification, 218–220
  - defense-in-depth, 216
  - education programs, 236–238
  - goals and objectives of, 220
  - guidelines, 222
  - identity management, 223–224
  - integrity, 215
  - internal Service Level Agreements, 223
  - mission statements, 220
  - outsourcing, 223
  - overview, 22, 444–446
  - personnel security, 224–229
  - policies, 221–222
  - procedures, 222
  - professional ethics, 238–241
  - risk management, 229–236
  - single points of failure, 216–217
  - standards, 222
  - training programs, 236–238
- information security laws, 263–269
- Information Systems Audit and Control Association (ISACA), 462
- Information Systems Security Architecture Professional (ISSAP), 37, 465–466
- Information Systems Security Association (ISSA), 431
- Information Systems Security Engineering Professional (ISSEP), 37, 466
- Information Systems Security Management Professional (ISSMP), 37, 466
- Informative policy, 222, 446
- INFOSYSSEC Web site, 470
- infrastructure support, loss of, 294
- inheritance, 95
- inrush, 316, 537
- instances, 95–96
- Institute of Electrical and Electronics Engineers (IEEE), 380
- Integrated Services Digital Network (ISDN), 382, 537
- integrity, 176, 215, 444, 537
- integrity verification procedures (IVP), 82, 352
- intellectual property, 254–256, 537
- intelligence attacks, 252
- interfaces, Physical Layer, 375–376
- International Data Encryption Algorithm (IDEA) Cipher, 191
- International Electrotechnical Commission (IEC), 10, 222
- International Information Systems Security Certification Consortium (ISC)<sup>2</sup>, 9–10, 28–33, 37, 432, 463–466
- international law, 249–250
- International Organization for Standardization (ISO), 10, 373
- Internet, 202–205, 366, 537
- Internet Architecture Board (IAB), 240
- Internet Assigned Numbers Authority (IANA), 390
- Internet Control Message Protocol (ICMP), 392, 537
- Internet Engineering Task Force (IETF), 64, 201, 536
- Internet Key Exchange (IKE), 204
- Internet Layer, TCP/IP model, 400
- Internet Message Access Protocol (IMAP), 398–399
- Internet Protocol (IP), 53, 391–392, 537
- Internet Protocol Security (IPSec), 203–204, 410–411, 537
- Internet Relay Chat (IRC), 122
- Internet Worm, 118
- Internetwork Packet Exchange (IPX), 392, 537
- interruption (cutover) test, DRP, 170–171
- intranet, 366, 537
- intrusion detection systems (IDSs), 301, 304–305, 325, 406–407, 537
- intrusion prevention systems (IPSs), 304–305, 406, 537
- investigations, 269–279, 299
- IPES (Improved Proposed Encryption Standard), 191
- iris pattern system, 62–63
- ISACA (Information Systems Audit and Control Association), 462
- (ISC)<sup>2</sup> (International Information Systems Security Certification Consortium), 9–10, 28–33, 37, 432, 463–466

(ISC)<sup>2</sup> Blog, 32  
(ISC)<sup>2</sup> Cyber Exchange, 32  
(ISC)<sup>2</sup> focus groups, 33  
(ISC)<sup>2</sup> Journal, 32  
(ISC)<sup>2</sup> Newsletter, 32  
ISDN (Integrated Services Digital Network), 382, 537  
ISO (International Organization for Standardization), 10, 373  
ISO/IEC 17024:2003 standard, 10  
ISO/IEC 27002 standard, 222  
ISSA (Information Systems Security Association), 431  
ISSAP (Information Systems Security Architecture Professional), 37, 465–466  
ISSEP (Information Systems Security Engineering Professional), 37, 466  
ISSMP (Information Systems Security Management Professional), 37, 466  
ITSEC (European Information Technology Security Evaluation Criteria), 356–357, 533  
IVP (integrity verification procedures), 82, 352

## • J •

Java, 92, 120–121  
job descriptions, 226  
job requirements and qualifications, 284  
job rotation, 229, 287, 449, 537, 546  
John the Ripper program, 55, 75  
Joint Photographic Experts Group (JPEG), 398

## • K •

Kerberos, 66, 538  
kernel rootkit, 119  
key clustering, 181, 444, 529  
Key Distribution Center (KDC), 66–67  
key escrow, 200–201  
key fobs, 52  
key logging, 538  
key management, 199–200  
key recovery, 200–201  
keyed digest, 199

keyspace, 180, 443  
keystroke dynamic identification, 63  
keystroke monitoring, 305  
knowledge-based IDS, 304, 407, 455  
knowledge-based systems, 102–103  
Known Plaintext Attack (KPA), 208  
KryptoKnight, 70–71, 538

## • L •

L0phtCrack program, 55, 75  
LANs (local area networks), 217, 363–364, 379–380, 538  
Last successful log-on message, 57  
Last username message, 57  
latency, 180  
lattice-based access controls, 80, 538  
Layer 2 Forwarding Protocol (L2F), 381, 410, 538  
Layer 2 Tunneling Protocol (L2TP), 381, 410, 538  
layering, 113, 216, 531  
LDAP (Lightweight Directory Access Protocol), 49, 71–72, 538  
leased lines, 381  
least privilege, 113, 288–289, 449, 538  
Legal, Regulations, Investigations, and Compliance domain, 23, 245–254, 269–279, 446–449. *See also* computer crime laws  
legal liability, 236  
legally permissible evidence, 273  
liability, 247–248  
library rootkit, 119  
life, loss of, 139  
life safety controls, 326–331  
Lightweight Directory Access Protocol (LDAP), 49, 71–72, 538  
Limited access security mode, 347  
line supervision, 326  
link encryption, 179–180, 538  
link-state protocol, 389  
Local Administrator, Windows Server, 115  
local alarm systems, 326  
local area networks (LANs), 217, 363–364, 379–380, 538  
local response capability, 326

local security chapter membership, 33–34  
 lockout duration, password, 56–57  
 locks, physical, 322  
 logic bombs, 120, 253, 538  
 logical controls, 49, 58, 324–326, 550  
 Logical Link Control (LLC), 377  
 logical security, DRP, 166–167  
 logistics, 155  
 Log-on banner message, 57  
 lookups, relational database, 101  
 loss of life, 139  
 Lucifer algorithm, 187

## • M •

MAC (Media Access Control), 53, 377–379  
 magnetic fields, 316  
 main memory, 341–342  
 maintenance, SDLC, 109–110  
 maintenance hooks, 127, 223, 349, 538  
 Maintenance mode, 127  
 maintenance windows, 116  
 malicious code, 117–121, 294, 416  
 malware, 123, 538  
 MAN (metropolitan area network), 364–365, 539  
 management roles and responsibilities, 226–227  
 mandatory access control (MAC), 80–81, 353, 539  
 mandatory vacations, 287–288  
 man-in-the-middle attack, 77, 195, 208, 539  
 man-made disasters, 137–138  
 man-made threats, 231  
 mantraps, 321, 451, 539  
 manual controls, 295, 450, 539  
 mashup, 94  
 Master Business Continuity Professional (MBCP), 460  
 Maximum Tolerable Downtime (MTD), 146–147, 442, 539  
 MD (Message Digest) family of algorithms, 64, 197–198  
 Media Access Control (MAC), 53, 377–379  
 media controls, 297, 539  
 medications, 437  
 meet-in-the-middle attack, 190, 208, 539  
 memory, computer, 341–343  
 memory addressing, 342–343, 539  
 memory space, 342, 539  
 Merkle-Hellman (Trapdoor) Knapsack, 49, 195  
 mesh topology, 369–370  
 message authentication, 195–199  
 message digests, 196–199, 539  
 messages, OO, 96  
 metadata, 539  
 metallic tape, 325  
 methods, 96  
 metropolitan area network (MAN), 364–365, 539  
 Microsoft security certifications, 466–467  
 military attacks, 252  
 MIME (Multipurpose Internet Mail Extensions), 540  
 MIME Object Security Services (MOSS), 539  
 misdemeanor, 246, 264, 540  
 mission statements, 220, 540  
 mixed law system, 250  
 monitoring, 92, 273, 302–308, 540  
 monoalphabetic substitution, 177, 183, 540  
 Montreal Protocol of 1987, 331  
 Moore's Law, 206  
 Morris Worm, 118  
 Mosaic Web browser, 90  
 motion detectors, 325  
 Motion Picture Experts Group (MPEG), 398  
 Motive, Opportunity, and Means (MOM), 277–278  
 MTD (Maximum Tolerable Downtime), 146–147, 442, 539  
 Multilevel security mode, 347  
 multi-level system, 80, 540  
 multiple inheritance, 96  
 multiprocessing system, 340, 540  
 multiprogramming system, 340, 540  
 Multi-Protocol Label Switching (MPLS), 205, 384, 540  
 Multipurpose Internet Mail Extensions (MIME), 540  
 multistate system, 340  
 Multistation Access Unit (MSAU), 370, 379  
 multitasking system, 340, 540  
 multiuser system, 340

• **N** •

NAT (Network Address Translation), 392, 454, 540

National Computer Security Center (NCSC), 353, 540

National Information Assurance  
 Certification and Accreditation  
 Process (NIACAP), 358–359, 540

National Institute of Standards and  
 Technology (NIST), 186, 200, 265, 470,  
 541

National Security Agency (NSA), 186, 265

natural access control, 317, 451

natural disasters, 136–137, 318

natural surveillance, 317, 451

natural threats, 231

need-to-know status, 288, 449, 540

NetBIOS (Network Basic Input/Output  
 System), 396

Network Access Layer, TCP/IP model, 400

network cabling, 375

network databases, 100

Network File System (NFS), 396

Network Layer, OSI model, 388–393

network security  
 firewalls, 401–405  
 intrusion detection systems, 406–407  
 remote access, 407–409  
 Virtual Private Networks, 409–412

network segment, 387

network topologies, 369–372

network-based intrusion detection (NIDS),  
 304, 406, 455

networking equipment, 376–377, 387–388,  
 393

networks, avoiding single point of failure,  
 217

neural network, 102–103, 441, 541

NIACAP (National Information Assurance  
 Certification and Accreditation  
 Process), 358–359, 540

NIC (network interface card), 376, 540

NIDS (network-based intrusion detection),  
 304, 406, 455

NIST (National Institute of Standards and  
 Technology), 186, 200, 265, 470, 541

nonce, 65, 71

non-interference model, 82, 352, 454, 541

non-repudiation, 51, 55, 176, 541

nonvolatile memory, 341

NSA (National Security Agency), 186, 265

• **O** •

object databases, 101

object orientation (OO), 94–96

object reuse, 353, 541

objectives, 541

objects, 46–47, 96, 439, 541

OFB (Output Feedback) mode, 187, 189,  
 542

off-site storage, BCP element, 152–153

one-time pad, 182, 184, 541

one-time passwords, 64, 541

one-way function, 193, 197, 541

on-the-job training, 238

open message format, 192, 196, 541

Open Shortest Path First (OSPF), 390

Open System authentication, WEP, 414

open systems, 346, 453, 541

Open Systems Interconnection (OSI)  
 Reference Model, 366–368, 541. *See*  
*also specific layers by name*

Open Web Application Security Project  
 (OWASP), 107–108

operating states, CPU, 339

operating system (OS), 84, 343–344, 541

operational assurance requirements,  
 353–354

operational impact, 236

Operations Security domain  
 administrative management and control,  
 283–290  
 attack methods, 292–294  
 audit trails, 298–302  
 auditing, 298  
 due care, 298  
 monitoring, 302–308  
 overview, 23–24, 449–450  
 records retention, 291  
 security controls, 294–298  
 sensitive information, handling, 290–291

Orange Book, 353, 355–356, 454, 542

org chart, 145

organized crime, 131

orientation, employee, 237  
 OS (operating system), 84, 343–344, 541  
 OSI (Open Systems Interconnection)  
   Reference Model, 366–368, 541. *See*  
   *also specific layers by name*  
 OSPF (Open Shortest Path First), 390  
 Output Feedback (OFB) mode, 187, 189,  
   542  
 outsourcing, 223  
 OWASP (Open Web Application Security  
   Project), 107–108  
 owners, 78, 227, 537, 542

● **p** ●

PAC (Privileged Attribute Certificates), 70  
 Packet Internet Groper (PING), 392  
 packet sniffing, 77, 303, 306, 542  
 packet-filtering firewalls, 401–404, 542, 546  
 packet-switched network, 384  
 PAN (personal area network), 365, 542  
 pandemics, planning for, 140  
 parallel tests, DRP, 169–170  
 parity bit, 187  
 PAS (Privileged Attribute Server), 70  
 passive IDS, 406  
 Password Authentication Protocol (PAP),  
   49, 55, 72, 408, 542  
 password sniffing, 77, 303, 306, 542  
 passwords, 54–58, 64, 73, 122, 541–542  
 patch management, 92, 297  
 Patent and Trademark Office (PTO), 255  
 Patent Cooperation Treaty (PCT), 255  
 patents, 255, 542  
 path-vector protocol, 389  
 PATRIOT Act, 266–268, 542  
 Payment Card Industry Data Security  
   Standard (PCI DSS), 108, 260–261  
 payroll, 145  
 PBX (Private Branch Exchange) fraud and  
   abuse, 419  
 PCAOB (Public Company Accounting  
   Oversight Board), 268  
 PEAP (Protected Extensible Authentication  
   Protocol), 544  
 PEM (Privacy Enhanced Mail), 201, 399, 543  
 pen register, 267  
 pencils, 437

penetration testing, 302–304, 542  
 performance and capacity monitoring, 92  
 Permanent Virtual Circuits (PVC), 384  
 permissions, 46, 79  
 permutation (transposition) ciphers, 183–  
   184, 551  
 Permutation boxes (P-boxes), 184  
 perpetrators, attack, 130–131  
 personal area network (PAN), 365, 542  
 personal identification number (PIN), 52,  
   58, 542  
 personally identifiable information (PII),  
   214  
 personnel, 151–152, 167, 224–229, 307, 316  
 PGP (Pretty Good Privacy), 191, 201, 543  
 pharming, 124, 416, 542  
 phishing, 77, 124, 416, 542  
 photo identification card, 323  
 photoelectric sensors, 325  
 phreakers, 131  
 Physical (Environmental) Security domain  
   administrative controls, 331–332  
   combining controls, 332–333  
   environmental safety controls, 326–331  
   life safety controls, 326–331  
   overview, 24, 450–453  
   physical access controls, 320–324  
   site and facility design considerations,  
     317–320  
   technical controls, 324–326  
   threats, 313–316  
 physical address, 378  
 physical controls, 49–50, 58, 320–324, 543  
 physical evidence, 270, 447, 544  
 Physical Layer, OSI model, 368–377  
 physical security, DRP, 166–167  
 Physical Security Professional (PSP), 38  
 physical support, loss of, 294  
 PID (Process ID), 53  
 PII (personally identifiable information),  
   214  
 PIN (personal identification number), 52,  
   58, 542  
 PING (Packet Internet Groper), 392  
 PKI (Public Key Infrastructure), 176, 223,  
   544  
 plaintext messages, 178, 443, 543  
 pluralistic law system, 250

- PMP (Project Management Professional), 38
- point-to-point links, 381
- Point-to-Point Protocol (PPP), 382, 543
- Point-to-Point Tunneling Protocol (PPTP), 382, 410, 543
- policies, 221–222, 543
- polling network, 379
- polyalphabetic substitution cipher, 183
- polynomial, 96, 543
- polymorphism, 96
- POP3 (Post Office Protocol Version 3), 399
- port scanning, 83, 303, 543
- Post-Accreditation phase, DITSCAP, 359
- post-employment screening, 225
- practice exams, 431–432
- preaction system, 330
- precedents, 245
- Prep Tests, 5
- preparing for exam, 12–15, 429–434
- Presentation Layer, OSI model, 397–398
- presentations, awareness, 237
- Pretty Good Privacy (PGP), 191, 201, 543
- preventive controls, 47, 49–50, 295, 439, 450, 543
- primary key, 101
- principal, 66, 68
- privacy, 214, 543
- Privacy Enhanced Mail (PEM), 201, 399, 543
- privacy laws, 256–261
- Private Branch Exchange (PBX) fraud and abuse, 419
- private key pair, 192
- Privileged Attribute Certificates (PAC), 70
- Privileged Attribute Server (PAS), 70
- privileged entity controls, 296
- problem management, 306
- procedures, 543
- Process ID (PID), 53
- process isolation, 112, 441, 543
- processes, 217
- proctoring examinations, 32
- professional liability, 292
- Project Management Professional (PMP), 38
- promiscuous mode, 303, 406, 543
- proprietary systems, 326
- Protected Extensible Authentication Protocol (PEAP), 544
- protection domain, 544
- protection rings, 347, 544
- proximate causation, 247, 544
- proximity card, 323
- proxy server, 403, 525
- prudent man rule, 544
- pseudo flaw, 126, 442, 544
- PSP (Physical Security Professional), 38
- PTO (U.S. Patent and Trademark Office), 255
- Public Company Accounting Oversight Board (PCAOB), 268
- public key, 525
- Public Key Infrastructure (PKI), 176, 223, 544
- public key pair, 192
- public utilities, damage to, 138
- punitive damages, 247, 544
- PVC (Permanent Virtual Circuits), 384
- **Q** •
- qualification program, 238
- qualitative asset value, 230
- qualitative impact, 143–144
- qualitative risk analysis, 233–234
- Quality of Service (QoS), 205
- quantitative asset value, 230
- quantitative impact, 143–144
- quantitative risk analysis, 234
- queries, database, 98
- **R** •
- RA (Registration Authority), 199, 545
- RA (risk analysis), 232–234, 545
- race condition, 348–349
- radiation monitoring, 303
- Radio Frequency Interference (RFI), 315, 372, 544
- RADIUS (Remote Authentication Dial-In User Service), 49, 72–73, 205, 409, 532, 545
- Random Access Memory (RAM), 341
- RARP (Reverse Address Resolution Protocol), 380, 545
- RAS (remote access service) server, 72, 408, 545

- RBAC (role-based access control), 79, 440, 545
- Read-Only Memory (ROM), 341
- real evidence, 447, 544
- real-time blackhole lists (RBLs), 415
- reciprocal site, 157
- reconstruction, event, 299
- records retention, 291
- recovery, DRP, 164
- recovery controls, 47–48, 439, 544
- Recovery Point Objective (RPO), 148–149
- recovery procedures, 348
- recovery targets, BIA, 147–149
- Recovery Time Objective (RTO), 147–149, 442, 544
- Red Book, 356
- Red Hat Certified Security Specialist (RHCSS), 39
- Reduced-Instruction-Set-Computing (RISC), 340, 544
- reference books, 473–474
- reference checks, 224
- reference monitor, 114–115, 346, 442, 545
- registration, exam, 11–12, 430, 436
- Registration Authority (RA), 199, 545
- regulations. *See* Legal, Regulations, Investigations, and Compliance domain
- regulatory law, 248, 447, 524
- Regulatory policy, 221, 446
- relational databases, 100–101
- relevant evidence, 273
- religious law system, 250
- remote access, 49, 407–409
- remote access service (RAS) server, 72, 408, 545
- Remote Authentication Dial-In User Service (RADIUS), 49, 72–73, 205, 409, 532, 545
- remote maintenance, 126–127
- Remote Procedure Call (RPC), 396
- remote station systems, 326
- renewing certification, 18
- repeater, 376
- Repeater mode, AP, 413
- Replay Attack, 208
- reporting, event, 307
- repository, 199, 545
- repudiation, 176
- resilient system, 348, 534
- resolution, security event, 307–308
- resource protection, 295–296
- Resource Requirements, BIA, 150
- responding to events, 306–308
- restricted address, 408
- restricted algorithm, 180
- restricted areas, 331
- results, exam, 17–18
- retina pattern system, 62–63
- return on investment (ROI), 141
- Reverse Address Resolution Protocol (RARP), 380, 545
- Review Seminar, CISSP, 432
- RFI (Radio Frequency Interference), 315, 372, 544
- RHCSS (Red Hat Certified Security Specialist), 39
- Rijndael Block Cipher, 190, 545
- ring topology, 370–371, 545
- RIP (Routing Information Protocol), 389–390
- RISC (Reduced-Instruction-Set-Computing), 340, 544
- risk acceptance, 235, 545
- risk analysis (RA), 232–234, 545
- risk assignment, 235, 545
- risk avoidance, 235
- risk identification, 230–232
- risk management, 229–236. *See also* Information Security Governance and Risk Management domain
- risk mitigation, 230, 545
- risk reduction, 235, 545
- Rivest, Shamir, Adleman (RSA) algorithm, 194, 545
- Rivest Ciphers, 191
- RJ-type connectors, 374
- ROI (return on investment), 141
- role-based access control (RBAC), 79, 440, 545
- ROM (Read-Only Memory), 341
- Root mode, AP, 413
- rootkits, 118–119, 348
- rotation of duties, 229, 287, 449, 537, 546
- rounds, 187
- route poisoning, 390
- routed protocols, 391–392

router, 393, 546  
 Routing Information Protocol (RIP), 389–390  
 routing protocols, 388–391  
 rows, relational database, 101  
 RPC (Remote Procedure Call), 396  
 RPO (Recovery Point Objective), 148–149  
 RSA (Rivest, Shamir, Adleman) algorithm, 194, 545  
 RTO (Recovery Time Objective), 147–149, 442, 544  
 rule-based access control, 80, 546  
 running ciphers, 184

## • S •

SA (security association), 204, 411  
 sabotage, 294, 316  
 Safe Harbor program, 269  
 safeguards, 234–235, 445–446, 546  
 sag, 316, 546  
 salvage team, DRP, 164  
 SAM (Security Account Manager) accounts, 54  
 SAN (storage-area network), 217, 365  
 sandbox, 92  
 SANS (Systems Administration, Networking, and Security) Institute, 14, 467, 471  
 Sarbanes-Oxley Act of 2002 (SOX), 268  
 S-boxes (Substitution boxes), 183  
 SBU (Sensitive but Unclassified), 187, 219, 347, 547  
 scalability, 186, 194  
 scalar processor, 340  
 scan, 546  
 schema, relational database, 101  
 scope creep, 142  
 scorecard, 116  
 screened-host gateways, 405  
 screened-subnets, 405  
 screening router, 401–404, 542, 546  
 script injection, 418  
 script kiddies, 130, 253–254  
 scytale, 177  
 SDH (Synchronous Digital Hierarchy), 384–385  
 SDLC (software development life cycle), 84, 548  
 SDLC (Synchronous Data Link Control), 386  
 SDLC (systems development life cycle), 103–112, 441  
 sealing evidence, 276  
 search and seizure, illegal, 273  
 search warrant, 275  
 secondary evidence, 271, 546  
 secondary memory, 342–343  
 Secret information, 219  
 secure and signed message format, 193, 546  
 Secure Electronic Transaction (SET), 202–203, 399, 546  
 Secure European System and Applications in a Multi-vendor Environment (SESAME), 70, 546  
 Secure Hash Algorithm (SHA), 198  
 Secure HyperText Transfer Protocol (S-HTTP), 203, 399, 546  
 secure message format, 192, 546  
 Secure Multipurpose Internet Mail Extensions (S/MIME), 201, 399, 547  
 Secure Remote Procedure Call (S-RPC), 399  
 Secure Shell (SSH), 205, 397, 547  
 Secure Sockets Layer/Transport Layer Security (SSL/TLS), 202, 395, 411–412, 547  
 Security Account Manager (SAM) accounts, 54  
 Security Architecture and Design domain  
   access control models, 350–352  
   computer architecture, 337–345  
   evaluation criteria, 352–358  
   overview, 24, 337, 453–454  
   security architecture, 345–349  
   system certification and accreditation, 358–359  
 security association (SA), 204, 411  
 security awareness, 236–237, 547  
 security badges, 323–324  
 security clearances, 224–225  
 security countermeasures, 349  
 security education programs, 236–238  
 Security Features User’s Guide (SFUG), 355  
 security guards, 321–322  
 security kernel, 114, 346, 453, 547

- security management principles, 216
- security models, 337
- security modes of operation, 347, 547
- Security Parameter Index (SPI), 204, 411
- security perimeter, 345, 547
- Security Protocol ID, 204, 411
- security technologies, 216
- security testing, 354
- security training programs, 236–238
- security violations, 307
- security zones, 317
- Security+ certification, 39
- Security5 certification, 39
- self-study, 13–14
- senior management, 141–142, 161–162, 221, 446
- Sensitive but Unclassified (SBU), 187, 219, 347, 547
- sensitive information, handling, 290–291
- sensitivity labels, 80, 353, 547
- separation of duties and responsibilities, 228, 286, 449, 547
- separation of privilege, 288–289, 449, 538
- separation of privilege (least privilege), 113
- Sequenced Packet Exchange (SPX) protocol, 395
- sequential memory, 342
- Serial Line Internet Protocol (SLIP), 382, 547
- server virtualization, 217
- Service Level Agreements (SLAs), 115–116, 223, 547
- Service Set Identifier (SSID), 205, 413
- Service Ticket, Kerberos, 69
- SESAME (Secure European System and Applications in a Multi-vendor Environment), 70, 546
- session hijacking, 77, 421, 548
- Session Initiation Protocol (SIP), 397
- session key, Kerberos, 70
- Session Layer, OSI model, 396–397
- SET (Secure Electronic Transaction), 202–203, 399, 546
- SFUG (Security Features User’s Guide), 355
- SHA (Secure Hash Algorithm) family, 198
- Shared Key authentication, 414
- shielded twisted pair (STP) cabling, 373, 375
- shoulder surfing, 548
- S-HTTP (Secure HyperText Transfer Protocol), 203, 399, 546
- side-channel attacks, 190
- signature dynamics system, 63–64
- signature-based IDS, 304, 407, 455
- Simovits Consulting site, 471
- simple integrity property, 526
- Simple Key Management for Internet Protocols (SKIP), 393, 548
- Simple Mail Transfer Protocol (SMTP), 399, 415
- Simple Network Management Protocol (SNMP), 399
- simple security property (ss property), 81–82, 350–351, 526
- simplex mode, 396
- simplification, BCP, 159–160
- Simula, 96
- simulations, DRP, 168–169
- Single Loss Expectancy (SLE), 233, 524
- single points of failure, 216–217
- single sign-on (SSO), 53, 65–71, 548
- SIP (Session Initiation Protocol), 397
- Site accreditation, DITSCAP, 359
- site design, 317–320
- Site Security Handbook, The*, 221
- S/Key protocol, 64
- SKIP (Simple Key Management for Internet Protocols), 393, 548
- SLAs (Service Level Agreements), 115–116, 223, 547
- Slashdot Web site, 471
- SLIP (Serial Line Internet Protocol), 382, 547
- Smalltalk, 96
- smart card, 52, 323
- SMDS (Switched Multimegabit Data Service), 385, 550
- S/MIME (Secure Multipurpose Internet Mail Extensions), 201, 399, 547
- SMTP (Simple Mail Transfer Protocol), 399, 415
- Smurfs, 421, 548
- snacks, during exam, 436–437
- sniffing, 127, 548
- SNMP (Simple Network Management Protocol), 399

- social engineering, 78, 124–126, 304, 548
- soda acid, 330, 452
- software, 90, 343–345, 548
- software development life cycle (SDLC), 84, 548
- software escrow agreement, 153–154, 442
- SONET (Synchronous Optical Network), 384, 548, 550
- SOX (Sarbanes-Oxley Act of 2002), 268
- spam, 123–124, 415–417, 548
- spear phishing, 125, 548
- SPI (Security Parameter Index), 204, 411
- spike, 316, 548
- split horizon, 390
- spoofing, 123, 549
- SPX (Sequenced Packet Exchange) protocol, 395
- spyware, 549
- SQL (Structured Query Language), 101–102, 397
- S-RPC (Secure Remote Procedure Call), 399
- SSCP (Systems Security Certified Practitioner), 35, 463–464
- SSH (Secure Shell), 205, 397, 547
- SSID (Service Set Identifier), 205, 413
- SSL/TLS (Secure Sockets Layer/Transport Layer Security), 202, 395, 411–412, 547
- SSO (single sign-on), 53, 65–71, 548
- stack overflow attack, 77, 418, 527
- standards, 549
- star, 549
- star integrity property (\*-integrity property), 351, 526
- star property (\* property), 81–82, 350, 526
- star topology, 369, 549
- state machine model, 549
- stateful inspection firewall, 403, 455, 549
- static password, 64–65, 549
- static routing protocol, 388
- statistical anomaly-based IDS, 407
- statistical attack, 206
- statutory damages, 247, 549
- statutory liability, 236
- steganography, 184–185, 549
- storage, 200, 276, 291, 322
- storage-area network (SAN), 217, 365
- STP (shielded twisted pair) cabling, 373, 375
- stream cipher, 181, 182, 549
- strong authentication, 52, 549
- Structured Query Language (SQL), 101–102, 397
- structured walkthroughs, DRP, 168
- study groups, 14–15, 33, 431
- study plans, 430
- subject, 46–47, 439, 549
- subpoena, 275
- Substitution boxes (S-boxes), 183
- substitution cipher, 182–183, 444, 549
- superscalar processor, 340
- supervising examinations, 32
- Supervisor mode, 115, 549
- surges, 316, 328, 550
- surveillance, 325
- switch, 387, 550
- Switched Multimegabit Data Service (SMDS), 385, 550
- Switched Virtual Circuit (SVC), 384
- symmetric key cryptography, 185–191, 444, 550
- SYN flood attacks, 121, 421–422, 550
- synchronous communication, 387
- Synchronous Data Link Control (SDLC), 386
- Synchronous Digital Hierarchy (SDH), 384–385
- synchronous dynamic password tokens, 65
- Synchronous Optical Network (SONET), 384, 548, 550
- system access controls, 51–53, 71–78, 440, 550. *See also* identification and authentication
- System accreditation, DITSCAP, 359
- system architecture, 353
- system certification and accreditation, 358–359
- System High mode, 114, 347, 442, 550
- system integrity, 353
- system messages, 57
- system test step, SDLC, 108
- systems, avoiding single point of failure, 217
- Systems Administration, Networking, and Security (SANS) Institute, 14, 467, 471
- systems development life cycle (SDLC), 103–112, 441
- Systems Security Certified Practitioner (SSCP), 35, 463–464

## • T •

- tables, relational database, 101
- TACACS (Terminal Access Controller Access Control System), 74, 409, 550
- Take-Grant model, 351, 550
- target hardening, 317
- TCB (Trusted Computing Base), 345–346, 453, 551
- TCO (total cost of ownership), 235–236
- TCP (Transmission Control Protocol), 394, 551
- TCP/IP (Transmission Control Protocol/Internet Protocol), 391, 400
- TCSEC (Trusted Computer System Evaluation Criteria), 352–356, 551
- Teardrop attack, 77, 422, 550
- technical controls, 49, 58, 324–326, 550
- technical non-(ISC)<sup>2</sup> certifications, 39
- technical training, 238
- Telecommunications and Network Security
  - domain. *See also* network security
  - e-mail security, 415–417
  - fax security, 418–419
  - network types, 363–366
  - overview, 25, 454–455
  - TCP/IP model, 400
  - telephone security, 419–420
  - threats, 420–422
  - Web security, 418
  - WLAN security, 412–414
- telecommunications circuits, 386
- telecommunications hotel, 217
- telephone security, 419–420
- Telnet, 123, 400, 550
- TEMPEST project, 349, 374
- Temporal Key Integrity Protocol (TKIP), 414
- “Ten Commandments of Computer Ethics,” 241
- Terminal Access Controller Access Control System (TACACS), 74, 409, 550
- termination of employment, 225–226, 290, 332
- territorial reinforcement, 317, 451
- terrorism, 252
- TFM (Trusted Facility Manual), 355
- TFTP (Trivial File Transfer Protocol), 400
- theft, 294
- theoretical related-key attack, 190
- thicknet cable, 372, 375
- thinnet cable, 372, 375
- threat analysis, 231–232
- threats, 229, 550. *See also specific threats by name*
- three-factor authentication, 52
- three-way handshake, 551
- throughput, 60–61
- Ticket Granting Service (TGS), KDC, 66–67
- Ticket Granting Ticket (TGT), KDC, 67
- TKIP (Temporal Key Integrity Protocol), 414
- TLS (Transport Layer Security), 202, 547
- TNI (Trusted Network Interpretation), 352, 356, 552
- token-passing network, 378–379
- Token-Ring, 379, 551
- tokens, 52, 64–65, 551
- Top Secret information, 219
- topologies, network, 369–372
- tort law, 246–249, 447, 528
- total cost of ownership (TCO), 235–236
- trade secrets, 256, 447, 551
- trademarks, 255, 551
- traffic analysis, 127–128, 305–306, 551
- traffic inference, 127–128
- training courses, CISSP, 14–15
- training programs, security, 236–238
- transaction throughput, 116
- transactions, database, 101–102
- transference, 235, 545
- transformation procedures (TP), 82, 352
- transient, 551
- Transmission Control Protocol (TCP), 394, 551
- Transmission Control Protocol/Internet Protocol (TCP/IP), 391, 400
- Transport Layer, 393–395, 400
- Transport Layer Security (TLS), 202, 547
- Transport Mode, IPsec, 204, 411
- transportation, 137, 139, 276
- transposition ciphers, 183–184, 551

trap and trace device, 267  
 trap door, 121, 551  
 trend analysis, 305–306  
 Triple DES (3DES), 189–190, 523  
 Trivial File Transfer Protocol (TFTP), 400  
 Trojan horse, 119–120, 551  
 trust model, 75, 201  
 trusted computer system, 551  
 Trusted Computer System Evaluation  
   Criteria (TCSEC), 352–356, 551  
 Trusted Computing Base (TCB), 345–346,  
   453, 551  
 Trusted Facility Manual (TFM), 355  
 Trusted Network Interpretation (TNI), 352,  
   356, 552  
 trusted path, 354, 552  
 trusted recovery, 298, 354, 552  
 trusted subject, 350  
 tunnel, 402  
 Tunnel Mode, IPsec, 204, 411  
 two-factor authentication, 52, 65, 552  
 Twofish Algorithm, 191  
 Type accreditation, DITSCAP, 359  
 Type I Error (False Reject Rate), 59–60, 324,  
   534  
 Type II Error (False Accept Rate), 59–60,  
   324, 534  
 typing dynamics system, 63

## • U •

UDP flood attack, 422  
 Unclassified information, 219  
 unconstrained data item (UDI), 82, 352  
 uninterruptible power supply (UPS), 155,  
   327, 552  
 unit testing, 107–108  
 unshielded twisted pair (UTP) cabling, 373,  
   375  
 Unsolicited Commercial E-mail (UCE),  
   123–124, 416–417, 548  
 unsubscribe links, 416  
 USA PATRIOT Act of 2001, 266–268, 542  
 User Datagram Protocol (UDP), 394–395,  
   552  
 User mode, 115, 552

users, 228, 289–290, 552  
 utilities, 137, 154–155, 319

## • V •

Validation phase, DITSCAP, 359  
 value-added network (VAN), 365  
 vendor non-(ISC)<sup>2</sup> certifications, 39  
 Verification phase, DITSCAP, 359  
 vernam ciphers, 184, 552  
 vibration, 314  
 view, 97, 552  
 violation analysis, 305, 552  
 virtual local area network (VLAN), 365  
 virtual memory, 342–343, 552  
 Virtual Private Networks (VPNs), 409–412,  
   455, 552  
 virtualization, 217, 344–345  
 virus writers (VXers), 117, 131  
 viruses, 117–118, 416, 552  
 visitor policies, 331  
 Voice over Internet Protocol (VoIP), 553  
 voice recognition system, 63–64  
 volatile memory, 341  
 volunteer opportunities, (ISC)<sup>2</sup>, 31–33  
 vulnerability, 180, 229, 553  
 vulnerability assessment, 143–144, 232, 442  
 vulnerability scanning, 303

## • W •

WANs (wide area networks), 364–366,  
   381–387, 553  
 WAP (Wireless Application Protocol), 205  
 war dialing, 303, 553  
 war driving, 303, 553  
 warm site, 156–157, 443, 553  
 water damage, 314  
 water protection, BCP element, 155  
 water sprinkler system, 329, 452  
 waterfall model, 111  
 weather, severe, 315  
 Web security, 418  
 Web sites, security, 469–472  
 well-formed transaction, 352  
 wet-pipe system, 330

- whaling, 125
  - white hats, 131
  - white-box testing, 83, 553
  - wide area networks (WANs), 364–366, 381–387, 553
  - WiFi (wireless fidelity), 553
  - WiFi Protected Access (WPA and WPA2), 414
  - WindowSecurity Network Security Library, 472
  - Wired Equivalent Privacy (WEP), 205, 381, 413–414, 553
  - Wireless Application Protocol (WAP), 205
  - wireless cards, 412
  - wireless local area network (WLAN), 365, 380–381, 412–414, 553
  - Wireless Transport Layer Security (WTLS), 205, 553
  - work factor, 206, 553
  - World Trade Center towers, 137–138
  - worms, 118, 553
  - Writ of Possession, 275
- ✕ ●
- X.25 network, 385, 553
  - xDSL (Digital Subscriber Line), 382–383, 531
  - XOR (Exclusive Or) function, 188, 533