Index

Symbols

802.11 standards, 269

A

abnormal events, tracking, 202-203

access creep, 301

accuracy of biometric systems, 388

acid (atomicity, consistency, isolation, durability) test, 464

ACID test (atomicity, consistency, isolation, and durability), 171, 229, 464

active attacks, 314-319, 467

active RFID tags, 218

administrative audits, 41

AES (Advanced Encryption Standard), 344

aggregation, 226

agile software development, 143-144

al-Kindi, Abu, 340

ALE (annual loss expectancy), 452

- calculating, 85, 416

algorithms, 341

alternative application-development techniques, 142-145

ANSI X12, 180

answers (practice exam), 509-525

application–development techniques, 142-145

application layer

- OSI reference model, 246
- TCP/IP model, 253-254

application proxies, 263

application testing, 172-173

applications

- auditing, 168
  - continuous online auditing, 173-175
  - data integrity controls, 170-171
  - via observation and testing, 169-170
- disposing of, 140-141
- testing, 172-173

AR (abandon rate), 199

arithmetic logic unit, 210

ARO (annual rate of occurrence) estimating, 416

ARP (Address Resolution Protocol), 251

artificial intelligence, 185

ASCII (American Standard Code for Information Exchange), 225

assemblers, 222, 463

asset identification, 81-83

assets, information assets

- classifying, 296-297
- evaluating, 296

asymmetric encryption, 341, 344

- ECC, 345
- RSA encryption, 345

asynchronous attacks, 316

ATBASH, 340

ATM (Asynchronous Transfer Mode), 267

attack-detection tools, 311

attacks

- active, 314-319
- against Bluetooth, 327
- cryptographic, 351-352
- passive, 313-314

attenuation, 256

attribute sampling, 47, 450

attributes, 226

- of CSAs, 51

audit monitors, 181

audit opinion, required elements, 49

audit planning process, 26-27

audit programs, 41

audit reduction tools, 200, 312

auditing, 39

- applications, 168
  - continuous online auditing, 173-175
  - data integrity controls, 170-171
  - testing methods, 172-173
  - via observation and testing, 169-170
- business application systems
  - business intelligence, 182-186
  - e-commerce, 179-180
  - EDI, 180-181
  - email, 181-182
- classifying types of audits, 40-41
- compliance testing, 46
- continuous auditing, 52
- continuous online auditing, 174
- CSAs, 50-51
- evidence, 47
  - reliability of, 48
- fraud, detecting, 49
- general control procedures, 37
- independence as requirement, 40
- information security, 335
  - data ownership, 335-336
  - security baselines, 336
- information system control procedures, 37
- infrastructure security, 337
  - change management, 339-340

network assessments, 339
penetration testing, 337-339
integrated auditing, 51-52
internal controls, CobiT, 38-39
ISACA code of ethics, 31-32
methodology, 42-43
documentation, 43-45
objectives, defining, 45
project management, 177-178
risk analysis, 32
categories of risk, 32-33
risk management, 33
monitoring phase, 35
risk management team, establishing, 33-34
risk mitigation, 34
risk-based, 35-36
sampling, 46-47
substantive testing, 46
systems development, 176-177

AUPs (acceptable use policies), 311

authentication
biometric systems, 387-389, 466
by characteristic, 306-307
by knowledge, 304-305
by ownership, 305
digital signatures, 346-347
Kerberos, 309
single sign-on, 307-309

automated WPs, documenting audit findings, 43-45

availability
reports, 219
role in IS, 295-296

awareness and training, role in overcoming privacy issues, 298

B

B-to-B (Business to Business) e-commerce model, 179

B-to-C (Business to Consumer) e-commerce model, 179

B-to-E (Business to Employee) e-commerce model, 179

B-to-G (Business to Government) e-commerce model, 179

background checks, 92

backup and restoration methods, 431-432
media rotation, 433
SANs, 434

backup power supplies, 382

balance data, 165

balanced matrix organizational form, 119

balanced score card, 71
performance, measuring, 72

base case system evaluation, 173

baseband transmission, 256

Basel Accord Standard II, 25

bastion hosts, 265

batch controls, 162

batch control, 160

BCP (business continuity plan), 409, 471
BIA, 411-412
criticality analysis, 416-417
information gathering, 413
loss, methods of calculating, 412-413
implementation and testing phase, 421-423
full operation tests, 424
paper tests, 423
preparedness tests, 424
monitoring and maintenance, 425
plan design and development, 419-420
project management and initiation, 410
recovery strategy, 417-419
tests, 473
training and awareness, 420-421
verifying, 436-437

Beaman, Bob, 225

Berners-Lee, Tim, 272

best practices for IT governance, goals of, 67-68

BIA (business impact analysis), 472
criticality analysis, 416-417
information gathering, 413
loss, methods of calculating, 412-413
role in BCP process, 411-412

biometric systems, 306-307, 387-389, 466

black hats, 331

black-box tests, 456

block cipher algorithm, 343

Blu-ray discs, 213

Bluetooth, 243, 327

bollards as physical security control, 373

bottom-up policy development, 75, 451

bottom-up testing, 137

BRI (basic rate interface), 268

bridges, 259, 261

broadband transmission, 256

broadcast domains, 259

broadcast transmission, 251

brute-force attacks, 318

bump keys, 379

bus topology, 255

business application development, 130-131
systems-development methodology, 131-132

business application systems
business intelligence, 182
artificial intelligence, 185
CRM, 185
data architecture components, 183
DSS, 184-185
SCM, 186
e-commerce, auditing, 179-180
EDI, 180-181
email, 181-182

business intelligence, 182
artificial intelligence, 185
CRM, 185

data architecture components, 183
DSS, 184-185
SCM, 186
business process controls, 159
input controls, 160-162
output controls, 166-167
processing controls, 162-164
data file controls, 165-166
Business Software Alliance, 230
bypass label processing, 311

C

CAATs (computer-assisted auditing techniques), 43
cabling
attenuation, 256
coaxial, 256
fiber-optic, 257
plenum-grade, 256
twisted pair, 256
wireless communication, 257
Caesar's Cipher, 340
calculating
ALE, 85, 416, 452
project task time estimates, 127
SLE, 86, 416
capacity management, 220-221, 463
categories of twisted-pair cabling, 256
CBD (component-based development), 145
CDs (compact discs), 213
Cerf, Vinton, 272
CERTs (Computer Emergency Response Teams), responding to incidents, 332-334
CGI (Common Gateway Interface), 273
chain of custody, 41
change-management, 95, 206-207, 339-340
post-deployment, 209
program library systems, 207-208
release management, 208-209
changeover, methods of, 456
chargeback method of security system funding, 74
chief privacy officer, role in information security, 295
chief security officer, role in information security, 295
cipher text-only attacks, 351
circuit-level firewalls, 321
circuit-level proxies, 264
circuit-switched WANs, 268
citizen programmers, 138
Class A networks, 251
Class B networks, 251
Class C networks, 251
classifying
information assets, 296-297
types of audits, 40-41
client systems, 215
client/server networks, 216
security, 324-325
closing projects, 128-129
CMM (capability maturity model), 98, 453
coaxial cable, 256
CobiT (Control Objectives for Information and Related Technology), 38-39, 98, 454
COBOL (Common Business-Oriented Language), 222
COCOMO (Constructive Cost Model), 122
Cohen, Fred, 316
cold sites, 427
collision domains, 259
collisions, 259
commercial data-classification system, 297
commercial information classification system, 393
Common Criteria, 76
communication-driven DSS, 184
comparative analysis, 317
comparing OSI reference model and TCP/IP model, 249
compilers, 222, 463
compliance
ensuring, 46-47
regulatory standards, verifying with external regulations, 25-26
compliance testing, 28, 46
computer forensics, 334-335
computer viruses, 316
computers, 214
types of, 462
confidential information, handling, 312-313
confidentiality, role in IS, 295-296
confidentiality-based data classification systems, 297
content switches, 260
continuous assurance, 52
continuous audit techniques, 52, 460
continuous online auditing, 173-175
continuous backups, 432
control procedures
information system control, 449-450
processing control, 458
control unit (CPU), 210
control zones, 314
controls
compliance testing, 46
for physical security, 371
exterior controls, 372-374
interior controls, 375-378
personnel controls, 379-381
cookies, 273
core competency, 94
corrective control, 76
COSO (Committee for Sponsoring Organizations of the Treadway Commission), 25, 99
cost of software, estimating, 122-123
CPM (critical path methodology), 127, 455

CPTED (crime prevention through environmental design), 373
CPUs, 210, 461
- Kilby, Jack, 212
- types of, 461

crackers, 331
crashing, 127
critical systems, 472
criticality analysis, quantitative method, 416-417
CRM (customer relationship management), 185, 227
cross-cut shredders, 369
CRs (change requests), 96
cryptographic attacks, 351-352
cryptographic keys, 341
cryptography, real-world solutions, 349-350
CSA (control self-assessment) process, 50-51
cut-through switching, 260
cyberterrorists, 332

D

DAC (discretionary access control), 301, 466
data mining, 226
data communications software, 225
data disposal, 141
data file controls, 165-166
data integrity controls, 170-171
data integrity testing, 170-171
data-link layer (OSI reference model), 247
- Layer 2 bridges, 259
- Layer 2 switches, 259

data mining, 184
data ownership, establishing, 335-336
data recovery, 431-432
data sinks, 225
data-driven DSS, 184
database servers, 216
databases, 226, 464
- ACID test, 229
- metadata, 226
- structure of, 227
  - HDMSs, 227
  - NDMSs, 227
  - RDMSs, 228

decompilers, 223
defense-in-depth, 293
defining
- audit objectives, 45
- physical security policies, 390

delay window, 202
Delphi Technique, 88
deluge water sprinklers, 386
DES (Date Encryption Standard), 343-344
design phase of SDLC, 136
destroying sensitive information, 369-370
detecting fraud, 49
developers, role in information security, 296
development methods
- SDLC. *See* SDLC
- types of, 456-457

development of Internet, 272
development phase of SDLC, 136-139
devices
- bridges, 259
- broadcast domains, 259
- collision domains, 259
- firewalls, 263
  - application proxies, 263
  - circuit-level proxies, 264
  - dual-homed gateways, 265
  - packet filters, 264
  - screened host firewalls, 265
- gateways, 260
- hubs, 259
- modems, 260
- portable wireless devices, 271
- repeaters, 259
- routers, 260
- switches, 259

DHCP (Dynamic Host Configuration Protocol), 254
dictionary attacks, 317
differential backups, 432
digital signatures, 346-347
directory services, 249
disaster recovery
- alternate processing sites, 426-429
- alternatives, 425
- and public relations, 408
- and reputation, 407
- backup and restoration, 432
  - media rotation, 433
  - SANs, 434
- BCP, 409
  - BIA, 411-413, 416-417
  - implementation and testing phase, 421-424
  - monitoring and maintenance, 425
  - plan design and development, 419-420
  - project management and initiation, 410
  - recovery strategy, 417-419
  - training and awareness, 420-421
- corrective control, 76
- hardware recovery, 429
  - RAID, 430-431
- incident classification, 406-407
- plans, verifying, 436-437
- software and data recovery, 431-432
- telecommunications recovery, 434-435

disposal of applications, 140-141
disposing
- of data, 141
- of sensitive information, 368-370

distance-vector protocols, 251
DMZs, 265, 322
DNS (Domain Name Service), 249
document-driven DSS, 184
documentation
- as part of auditing methodology, WPs, 43-45
- reviewing, 78-79

doors as physical security control, 375-376

DoS attacks, 318, 467
DOSD (data-oriented system development), 145
DRAM (dynamic RAM), 212
Draper, John, 328
DRII (Disaster Recovery Institute International), 409
dry pipe water sprinklers, 385
DSL, 268
DSS (decision support system), 184-185
DSSS (direct-sequence spread spectrum), 270
dual-homed gateways, 265
dual-homed host firewalls, 322
dumpster diving, 315, 368
duplex communication, 225
durability of locks, 378
DVDs (digital video discs), 213
dwell time, 270
dynamic packet filtering, 321, 468

E

e-commerce models, 179-180
EA (enterprise architecture) plan, 73
EBCDIC (Extended Binary Coded Decimal Interchange Code), 225
ECC (Elliptic Curve Cryptosystem), 345
EDI (electronic data interchange), 180-181
edit controls, 167, 458-459
Edmondson, Dave, 89
EER (equal error rate), 467
electricity. *See* power systems
electronic vaulting, 434
email, 181-182
embedded audit modules, 47
emergency fixes, 208, 461
emergency response, 332-334
EMI (electromagnetic interference), 382
employee management, 89. *See also* employees
  termination procedures, 92
  training, 91
  background checks, 92
  employee handbooks, 90
  hiring practices, 89-90
employees
  hiring best practices, 452-453
  segregation of duties, 101-102
    compensating controls, 102-103
  roles, understanding, 100-101
encryption, 340-341
  asymmetric, 344
    ECC, 345
    RSA, 345
  cryptographic attacks, 351-352
  end-to-end, 350
  methods of, 341
  PKI, 347-348
  quantum cryptography, 345
  symmetric
    AES, 344
    DES, 343-344
    private key encryption, 342-343
end-to-end encryption, 350
ensuring compliance using sampling methods, 46-47
entity integrity, 171
EPO (emergency power-off) buttons, 382
ERD (entity relationship diagram), 455
ERP (enterprise resource planning), 98
establishing risk management team, 33-34
estimating
  project tasks completion times, 127
  software costs, 122-123
  software size, 123-124
estimating ARO, 416
Ethernet, 243
ethical hacking, 337
EULA (End-User License Agreement), 230
evidence, 47
  reliability of, 48
exam. *See also* practice exams
  job practice areas, 2-4
  objectives, 2-4
  preparing for
    methods of, 7-9
    resources, 4-5
    study tips, 9-10
executive management, role in information security, 295
exterior controls for physical security, 372
  bollards, 373
  fences, 372-373
  gates, 373
  guard dogs, 374
  lighting, 374
  low-key building design, 374

F

FACTA (U.S. Fair and Accurate Credit Transaction Act), 25
fail safe locks, 376
fail soft locks, 376
FAR (false acceptance rate), 388, 467
fault tolerance, 256
FCR (first call resolution), 200
FEA (Federal Enterprise Architecture) reference model, 73
feedback, emailing to author, 6
fences as physical security control, 372-373
FHSS (frequency-hopping spread spectrum), 270
fiber-optic cable, 257
fiduciary responsibility of auditor, 39
fields, 226

file servers, 216
final acceptance testing, 137
financial audits, 41
fingerprint-scanning systems, 388
fire prevention, detection, and suppression, 384-385
  Halon, 386
  water sprinklers, 385-386
firewalls, 217, 263, 321-322, 468
  application proxies, 263
  circuit-level proxies, 264
  dual-homed gateways, 265
  packet filters, 264
  screened host firewalls, 265
  stateful inspection, 264
  stateless, 322
FireWire, 214
FISMA (U.S. Federal Information Security Management Act), 25
floppy disks, 212
foreign keys, 226
forensic audits, 41
FORTRAN, 222
FPA (function point analysis), 123
FQDNs (fully qualified domain names), 249
fragmentation attacks, 317
Frame Relay, 267
FRAP (Facilitated Risk Assessment Process), 88
fraud, 49
FRR (false reject rate), 467
FRR (false rejection rate), 388
FTP (File Transfer Protocol), 248
full backups, 432
full operation testing, 424, 473
full-mesh topology, network redundancy, 256
function point analysis, 125
function points, 124
function tests, 456
fuzzing, 317

G

Gantt charts, 125
gates as physical security control, 373
gateways, 260
general control procedures, 37, 449-450
general user state, 211
generations
  of computer languages, 464
  of programming languages, 223
generators, 383
goals
  of IT governance best practices, 67-68
  of logical security, 294
governmental information classification system, 392
grandfather-father-son tape rotation scheme, 433
granularity, 226
guard dogs as physical security control, 374
guards as physical security control, 379-380
guidelines, 78
  for ISACA auditing, 29-30
  versus standards, 28

H

hackers, 331
Halon, 386, 470
Halstead Complexity Measures, 124
handling confidential information, 312-313
hard changeover, 456
hard disk drives, 212
hardware
  capacity management, 220-221
  computers, 214
  CPU, 210
  I/O bus standards, 213
  maintenance, 219
  memory, 212
  monitoring, 219
  recovery mechanisms, 429
    RAID, 430-431
  RFID tags, 218-219
  tape-management systems, 219
hardware error reports, 219
hashing, 346-347
HDMS (hierarchical database-management systems), 464
HDMSs (hierarchical database-management systems, 227
help desk, 204-206, 274
  problem escalation, 205
  trouble tickets, 204
HIDS (host-based intrusion-detection systems), 323
Hill, Zachary, 315
HIPAA (U.S. Health Insurance and Portability and Accountability Act), 25
hiring employees, best practices, 452-453
honey nets, 324
honey pots, 324
host-to-host layer (TCP/IP model), 252-253
hot fixes, 208
hot site facilities, 426
hot-swappable disks, 430
HR (human resources), employee management, 89
  employee handbooks, 90
  hiring practices, 89-90, 452-453
  termination procedures, 92
  training, 91
HTML (Hypertext Markup Language), 272
HTTP (Hypertext Transfer Protocol), 249, 272
hubs, 217, 259-261
HVAC systems, 383
hybrid password-cracking attacks, 317

I

I&A (identification and authentication) process, 303
- authentication by characteristic, 306-307
- authentication by knowledge, 304-305
- authentication by ownership, 305

I/O bus standards, 213-214

identification as physical security control, 380

identifying
- assets, 81-83
- threats, 81

identity theft, 367-368

IDSs, 323-324, 468
- as physical security control, 380-381

IDSs (intrusion detection systems), 217

implementation phase of SDLC, 139-140

implementing physical security policies, 391

incident classification, 406-407, 470-471

incident handling, 201
- delay window, 202
- responding to incidents, 330-332
  - auditing information security, 335-336
  - computer forensics, 334-335
  - emergency response, 332-334

incremental backups, 432

incremental development, 142, 456

independence of auditor, necessity of, 40

indicators of fraud, 49

influence organizational form, 119

information assets
- classifying, 296-297
- evaluating, 296

information classification methods, 392-394

information security governance, funding, 73

information systems control, 37, 449-450
- audits, 41
- maintenance practices, 146
- sourcing, 93
  - SLAs, 95-96

infrastructure security, auditing, 337
- change management, 339-340
- network assessments, 339
- penetration testing, 337-339

input controls, 160-162

integrated auditing, 51-52

integrity, role in IS, 295-296

integrity-based data classification system, 297

interface testing, 137

interior controls for physical security, 375
- doors, 375-376
- locks, 377-378
- walls, 377
- windows, 376

internal controls, general control procedures, 37

Internet
- CGI, 273
- cookies, 273
- development of, 272
- firewalls, 321-322
- Java, 273
- privacy issues, 273
- URLs, 272

internet layer (TCP/IP model), 250-252

interoffice communication, securing, 392

interpreters, 222, 463

interruptions, types of, 418

IOCE (International Organization of Computer Evidence), 335

IP (Internet Protocol), 247

IPsec (IP Security), 350

IPSs (intrusion prevention systems), 217, 324

IPv6, 251

IS operations
- change-management process, 206-207
  - post-deployment, 209
  - program library systems, 207-208
  - release management, 208-209
- help desk and support, 204-206
- resource monitoring, keystroke monitoring, 200
- resource usage, monitoring, 200
  - abnormal events, tracking, 202-203
  - incident handling, 201
  - problem management, 202

IS security steering committee, 295

ISA (Industry Standard Architecture) bus, 213

ISACA (Information Systems Audit and Control Association), 38
- auditing standards, 28-29
  - code of ethics, 31
  - guidelines, 29-30
  - procedures, 30-31
  - website, 30

ISDN, 268

ISO (International Organization for Standardization), 244
- OSI reference model. *See* OSI reference model

ISO 17799, 76

ISO 9001 certification, 96

ISPs, 272

IT governance, 67, 99
- asset identification, 81-83
- auditor's role in, 69
- best practices, goals of, 67-68
- bottom-up policy development, 451
- change management, 95
- CobiT, 454
- documentation, reviewing, 78-79
- employee management, 89
  - employee handbooks, 90
  - termination procedures, 92
  - training, 91
  - hiring practices, 89-90
- employee roles, 100-101
  - segregation of duties, 101-103
- guidelines, 78
- information security governance, funding, 73
- performance, measuring, 71-72
- policies, 76-77
- procedures, 77
- quality management, 96-98
  - CobiT, 98
  - COSO, 99
  - ERP, 98
- risk assessment
  - qualitative, 87-88
  - quantitative, 83-86
- risk management, 79-80
- sourcing, 93
  - SLAs, 95-96
- standards, 78
- steering committee, 70
- threat identification, 81
- top-down policy development, 75-77, 451

IT steering committee, 70

ITF (integrated test facilities), 47

ITGI (IT Governance Institute), 38

J

Java, 222, 273

JBOD (Just a Bunch of Disks), 431

K

Kaplan, Robert, 71

Kerberos, 308-309

kernel mode (CPU), 211

kernel proxy, 321, 468

key roles in logical security, 295-296

key verification, 94

keys, bump keys, 379

keystroke monitoring, 200

Kilby, Jack, 212

kitchen sink syndrome, 136

KLOC (kilo lines of code), 123

knowledge-driven DSS, 184

known plain-text attacks, 351

L

LANs (local area networks), 243
- security, 325

laptops, 215

latency, 274

Layer 1. *See* physical layer (OSI reference model)

Layer 2. *See* data-link layer (OSI reference model)

Layer 3. *See* network layer (OSI reference model)

Layer 4. *See* transport layer (OSI reference model)

Layer 5. *See* session layer (OSI reference model)

Layer 6. *See* presentation layer (OSI reference model)

Layer 7. *See* application layer (OSI reference model)

layered approach to physical security controls, 371

layers of OSI reference model
- application layer, 246
- data link layer, 247
- network layer, 247
- physical layer, 247
- presentation layer, 246
- session layer, 246
- transport layer, 246

layers of system-access controls, 299-300

layers of TCP/IP model
- application layer, 253-254
- host-to-host layer, 252-253
- internet layer, 250-252
- network access layer, 250

legislation
- Safe Harbor Act, 24
- SOX, 40
- verifying compliance with external regulations, 25-26

lifecycle management
- alternative application-development techniques, 142-145
- business application development, 130-131
  - systems-development methodology, 131-132
- project management, 117
  - key roles, 118
  - project control and execution, 128
  - project culture and objectives, 119-120
  - project initiation, 121
  - project organizational forms, 119
  - project planning, 121-128
  - projects, closing, 128-129

lighting as physical security control, 374

lights-out operations, 200

link-state routing protocols, 252

load balancers, 217

locks
- as physical security control, 376-378
- durability of, 378
- picking, methods of, 378
- scrubbing, 379
- tubular, 377
- tumbler locks, 377
- warded locks, 377

logging as logical access control, 311-312

logical access controls, 303
- attacks
  - active, 314-319
  - passive, 313-314

auditing and logging, 311-312
I&A process, 303
authentication by characteristic, 306-307
authentication by knowledge, 304-305
authentication by ownership, 305
remote-access security, 309-311
single sign-on, 307-309
logical bombs, 316
logical security
goals of, 294
IS protection mechanisms, 294-295
key roles, 295-296
network infrastructure
firewalls, 321-322
IDSs, 323-324
on client/server networks, 324-325
on LANs, 325
on wireless LANs, 326-328
low-key building design as physical security control, 374

M

MAC (mandatory access control), 302, 466
MAID (Massive Array of Inactive Disks), 432
mainframes, 215
major releases, 208, 461
MAN (metropolitan area network), 243
man-in-the-middle attacks, 351
man-made physical security vulnerabilities, 366-367
sources of attacks, 370-371
manual authorization controls, 160
masquerading, 318
material risks, 36
McCarty, Eric, 172
measuring performance, 71-72
media rotation, 433
memory, 212
ROM, 462
secondary storage, 212, 224
mesh topology, 255
metadata, 226
Metcalfe, Robert, 243
MIB (management information base), 275
military data-classification system, 297
minor releases, 208, 461
mitigating risks, 34, 448
mobile sites, 426
model-driven DSS, 184
modems, 260
monitoring
hardware, 219
resource usage, 200
abnormal events, tracking, 202-203
incident handling, 201
problem management, 202
risks, 35
MPLS (Multiprotocol Label Switching), 267
MTBF (mean time between failures), 429
MTD (maximum tolerable downtime), 426
MTTR (mean time to repair), 430
multicast transmission, 251
multiple encryption, 343
multiprocessor CPUs, 211, 461
multiprogramming CPUs, 210, 461
multitasking CPUs, 210, 461

N

NAT (Network Address Translation) , 266, 322
national access points, 272
naturally occurring physical security vulnerabilities, 365-366
NDMS (network database-management systems), 464
NDMSs (network database-management systems), 227
network access layer (TCP/IP model), 250
network administration
help desks, 274
SNMP, 275
network analysis, 314
network infrastructure
controls, 319-320
firewalls, 321-322
IDSs, 323-324
physical controls, verifying, 276
pre-deployment considerations, 258
network layer (OSI reference model), 247
network protection methods, 434-435
network services, 248-249
network sniffers, 313
networks
devices, 465-466
elements of, 462-463
topologies, 465
neural IDS detection, 323, 469
NIDS (network-based intrusion detection systems), 323
noncritical systems, 472
nonstatistical sampling, 46
Norton, David, 71
NSPs, 272

O

objectives of audit, defining, 45
OBS (object breakdown structure), 120
OFDM (orthogonal frequency-division multiplexing), 270
off-site storage, 433
on-site storage, 433
online UPS systems, 383
OOSD (object-oriented systems development), 145
operational audits, 41
organization of book, 6-7

- **organizational framework of projects, 119**
- **OSI reference model, 244**
  - application layer, 246
  - data link layer, 247
  - network layer, 247
  - physical layer, 247
  - presentation layer, 246
  - session layer, 246
  - transport layer, 246
  - versus TCP/IP model, 249
- **OSs (operating systems), 223**
  - supervisory mode, 224
- **OSSTMM (Open Source Security Test Methodology Manual), 338**
- **output controls, 166-167, 459**

P

- **packet filtering, 263-264, 321, 468**
- **packet-switched WANs, 267-268**
- **PAN (personal area network), 243**
- **paper testing, 423, 473**
- **parallel simulation, 47**
- **parallel tests, 456**
- **passive attacks, 313-314, 467**
- **passive RFID tags, 218**
- **password-cracking attacks, 317**
- **PBX (private branch exchange), 328-329**
- **PCI (Peripheral Component Interface) bus, 213**
- **PCMCIA (Personal Computer Memory Card International Association) cards, 213**
- **PDAs, handheld computers, 215**
- **PDCA (Plan-Do-Check-Act), 209**
- **peer-to-peer networks, 215**
- **penetration testing, 337-339**
- **performance, measuring, 71-72**
- **personnel controls for physical security, 379**
  - guards, 379-380
  - identification, 380
  - IDSs, 380-381
- **PERT (Program Evaluation and Review Technique), 125**
  - project completion times, calculating, 127
- **PGP (Pretty Good Privacy), 349**
- **phased changeover, 456**
- **phases of DHCP operation, 254**
- **phases of SLDC implementation, 142**
- **phishing, 315**
- **phreakers, 328, 331**
- **physical layer (OSI reference model), 247**
- **physical security**
  - authentication, 387
    - biometrics, 387-389
  - breaches, sources of, 370-371
  - controls, 371
  - environmental controls
    - backup power supplies, 381-383
    - fire prevention, detection, and suppression, 384-386
    - HVAC, 383
  - exterior controls, 372-374
  - interior controls, 375
    - doors, 375-376
    - locks, 377-378
    - windows, 376-377
  - personnel controls, 379
    - guards, 379-380
    - identification, 380
    - IDSs, 380-381
  - policies, 389
    - commercial information classification system, 393
    - defining, 390
    - governmental information classification system, 392
    - implementing, 391
    - purposes of, 390
  - vulnerabilities, 365
    - man-made events, 366-367
    - natural events, 365-366
- **PIA (privacy impact analysis), 298, 466**
- **picking locks, methods of, 378**
- **PIDAS (perimeter intrusion and detection assessment system), 373**
- **pilot tests, 456**
- **ping command, 274**
- **ping of death, 318**
- **PKI (public key infrastructure), 347-348, 469-470**
- **plan design and development, 419-420**
- **plenum-grade cable, 256**
- **policies, 76-77**
  - disaster recovery, corrective control, 76
  - for physical security, 389
    - commercial information classification system, 393
    - defining, 390
    - governmental information classification system, 392
    - implementing, 391
    - purposes of, 390
  - reviewing, 78-79
- **policy development, 75, 77**
- **POP3 (Post Office Protocol version 3), 249**
- **portable wireless devices, 271**
- **post-deployment change-management process, 209**
- **post-implementation phase of SDLC, 140**
- **POTS (plain old telephone system), 268**
- **power systems**
  - anomalies vulnerable to, 381
  - EPO buttons, 382
  - protecting, 382
    - UPSs, 382-383
- **practice exams**
  - answers, 509-525
  - questions, 476-508
- **preaction water sprinklers, 385**
- **preparedness testing, 424, 473**
- **preparing for exam**
  - methods of, 7-9
  - resources, 4-5
  - study tips, 9-10
- **presentation layer (OSI reference model), 246**
- **pretexting, 315**
- **PRI (primary rate interface), 268**

- **print servers, 216**
- **privacy, 298**
  - and trust, 298-299
  - Internet issues, 273
  - WEP, 326
- **private IP addresses, 322**
- **private key encryption, 342-343**
- **problem escalation, 205**
- **problem management, 202**
- **procedures, 77**
  - for ISACA auditing, 30-31
  - reviewing, 78-79
- **process owner, role in information security, 295**
- **processing controls, 162-164, 458**
  - data file controls, 165-166
- **program library systems, 207-208**
- **program servers, 216**
- **programming languages, 222**
  - generations of, 223
- **project management, 117**
  - auditing, 177-178
  - CPM, 455
  - key roles, 118
  - project control and execution, 128
  - project culture and objectives, 119-120
  - project initiation, 121
  - project organizational forms, 119
  - project organizational types, 454
  - project planning, 121
    - critical paths, 127
    - scheduling, 125-127
    - software cost estimation, 122-123
    - software size estimation, 123-124
    - timebox management, 128
  - projects, closing, 128-129
  - role in BCP process, 410
  - SDLC, 455
- **protecting power systems, 382**
  - UPSs, 382-383
- **protocol analyzers, 275**
- **protocols, 244**
- **prototyping, 143, 457**
- **proxies, 263, 321**
  - application proxies, 263
  - circuit-level proxies, 264
- **proxy servers, 216**
- **public key encryption, 344**
- **public relations, role in disaster recovery process, 408**
- **pure project organizational form, 119**

Q

- **qualitative risk assessment, 87-88**
- **quality management, 96-98**
  - CobiT, 98
  - COSO, 99
  - ERP, 98
- **quantitative analysis, 412**
- **quantitative risk assessment, 83-86, 452-453**
- **quantum cryptography, 345**
- **questionnaires, information gathering for BIA, 413**
- **questions (practice exam), 476-508**

R

- **RAD (rapid application development), 143, 457**
- **RADIUS (Remote Access Dial-In User Service), 310**
- **RAID (Redundant Array of Inexpensive Disks), 430-431**
- **rainbow tables, 318**
- **RAM (random access memory), 212, 259**
- **RBAC (role-based access control), 302-303**
- **RDMSs (relational database-management systems), 228, 464**
- **real-world cryptographic solutions, 349-350**
- **reciprocal agreements, 428**
- **recovering**
  - from hardware failures, 429
    - RAID, 430-431
  - from software failures, 431-432
- **recovery alternatives, 425**
  - alternate processing sites, 426-429
- **recovery strategies, 417-419**
  - interruptions, types of, 418
- **red team activities, 337**
- **redundant processing sites, 426**
- **reengineering, 144**
- **referential integrity, 170**
- **regression tests, 456**
- **regulatory standards, 24-25. *See also* legislation**
  - verifying compliance with, 25-26
- **relational integrity, 171**
- **release management, 208-209, 461**
- **reliability of evidence, determining, 48**
- **remote-access security, 309-311**
- **repeaters, 259-261**
- **Rescorla, Rick, 384**
- **resource usage, monitoring, 200**
  - abnormal events, tracking, 202-203
  - incident handling, 201
  - keystroke monitoring, 200
  - problem management, 202
- **responding to incidents, 330-332**
  - auditing information security, 335
    - data ownership, 335-336
    - security baselines, 336
  - computer forensics, 334-335
  - emergency response, 332-334
- **reviewing policies, 78-79**
- **RFI (radio frequency interference), 382**
- **RFID tags, 218-219**

- **right-to-audit statements, 94**
- **Rijndael, 344**
- **ring topology, 255**
- **risk analysis, 32**
  - categories of risk, 32-33
  - material risks, 36
  - risk-based auditing, 35-36
- **risk assessment**
  - qualitative, 87-88
  - quantitative, 83-86
- **risk management, 33, 79**
  - monitoring phase, 35
  - risk management team, establishing, 33-34
  - risk mitigation, 34
- **risks**
  - mitigating, 448
  - transferring, 449
  - types of, 448
- **RMON (Remote Monitoring), 275**
- **roles**
  - of auditor in IT governance, 69
  - of employees, understanding, 100-101
    - segregation of duties, 101-103
  - project management-related, 118
- **roll-up fixes, 208**
- **ROM (read-only memory), 212, 462**
- **rounding-down attacks, 317**
- **routers, 217, 260**
- **routing protocols, 251**
- **Royce, W.W., 131**
- **RPO (recovery point objective), 414, 472**
- **RSA encryption, 345**
- **RTO (recovery time objective), 414, 472**

S

- **S-HTTP (Secure Hypertext Transfer Protocol), 349**
- **S/MIME (Secure Multipurpose Internet Mail Extensions), 349**
- **Safe Harbor Act, 24**
- **salami technique, 317**
- **sampling, 46-47, 450**
- **sandbox scheme, 222**
- **SANs (storage area networks), 243, 434**
- **SAS 70 reports, 95**
- **satellite systems, 257**
- **SCADA (U.S. Supervisory Controls and Data Acquisition), 25**
- **SCARF/EAM (systems control audit review file and embedded audit modules), 460**
- **scheduling project tasks, 125**
  - estimating task completion times, 126-127
- **SCM (supply chain management), 186**
- **scope creep, 136**
- **screened host firewalls, 265, 322**
- **screened subnets, 265**
- **script kiddies, 331**
- **scrubbing locks, 379**
- **scrum, 144, 457**
- **SCSI (Small Computer Systems Interface) bus, 213**
- **SDLC (system development lifecycle), 117, 455**
  - application disposal, 140-141
  - business application development, 130-131
    - systems-development methodology, 131-132
  - changeover methods, 456
  - design phase, 136
  - development phase, 136-139
  - feasibility, 133
  - implementation phase, 139-140
  - phases of, 142
  - post-implementation phase, 140
  - project management, 117
    - key roles, 118
    - project control and execution, 128
    - project culture and objectives, 119-120
    - project initiation, 121
    - project organizational forms, 119
    - project planning, 121-128
    - projects, closing, 128-129
  - requirements definition, 133-135
  - testing phase, 456
- **secondary storage, 212, 224**
- **security**
  - authentication, biometric systems, 466
  - baselines, establishing, 336
  - defense-in-depth, 293
  - firewalls, 263, 468
    - screened host firewalls, 265
  - information security governance, funding, 73
  - logical
    - goals of, 294
    - IS protection mechanisms, 294-295
    - key roles in, 295-296
    - logical access controls, 303-312
  - of wireless networks, 271
  - physical controls, 470
    - verifying, 276
- **security advisory group, role in information security, 295**
- **segregation of duties, 101-102**
  - compensating controls, 102-103
- **semipassive RFID tags, 218**
- **semiquantitative analysis, 88**
- **sensitive information**
  - destroying, 369-370
  - privacy issues, 298-299
- **sensitive systems, 472**
- **servers, 215**
- **service packs, 208**
- **session layer (OSI reference model), 246**
- **SET (Secure Electronic Transaction), 349**
- **shared cost method of security system funding, 73**
- **shredders, types of, 369**
- **signature IDS detection, 323, 469**

simple backup-rotation schemes, 433
simplex communication, 225
single sign-on, 307-309
site licensing, 230
size of software, estimating, 123-124
SLAs (service level agreements), 95-96, 199
SLE (single loss expectancy), calculating, 86, 416
SLOC (source lines of code), 123
SMTP (Simple Mail Transfer Protocol), 248
smurf attacks, 318
sniffers, 275
SNMP (Simple Network Management Protocol), 249, 275
sociability tests, 456
social engineering, 314
software
- cost estimation, 122-123
- licensing issues, 230
- size estimation, 123-124
- testing, 455-456

software development, 221
- decompilers, 223
- programming languages, 222
- sandbox scheme, 222

software escrow, 434
software recovery, 431-432
source code, verifying, 460
sources of physical security breaches, 370-371
sourcing, 93
- SLAs, 95-96

SOX (Sarbanes-Oxley Act), 25, 40
spiral application development model, 143, 457
sponsor payment method of security system funding, 74
spreading code, 270
sprints, 144
SSH (Secure Shell), 349
SSIDs (Service Set IDs), 269
SSL (Secure Sockets Layer), 349
standards, 28, 78
- ISACA auditing standards, 28-29

standby database shadowing, 434
standby UPS systems, 383
standing data, 165
star topologies, 255
stateful inspection firewalls, 264, 321, 468
stateless connections, 249
stateless firewalls, 322
statistical IDS detection, 323, 468
statistical sampling, 46
steering committee, 70
stochastic events, 85
store-and-forward switching, 260
STP (shielded twisted-pair), 256
strategic planning, 26
stream cipher algorithm, 343
strip-cut shredders, 369
strong matrix organizational form, 119
study tips, 9-10
subnetworks, 250
substantive testing, 46
substantive tests, 28
supercomputers, 215
supervisory mode, 224
SURRE (Sufficient, Useable, Reliable, Relevant, Effective) rule, 47
switches, 217, 259-261
symmetric encryption, 341
- AES, 344
- DES, 343-344
- private key encryption, 342-343

symmetric encryption algorithms, 469
syn floods, 319
system access
- access creep, 301
- discretionary access control, 301
- layers of security controls, 299-300
- mandatory access control, 302
- role-based access control, 302-303

system testing, 137
System-control parameter, 165
systems development, auditing, 176-177

T

T-carriers, 268
TACACS, 310
tactical planning, 26
tape-management systems, 219
tasks, CPM, 127
TCP (Transmission Control Protocol), 246
TCP/IP model
- application layer, 253-254
- host-to-host layer, 252-253
- internet layer, 250-252
- network access layer, 250
- versus OSI reference model, 249

technical support, 204, 206
telecommunications recovery, 434-435
TEMPEST, 314
TES (terminal-emulation software), 249
testing applications, 172-173
testing methodologies, 137
testing phase of BCP process, 421-423
- full operation testing, 424
- paper tests, 423
- preparedness testing, 424

testing software, 456
tests (practice)
- answers, 509-525
- questions, 476-508

threat identification, 81
threats, 32. *See also* incident handling

timebox management, 128
tokens, 305
top-down policy development, 75, 451
top-down testing, 137
topologies, 254-255, 465
Tower of Hanoi tape-rotation scheme, 434
tracking abnormal events, 202-203
training and awareness, role in BCP process, 420-421
Transaction files, 165
transaction integrity, 46
transferring risks, 449
transport layer (OSI reference model), 246
trend-/variance-detect tools, 311
Trinoo attacks, 319
Trojan horse programs, 316
trouble tickets, 204
TSF (time service factor), 199
tubular locks, 377
tumbler locks, 377
tuples, 228
twisted-pair cable, 256
two-factor authentication schemes, 305

U

UAs (uptime agreements), 199
UDP (User Datagram Protocol), 246
unicast transmission, 251
Unicode, 226
unit testing, 137
UPSs (uninterruptible power supplies), 382-383
URLs, 272
USB, 214
user mode (CPU), 211
utilization reports, 219
UTP (unshielded twisted-pair), 256

V

vandalism, 366
VANs (value-added networks), 180
variable sampling, 46, 450
variance detection tools, 200
verifying
  BCP, 436-437
  compliance with external regulations, 25-26
  disaster recovery plans, 436-437
  network infrastructure physical controls, 276
  source code, 460
virtual memory, 224
viruses, 316, 329-330
Visual Basic, 222
vital systems, 472
VLANs (virtual LANs), 261
voice communications
  PBX systems, 328-329
  phreakers, 328
  VoIP, 329
VoIP (Voice over IP), 268, 329
VPNs (virtual private networks), 310
vulnerabilities
  to physical security, 365
    breaches, sources of, 370-371
    man-made events, 366-367
    natural events, 365-366
  to power systems, 381

W

walk-through testing, 423
walls as physical security control, 377
WANs (wide area networks), 243
  circuit-switched, 268
  packet-switched, 267-268
war chalking, 327
war dialing, 316
war driving, 327
warded locks, 377
warm sites, 427
water sprinklers, 385-386
waterfall development model, 131, 456
WBAD (web-based application development), 145
WBS (work breakdown structure), 120
weak matrix organizational form, 119
web browsers, 272-273
web servers, 216
web-based trouble tickets, 204
websites
  DRII, 409
  ISACA, 9
  ISACA auditing standards, 30
  ISACA code of ethics, 32
WEP (Wired Equivalent Privacy), 269-271, 326
wet pipe water sprinklers, 385
white-box tests, 456
windows as physical security control, 376
wireless APs, 260-261
wireless communication, 257
  APs, 260-261
wireless devices, 271
wireless LANs, security, 326-328
wireless networks, 269
  802.11 standards, 269
  broadcasting methods, 270
  security, 271
World Wide Web, 272
WPAN (wireless PAN), 243
WPs, documenting audit findings, 43-45

X-Y-Z

X.25, 267
XP (extreme programming), 143, 457

Zachma, John, 73