

Index

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

A

- Abagnale, Frank, 377
- Absolute Software, 351
- accept risk response, 71
- acceptable use policy (AUP)
 - violations, 354
- access paths
 - documentation, 386
- access point (APs) in wireless networks, 235, 420
- access servers, 231
- accountability
 - in audit charters, 61
 - in software controls, 400
 - in WLANs, 423
- accounts
 - login, 342–343
 - maintenance, 343, 379–380
 - managing, 341–342
- accreditation in SDLC, 297
- ACID (atomicity, consistency, isolation, and durability) model, 306
- acquisition phase in problem management, 356–357
- act step in process technique, 69, 69
- activation criteria for
 - emergency response, 477
- active attacks, 377–382, 381
- active content, 346
- Active Server Pages (ASP), 347
- ActiveX, 347
- activities in business process
 - documentation, 159
- ad hoc wireless networks, 235–236, 419
- adapting in benchmarking, 160
- adaptive responses, 414
- Address Resolution Protocol (ARP), 208–209
- “addressed” term, 24
- addresses
 - IP, 207–209, 208
 - MAC, 205, 205–206, 208–209, 208
 - spoofing, 234
- Adelphia Communications Corporation, 3
- administrative audits, 10
- administrative controls, 83, 351–352
- administrative protection of
 - assets, 382
 - access paths
 - documentation, 386
 - authority roles, 384–385
 - data retention
 - requirements, 385–386
 - information security
 - management, 382–383
 - IT governance, 383–384
 - personnel management, 387–389
- administrators
 - database, 332
 - network, 195, 331
 - server, 331
 - on steering
 - committee, 122
- Advanced Encryption Standard (AES), 427
- advisory policies, 131
- after-image journals, 306
- Agile development method, 287–288, 288
- air-conditioning equipment, 393, 395
- alarm systems, 390–391
- Alexander, Jacob “Kobi”, 3
- aligning software to business needs, 261–263
- allocating staffing, 75–76
- alternate communications in
 - business continuity, 487
- alternate processing
 - locations in business continuity, 471
- Amazon.com, 119
- America West Airlines (AWA), 454
- American Apparel company, 137
- American Institute of Certified Public Accountants (AICPA), 13
- American International Group (AIG), 3
- amnesty, 8–9, 143
- AMR company, 128
- analysis
 - for benchmarking, 160
 - Business Impact Analysis, 160–162, 467–469, 468
 - in evidence life cycle, 94
 - Function Point Analysis, 273–275, 274
 - host traffic, 376–377
 - in incident handling, 355
 - risk. *See* risk assessment and analysis
 - test results, 100–101
- annual loss expectancy (ALE), 144
- antivirus (AV) software, 345
- AOL, 455
- applets, 347
- appliance devices, 191
- application controls
 - description, 82
 - monitoring, 344–345
 - in security, 400–401
- Application layer in OSI model, 214–215, 214
- application management
 - plans for strategy implementation, 132
- application proxy filters, 414

548 applications programmer responsibilities – authorization

- applications programmer responsibilities, 331
 - architecture
 - computer, 184–187, 185–188
 - data, 301–306, 303–306
 - program, 309
 - Arthur Andersen, 3
 - artificial intelligence (AI), 308
 - assembly language, 284
 - assessments
 - audit risk, 73
 - vs. audits, 10–11, 69–70
 - physical maps for, 386
 - project risk, 162–164
 - asset value (AV) in risk management, 144
 - assets
 - defined, 5
 - disposal process, 351–352
 - protecting. *See* information asset protection
 - tracking, 351
 - associate level DSS, 307
 - assurance level controls, 81
 - Asynchronous Transfer Mode (ATM), 232, 234
 - attack methods, 376
 - active, 377–382, 381
 - passive, 376–377
 - attackers, 373–376
 - attestation, 104
 - attributes
 - database, 304, 304
 - sampling, 98
 - auction software, 255
 - audit charters, 60–61
 - audit committees in, 62–63, 62
 - engagement letters, 63
 - ISACA standards, 14
 - audit coefficients, 99
 - audit committees, 28, 62–63, 62
 - audit evidence, 85
 - CAAT for, 87–89
 - documentation, 96
 - electronic discovery, 89–90
 - grading, 90–92
 - life cycle, 93–95, 95
 - for proof, 85–86
 - samples, 96–98, 97
 - timing, 92
 - types, 86
 - typical, 86
 - audit process, 59–60, 61
 - audit charters, 60–63, 62
 - audit evidence. *See* audit evidence
 - audit risk assessment, 73
 - auditee communication requirements, 77–78
 - data collection techniques, 78–80
 - exam essentials, 105–107
 - feasibility determination, 74
 - follow-up activities, 105
 - internal controls, 80–85
 - preplanning. *See* preplanning
 - quality control, 77
 - reporting, 103–104
 - review questions, 108–116
 - staffing allocation, 75–76
 - summary, 105
 - testing in, 98–102
 - audit rights in SLAs, 337
 - audit risk assessment, 73
 - auditees, 11
 - communication requirements, 77–78
 - IT environment, 79–80
 - preplanning audits duties, 67
 - auditing overview, 2
 - vs. assessments, 69–70
 - auditor vs. auditee, 11
 - audits vs. assessments, 10–11
 - code of professional ethics, 6–8
 - communication and integration, 21
 - compensating controls, 352
 - confidentiality, 19–20
 - conflicts and failures, 24
 - corporate organizational structure, 27–31, 28, 30
 - demand for, 2–5
 - documentation, 21
 - ethical conflicts, 8–9
 - evidence rule, 25–26
 - exam essentials, 48–49
 - independence test, 11–13
 - interviews, 26–27
 - lawyer relationships, 20
 - leadership duties, 22
 - priorities, 22–23
 - project management. *See* project management
 - purpose, 9
 - regulations for best practices, 16–18
 - responsibility, 10
 - review questions, 50–58
 - standard terms of reference, 23–24
 - standards, 13–16, 16
 - summary, 48
 - types, 9–10, 18–19
 - value, 24–25
- auditor interests and duties
 - preplanning audits, 67
 - SDLC phases
 - Development, 293
 - Disposal, 301
 - Feasibility Study, 275–276
 - Implementation, 299
 - Postimplementation, 300
 - Requirements
 - Definition, 279
 - System Design, 283
 - tactical management, 168
 - authentication, 400–402
 - biometrics. *See* biometrics
 - types, 402–403, 402–403
 - WLANs, 422
 - authentication headers (AHs), 419
 - authenticode, 347
 - authority and authority roles
 - in audit charters, 61
 - over data, 384–385
 - for emergency response, 479
 - for project managers, 36
 - authorization, 11
 - change, 349
 - software controls, 400

automated cable testers, 239
 automated controls, 399
 available evidence for
 metrics, 335
 avoid risk response, 71

B

background checks, 388
 backups
 business continuity
 strategy, 474–475
 logical, 356
 monitoring, 348
 policies for, 146
 triple mirror, 197
 badge readers, 390
 balanced matrix
 organizations, 36
 balanced scorecards,
 125–126, 127
 advantages, 126–127
 disadvantages, 127–128
 IT subset, 128–129
 bandwidth in fiber-optic
 cable, 223
 banking and investment
 industry, 5
 Basel Accord Standard II
 (Basel II), 14
 basements for data
 centers, 391
 basic care in preplanning
 audits, 68
 Basic Input/Output System
 (BIOS), 185
 BASIC programming
 language, 347
 bastion hosts, 415
 batch totals in processing
 controls, 344
 before-image journals, 306
 behavioral characteristics in
 biometrics, 405–406, 406
 benchmarking in BPR,
 159–160, 160
 benefits of software, 262
 best practices, regulations for,
 16–18
 betrayal, 374
 binding IP addresses, 208
 biometrics, 390, 403
 behavioral characteristics,
 405–406, 406
 disposal phase, 410
 feasibility, 407
 implementation, 409–410
 management, 406–407
 physiological
 characteristics,
 403–405, 404–405
 post-implementation, 410
 problems with,
 410–411, 411
 requirements, 407–408
 system configuration, 409
 system selection, 408–409
 BIOS (Basic Input/Output
 System), 185
 bitstream imaging, 356
 black-box testing, 292
 blackmail, 372
 Bluetooth technology, 236
 boards of directors, 27–28
 Boehm, Barry, 267, 273
 boiler insurance, 476
 bonding process, 388
 business continuity
 strategy, 475
 evidence storage
 facilities, 95
 boot strapping, 185
 Border Gateway Protocol
 (BGP), 211
 Bourne movies, 375
 Boyle, Dan, 3
 BPR. *See* business process
 reengineering (BPR)
 brand name valuing, 453
 “breaking the mirror” backup
 process, 197
 bridges, 216, 226
 British Standards, 13, 143
 broadcast domains, 205, 208
 broadcast IP addresses, 208
 browser functions, 346
 brute force attacks, 379
 buffers, 201
 build decision in SDLC,
 270–271
 burglar alarms, 390–391
 bus topologies, 217, 217
 business continuity (BC)
 best practices, 460, 460
 exam essentials, 489–490
 practice areas
 business impact
 analysis,
 467–469, 468
 crisis communications,
 486–487
 emergency response,
 476–479, 479
 initiation,
 461–463, 463
 integration with other
 plans, 488
 maintenance
 and testing,
 484–485, 486
 overview,
 458–461, 459
 plan creation,
 480–484,
 480–481
 risk analysis, 464–467,
 464–466
 strategy, 469–476, 476
 purpose, 454–456
 review questions, 491–499
 and steering
 committee, 122
 summary, 488
 training and
 awareness, 484
 uniting other plans with,
 457–458, 457
 Business Continuity Maturity
 Model (BCMM), 140
 business evolution, 150
 Business Impact Analysis
 (BIA), 160–162,
 467–469, 468
 business interruption (BI)
 insurance, 476
 business operations
 knowledge in
 preplanning process,
 63–64
 business process reengineering
 (BPR), 150
 application steps, 155–158

550 business risks – closing process group

- benchmarking, 159–160, 160
 - benefits, 151
 - Business Impact Analysis, 160–162
 - goals, 153
 - IS role, 158
 - knowledge
 - requirements, 154
 - methodology, 152
 - practical application, 164–166
 - principles, 153–154
 - process documentation, 158–159
 - project risk assessment, 162–164
 - selection methods, 166–167
 - techniques, 154–155, 159
 - tools, 159
 - troubleshooting, 167–168
 - business risks, 73
 - business-to-business (B-to-B) transactions, 310, 310
 - business-to-consumer (B-to-C) transactions, 310, 310
 - business-to-employee (B-to-E) transactions, 310, 310
 - business-to-government (B-to-G) transactions, 310, 310
 - business unit recovery teams, 484
 - buy decision in SDLC, 271
 - bytecoding, 285
-
- C**
- C programming language, 189
 - cable plants, 221
 - cables and cable types, 221
 - automated testers, 239
 - bus topologies, 217
 - coaxial, 221–222, 222
 - fiber-optic, 223, 223
 - laptops, 20
 - UTP, 222–223, 222
 - caches, 185
 - campus area networks (CANs), 238
 - candidate keys, 302
 - Capability Maturity Model (CMM), 140
 - levels, 141–142, 142
 - for performance management, 149, 150
 - for quality management, 255–256
 - vs. SDLC, 272
 - capacity management, 353
 - CASE tools, 287, 287
 - casualty insurance, 475
 - Catch Me If You Can movie, 377
 - CD-ROM drives, 199
 - CD-RW drives, 199
 - cells
 - in statistical sampling, 97
 - in wireless networks, 235, 420
 - Cendant, 3
 - central processing units (CPUs), 184–187, 185–187
 - centralization vs. decentralization, 309
 - centralized system logging, 340
 - certificate authorities (CAs), 432–433
 - certificate revocation lists (CRLs), 432, 434
 - certificates, digital, 403, 433–434
 - certification in SDLC, 294–297, 295
 - certification practice statements (CPS), 432, 434
 - certification testing, 271
 - CertTest Training Center, 32
 - chain of custody, 93–95, 95
 - Champy, James, *Reengineering the Corporation*, 153
 - change control, 169–170
 - change control boards (CCBs), 265
 - change control manager responsibilities, 331
 - change management and procedures authorization, 349
 - life cycle management, 265
 - in outsourcing contracts, 338
 - in SLAs, 337
 - changeover in SDLC, 297–298
 - channel service units (CSUs), 231
 - charge-backs in strategy selection, 130
 - charters, audit, 60–61
 - audit committees in, 62–63, 62
 - engagement letters, 63
 - ISACA standards, 14
 - check step in process technique, 68–69, 69
 - chief executive officers (CEOs), 26, 29
 - chief financial officers (CFOs), 29
 - chief information officers (CIOs), 29
 - chief operating officers (COOs), 29
 - chief privacy officers (CPOs), 383
 - chief security officers (CSOs), 383
 - China
 - banned products, 138
 - fish from, 71
 - cipher locks, 390
 - circuit-level firewalls, 414
 - circumstantial evidence, 86
 - classes, object, 305
 - classification controls, 400
 - information, 383–384
 - client duties in preplanning audits, 66
 - clients, 11
 - closed-circuit television, 389
 - closed system architecture, 309
 - closing process group, 38

- coaxial cable, 221–222, 222
- COBIT (Control Objectives for Information and related Technology), 14, 134
- code of professional ethics, 6–8
- coding. *See* Development phase in SDLC
- cold sites, 473
- colleague level DSS, 307
- collection process
 - in audit process, 78–80
 - in evidence life cycle, 93–94
- collisions in Ethernet networks, 206
- columns in databases, 304, 304
- commercial category in business continuity, 462
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 13
- Common Criteria (CC) standard, 294–297, 295
- communications, 21
 - auditee requirements, 77–78
 - managing, 43
- communications teams in business continuity plans, 483
- community strings, 240
- compensating controls, 352–353
- competence
 - evidence providers, 91–92
 - staff, 76
- competitive advantage
 - business continuity for, 455
 - in sourcing decisions, 137
- compiling software programs, 289, 290
- compliance, 6
 - sourcing issues, 137
 - testing, 13, 98
- compliance audits, 10
- computer architecture, 184–187, 185–188
- computer assisted audit tools (CAAT)
 - for data collection, 79
 - for evidence, 87–89
- computer console protection, 388
- computer networking. *See* networks and networking
- computer operator responsibilities, 332
- ConAgra, 138
- concerns in test results, 100
- Concurrent Version System (CVS), 291
- confidential classification, 384
- confidentiality, auditor, 19–20
- confidentiality agreements, 147
- configuration
 - controlling, 290, 349
 - managing, 289–291
 - reporting, 291
- confirmed delivery, 212
- conflicts
 - dealing with, 24
 - ethical, 8–9
- conformity in test results, 100
- consistency in
 - documentation, 96
- console protection, 388
- constraints in project management, 34
- Constructive Cost Model (COCOMO), 273–275, 274
- consultants, 30–31
- consulting firms
 - organizational structure, 29–31, 30
- containment in incident handling, 355
- context in classification schemes, 384
- continuity planning, 149. *See also* business continuity (BC)
- continuous and intermittent simulation (CIS) audits, 88
- continuous improvement, 150
- continuous online audits, 88–89
- contradictory evidence in test results, 101
- Control Objectives for Information and related Technology (COBIT), 14, 134
- control risks, 73
- control self-assessments (CSAs), 70, 438
- controls
 - applications, 82, 344–345, 400–401
 - classification, 400
 - internal, 80–82
 - reviewing, 82–84
 - in SDLC, 279
 - strong, 84–85
 - monitoring. *See* monitoring in planning and performance, 140–143, 142
- Converse Technology, 3
- cooperative recovery sites, 474
- copyright violations, 8
- core processes in business continuity strategy, 469–470
- corporate governance, 118
- corporate organizational structure, 27
- consulting firms, 29–31, 30
- roles, 27–29
- corrective controls, 83–84, 279
- corrective counseling policies, 148
- cost management, 41
- cost of service in SLAs, 337
- counseling policies, 148
- crackers, 374
- crash dumps, 356
- crash-restart attacks, 379
- credibility, losing, 372
- criminal cases
 - and investigations chain of custody, 93–95, 95
 - electronic discovery, 90
- crisis communications, 486–487
- critical functions in business continuity strategy, 470

552 critical paths – differential backups

critical paths, 45
 critical success factors (CSFs)
 business continuity, 461
 identifying, 261
 in strategy planning, 119
 Crosby, Philip, 68, 256, 280
 cross-network connectivity
 attacks, 380, 381
 crossover error rate (CER) in
 biometrics, 411, 411
 crystal-box testing, 292
 cultural risks in BPR, 164
 custodians, data, 385
 customer needs, business
 continuity for, 456
 customer satisfaction,
 281–282, 281
 customer support teams in
 business continuity
 plans, 483
 cut over, 297
 cyclic redundancy check
 (CRC) approach, 423

D

da Vinci, Leonardo, 152
 Daemen, Joan, 427
 Daisytek International, 455
 damage assessment teams, 482
 data
 architecture. *See* databases
 backups, 474
 collection techniques,
 78–80
 conversion plans, 294
 integrity, 146, 337
 retention requirements,
 385–386
 storage, 185,
 195–199, 198
 data bus, 185, 185
 data custodians, 385
 data dictionaries, 277
 Data Encryption Standard
 (DES), 427
 data entry staff
 business continuity
 plans, 483
 responsibilities, 332

data file controls, 343–344
 data link connection
 identifiers (DLCIs), 234
 Data-Link layer in OSI model,
 204–206, 204–206
 data marts, 307
 data mining, 307
 data-oriented databases
 (DODBs), 302–305,
 303–304
 data-oriented structured
 databases (DOSDs), 302
 data owners, 384
 data plans for strategy
 implementation, 132
 data process restrictions in
 BPR, 159
 data processing locations, 391
 data sets, 332
 data source for metrics, 335
 data users, 385
 data warehouses, 307, 308
 database administrator
 responsibilities, 332
 database schema for
 ERDs, 277
 databases, 301–302
 data-oriented, 302–305,
 303–304
 object-oriented, 305, 306
 security for, 401, 401
 servers, 191
 transaction integrity, 306
 de facto risk response, 71
 debugging, 291
 decentralization vs.
 centralization, 309
 decision support systems
 (DSSs), 307–308, 308
 decision trees for emergency
 response, 478
 decompiling requirements, 66
 dedicated telephone circuits,
 232–233, 233
 default gateways, 210
 default settings, 201
 defuzzification, 307
 degaussing, 399
 deleted file recovery, 356
 Delphi technique, 158
 demand for IS Audits, 2–5
 demilitarized zones (DMZs),
 416, 416
 Deming, Edwards, 68, 256
 denial of service (DoS)
 attacks, 195, 379
 Dense Wave Multiplexing
 (DWM), 223, 232
 department directors, 29
 depth of controls, 85
 design risks, 162–163
 desktop reviews in business
 continuity, 485
 detailed IS controls, 82
 details in outsourcing
 contracts, 338
 detection and analysis in
 incident handling, 355
 detection risks, 73
 detective controls, 83–84, 279
 deterrent controls, 82
 Development phase in SDLC,
 271, 283
 alternative development
 techniques,
 287–288, 288
 auditor interests, 293
 compiling software
 programs, 289, 290
 configuration and
 version management,
 289–291
 debugging, 291
 integrated development
 environment tools,
 286–287, 287
 programming languages,
 284–286, 285–286
 programming standards
 and quality control,
 283–284
 prototypes, 288–289
 review and approval, 293
 schedules, 284
 testing, 292–293
 diagnose step in BPR, 156
 diagramming techniques,
 45–48, 46–47
 dial-up access, 417
 diesel generators, 393
 difference estimation, 99
 differential backups, 475

- digital certificates, 403, 433–434
 - digital forensic investigations, 355–356
 - digital signatures, 430–434, 430–431, 433
 - Digital Subscriber Line (DSL), 232
 - direct evidence, 86
 - director responsibilities, 330
 - disaster recovery, 451–452.
 - See also* business continuity (BC)
 - brand names, 453
 - financial challenges, 452–453
 - rebuilding in, 453–454
 - Disaster Recovery Institute International (DRII), 452
 - disclosure, unauthorized, 372
 - discovery
 - electronic, 89–90
 - sampling, 98
 - discretionary access controls (DAC), 400
 - discretionary actions, 16
 - discretionary compliance, 6
 - discretionary control, 146
 - discretionary processes in
 - business continuity strategy, 470
 - disk management systems (DMSs), 196–198, 198
 - disk mirroring, 196–197, 198
 - disk strings, 196, 198, 198
 - disposal procedures
 - assets, 351–352
 - biometrics, 410
 - media, 399
 - SDLC, 271–272, 301
 - distributed denial of service (DDoS) attacks, 379
 - DMZs (demilitarized zones), 416, 416
 - do step in process technique, 68–69, 69
 - documentation
 - access paths, 386
 - archives, 20
 - audit, 96
 - BPR, 158–159
 - retaining, 21
 - reviewing, 78–79
 - DoD TCP/IP model, 203
 - Domain Name System (DNS), 191, 209, 214, 226–227, 227
 - domains, 205, 208
 - double mirror systems, 197, 198
 - downtime monitoring, 340
 - dry chemical fire suppression systems, 396
 - dry pipe fire suppression systems, 395, 396
 - dual-homed firewalls, 415, 416
 - dual operations, 297–298
 - dual power leads, 394
 - due care in preplanning audits, 68
 - dumpster diving, 378
 - Duncan, David, 3
 - duplicate firewalls, 353
 - durable media disposal process, 399
 - Duran, Joseph, 256
 - DVD drives, 199
 - Dynamic Host Configuration Protocol (DHCP), 209, 227–229, 228–229
 - dynamic routing, 210–211, 211
-
- E**
- e-commerce, 309–310, 310
 - e-discovery, 89–90
 - earned value (EV), 41–42
 - eavesdropping, 377
 - eBay auction software, 255
 - Ebbers, Bernard, 4
 - effectiveness metrics, 334, 335
 - efficiency
 - BPR for, 151
 - metrics, 334, 335
 - Eisner, Michael, 26
 - electrical power, 392–394, 392, 394
 - electromagnetic interference (EMI), 222
 - electronic commerce, 309–310, 310
 - electronic commerce controls, 15
 - electronic discovery, 89–90
 - electronic locks, 390
 - electronically erasable programmable read-only memory (EEPROM), 199
 - elliptic-curve cryptography, 432
 - email spamming, 382
 - embedded audit modules (EAMs), 88
 - embedded program audit hooks, 88
 - emergency changes, 349
 - emergency management teams (EMTs), 478–479, 482
 - Emergency Operations Centers (EOCs), 478–479, 482
 - emergency power off (EPO) switches, 392
 - emergency power shutoff, 392
 - emergency response phase in
 - business continuity, 476–479, 479
 - emergency response teams, 482
 - emergency software fixes, 294
 - employee betrayal, 374
 - employee check-in aids, 487
 - employee contracts, 147
 - EnCase Forensic software, 357
 - encryption, 427
 - Application layer, 214
 - digital signatures, 430–431, 430–431
 - elliptic-curve, 432
 - IPsec, 418
 - PKI, 432–435, 433–434
 - Presentation layer, 213
 - private-key, 427, 428
 - public-key, 427–429, 428–429
 - quantum, 432
 - ending IP addresses, 207
 - engagement letters, 63

engagement managers, 30
 enhanced WEP, 423
 enrollment process for
 biometrics, 411
 Enron, 3
 enterprise resource
 planning (ERP)
 implementation, 152
 entity-relationship diagrams
 (ERDs), 277–278, 277
 environment changes in
 SDLC, 300
 environmental controls,
 392, 392
 electrical power, 392–394
 fire protection, 395–397,
 396–397
 heating, ventilation, and
 air-conditioning, 395
 water detection, 397, 398
 environmental sensors, 391
 environmental standards for
 offshore functions, 134
 envision step in BPR, 155
 equal error rate (ERR),
 biometrics, 411
 error rates
 biometrics, 411, 411
 in testing, 99–100
 espionage, 372
 Ethernet networks, 206
 ethical hackers, 374–375
 ethics
 code of professional
 ethics, 6–8
 conflicts, 8–9
 ISACA standards, 14
 organization statements
 on, 148
 evaluate step in BPR, 157–158
 evaluation assurance levels
 (EALs), 295, 295
 event logs, 345
 event monitors, 88
 evidence
 audit. *See* audit evidence
 ISACA standards, 15
 evidence rule, 25–26
 evolutionary software
 development, 265–266
 exception reports, 345, 353

excluded processes in
 BPR, 167
 executing process group, 38
 executives
 interviewing, 26
 performance reviews, 139
 exit interviews, 104
 expected error rate in
 compliance testing, 98
 expert level DSS, 307
 experts, legal, 91
 explanations,
 unsatisfactory, 101
 exposure factor (EF) in risk
 management, 144
 external agency teams in
 business continuity
 plans, 484
 external auditors, value of,
 24–25
 external audits, 9
 external measures, 325
 extortion, 372
 extraordinary care in
 preplanning audits, 68

F

face scans, 405, 406
 facilities plans in strategy
 implementation, 134
 failure to enroll (FTEr) in
 biometrics, 411
 failures, dealing with, 24
 Fair and Accurate Credit
 Transactions Act, 5, 343
 fairness, 12
 false acceptance rate (FAR) in
 biometrics, 411, 411
 false rejection rate (FRR) in
 biometrics, 411, 411
 Fastow, Andrew, 3
 Fastow, Lea, 3
 feasibility of biometrics, 407
 Feasibility Study phase
 in SDLC, 269,
 272–276, 274
 Federal Financial Institutions
 Examination Council
 (FFIEC) regulations, 5
 Federal Information
 Processing Standards
 (FIPS), 142
 Federal Information Security
 Management Act
 (FISMA), 5, 14, 140,
 142, 296
 FedEx, 456
 Feynman, Richard, *Surely
 You're Joking, Mr.
 Feynman!*, 201
 fiber-optic cable, 223, 223
 fidelity bonding, 388, 475
 fiduciary relationships, 10
 fifth-generation programming
 languages (5GL),
 286, 286
 file servers, 191
 File Transfer Protocol
 (FTP), 201
 filters, firewall. *See* firewalls
 finance representation
 business continuity
 plans, 483
 steering committees, 121
 Financial Accounting
 Standards Board
 (FASB), 13
 financial audits, 10
 financial category in business
 continuity, 462
 financial challenges,
 surviving, 452–453
 financial objectives in
 preplanning process, 64
 financial-reporting
 controls, 192
 fingerprints, 404, 404
 fire detection and suppression,
 395–397, 396–397
 fire sales, 454
 firewalls
 duplicate, 353
 overview, 413–416,
 415–417
 for wireless networks,
 424, 425–426
 first-generation programming
 languages (1GL), 284
 fish from Chinese
 suppliers, 71

fixed interval sampling, 97
 flame detection, 395
 flash memory, 199
 flowcharts, 278–279, 278
 “follow the sun” concept, 135
 follow-up activities in ISACA standards, 14
 food contamination, 71, 138
 footprinting process, 376
 Foreign Intelligence Surveillance Act (FISA), 145
 foreign keys for relational databases, 302
 forensic investigations, 355–356
 formulas for metrics, 336
 fortifications in business continuity strategy, 474
 fourth-generation programming languages (4GL), 285, 285
 Frame relay (FR), 233–234
 fraud, 101, 371–372
 free password generators, 342
 frequency of metrics, 336
 Frontier Airlines, 453
 full backups, 474
 full mesh networks, 220, 220
 full operation tests, 485
 fully qualified domain names (FQDNs), 227
 Function Point Analysis (FPA), 273–275, 274
 functional objectives, 326–327
 functional organizations, project management authority in, 36
 functional tests, 292, 485
 fuzzification, 307
 fuzzy logic, 286, 307

G

Gantt charts, 45–46, 46
 gaseous halon, 396
 general controls, 81
 general managers, 29
 general user state, 195

Generally Accepted Accounting Principles (GAAP), 13
 generations of programming languages, 284–286, 285–286
 genius and insanity, 152
 Glisan, Ben, Jr., 3
 globalization issues in sourcing, 136–137
 goals
 metrics, 335
 supporting, 329
 going live in SDLC, 297–298
 gold plating, 281
 governance
 IT. *See* information technology (IT)
 governance in software development, 254–255
 grading of evidence, 90–92
 Gramm-Leach-Bliley Act, 5
 guards, 389
 Guide to the Project Management Body of Knowledge (PMBOK), 32
 guidelines, 6, 7

H

hackers, 195, 373–375
 halon gas, 396
 Hammer, Michael, *Reengineering the Corporation*, 153
 hand geometry, 405
 haphazard sampling, 98
 hard changeover, 298
 hard tokens, 403, 403
 hardware
 monitoring, 339
 ports, 200, 200
 redundancy, 353, 471
 hash message authentication code (HMAC), 423
 Health Insurance Portability and Accountability Act (HIPAA), 5
 HealthSouth, 4
 Heartland Payment Systems, 138
 heat detection, 395
 heating, ventilation, and air-conditioning, 395
 help desk
 evaluating, 336
 responsibilities, 332–333
 Hewlett-Packard, 373
 hierarchy of internal controls, 80–85
 high-availability servers, 436, 437, 471
 high-level flowcharts, 278, 278
 hiring policies, 147
 honey nets, 427
 honey pots, 426
 Hopkins, Claude, 124
 host-based IDS (HIDS) systems, 425
 host enumeration, 438
 host traffic analysis, 376–377
 hot fixes, 294
 hot sites, 472–473
 HP OpenView tool, 376
 hubs, 224, 226
 human implants, 237
 human resources
 managing, 42–43
 policies, 147–148
 steering committee representation, 122
 humidity, 395
 Hurricane Andrew, 452
 hybrid approach to BPR, 153–154
 hybrid RAID systems, 196
 hybrid sourcing models, 136
 Hypertext Markup Language (HTML), 346
 hypotheses, 86, 152

I

identification process
 vs. authentication, 401–402
 in evidence life cycle, 93

556 IEEE (Institute of Electrical and Electronics Engineers) – information technology

- IEEE (Institute of Electrical and Electronics Engineers)
 - port designations, 199, 201
 - wireless network standards, 421, 423
- ignorance as defense, 376
- illegal acts
 - detecting, 101–102
 - ISACA standards, 14
- ImClone Systems, 4
- immunization, 378
- impact metrics, 334, 335
- impact of changes, 261–262
- implementation metrics, 334, 335
- Implementation phase in SDLC, 271, 293
 - auditor interests, 299
 - data conversion plans, 294
 - going live and changeover, 297–298
 - review and approval, 298–299
 - software release and patch management, 293–294
 - system accreditation, 297
 - system certification, 294–297, 295
 - user training, 297
- implementation risks in BPR, 163
- improvements
 - for benchmarking, 160
 - BPR for, 151
 - test results for, 100
- in-house services, 136, 138
- Incident Command System (ICS), 478–479, 479
- incident commanders (ICs), 478
- incident response teams (IRTs), 354–355
- incidents
 - emergency response for, 476–479, 479
 - handling, 354–355, 388–389
 - policies for, 146–147
- incremental approach to BPR, 153
- incremental backups, 475
- incremental software development, 266
- independence
 - evidence, 91
 - ISACA standards, 14
 - self-assessment test, 11–13
- independent audits, 9
- Independent Basic Service Sets (IBSS), 235
- indicators
 - illegal and irregular activity, 101–102
 - metrics, 336
- indirect evidence, 86
- individual modems, 230–231
- industrial espionage, 372
- ineffective and inefficient controls, 352
- inference, 86
- information asset protection, 369–370
 - administrative. *See* administrative protection of assets
 - attack methods, 376–382, 381
 - exam essentials, 439–440
 - perpetrators, 373–376
 - physical protection. *See* physical protection of assets
 - review questions, 441–449
 - summary, 439
 - technical protection. *See* technical protection of assets
 - threats, 370–372, 371
- Information Evaluation Methodology (IEM), 438
- information security management, 382–383
- information security manager (ISM) responsibilities, 330
- information security risk, 145
- Information Systems Assessment methodology (IAM), 438
- Information Systems Audit and Control Association (ISACA), 14
 - BPR risks, 162
 - code of professional ethics, 6–8
 - control standards, 81
 - IS audit standards, 14–15
- information systems
 - certifications and accreditations, 10
- information systems security analysts (ISSAs), 331
- information systems security managers (ISSMs), 383
- information technology (IT)
 - auditee environment, 79–80
 - control standards, 15
 - director
 - responsibilities, 330
 - governance. *See* information technology (IT) governance
 - operations manager
 - responsibilities, 330
 - recovery teams, 482
 - services. *See* services steering committee representation, 122
- information technology (IT) governance, 117–118
 - asset protection, 383–384
 - balanced scorecards, 125–129, 127
 - BPR. *See* business process reengineering (BPR)
 - COBIT, 134
 - evidence of, 139
 - exam essentials, 171
 - executive performance reviews, 139
 - ISACA standards, 15
 - operations management, 169–170
 - planning. *See* planning policies, 130–131
 - review questions, 172–181
 - sourcing locations, 134–138
 - steering committee, 120–125, 121, 123
 - strategy
 - implementing, 131–134, 133

- planning, 118–120, 119–120
 - selecting, 129–130, 129
 - summary, 170
 - tactical management, 139–140, 139
 - Information Technology Infrastructure Library (ITIL), 327–328, 329
 - Information Technology Security Evaluation Criteria (ITSEC), 294, 295
 - informational policies, 131
 - infrastructure library, 327–328, 329
 - infrastructure mode in LANs, 419
 - inherent risks, 73
 - inherited liability, 71
 - initial preservation storage in evidence life cycle, 94
 - initial program load (IPL) function, 185
 - initiate step in BPR, 155
 - initiating process group, 37–38
 - initiation practice area in business continuity, 461–463, 463
 - initiatives on balanced scorecards, 125
 - inoculation, 378
 - input controls, 344
 - input/output (I/O) components, 184–185, 185
 - insanity and genius, 152
 - Institute of Electrical and Electronics Engineers (IEEE)
 - port designations, 199, 201
 - wireless network standards, 421, 423
 - insurance
 - business continuity strategy, 475–476
 - in risk management, 149
 - USAA, 166
 - insurance teams in business continuity plans, 484
 - integrated audits, 10
 - integrated development environment (IDE) tools, 286–287, 287
 - Integrated Services Digital Network (ISDN), 232
 - integrated test facilities, 88
 - integration, 21, 39
 - integrity
 - data, 146
 - referential, 303, 303
 - SLAs, 337
 - transaction, 306
 - WLANs, 423
 - intellectual property
 - policies, 146
 - interfaces
 - networking technology, 199–201, 200
 - restricted, 401
 - Interior Gateway Protocol (IGP), 211
 - internal auditors, value of, 24–25
 - internal audits and assessments, 9
 - internal controls, 80–82
 - reviewing, 82–84
 - in SDLC, 279
 - strong, 84–85
 - internal measures, 325
 - International Federation of Accountants (IFAC), 13
 - International Organization for Standardization (ISO), 13, 202
 - Common Criteria, 294–297, 295
 - software quality, 256–260
 - International Product Investment Corp. (IPIC), 3
 - international regulations, 136–137
 - international standards in planning and performance, 143
 - Internet Protocol (IP), 207–209, 208, 226–227, 227
 - interrupt masking, 187
 - interviews
 - for data collection, 79
 - determining, 26–27
 - exit, 104
 - intrusion detection and prevention systems (IDPS), 425
 - intrusion detection systems (IDS), 424–427
 - intrusion prevention systems (IPS), 425
 - invocation procedures for emergency response, 478
 - IP addresses, 207–209, 208, 226–227, 227
 - IP fragmentation attacks, 379
 - IP security (IPsec) protocol, 418–419, 418–420, 435
 - IP version 4, 209
 - IP version 6, 209
 - ipconfig /all command, 205
 - iris scans, 405
 - irregularities
 - detection, 101–102
 - ISACA standards, 14
 - irrelevant evidence, 91
 - ISACA. *See* Information Systems Audit and Control Association (ISACA)
 - ISACA Audit Standards, Guidelines, and Procedures, 162
 - ISO 9001, 32, 257–258
 - ISO 9126, 258
 - ISO 15408, 294–297, 295
 - ISO 15489, 258–260
 - ISO 15504, 257
 - IT. *See* information technology (IT)
 - IT Governance Institute (ITGI), 14, 103
 - iterative management process, 39
-
- J**
- Java programs, 347
 - Java Virtual Machine (JVM) program, 347
 - JavaScript (JScript), 347

558 job accounting – MAC (Media Access Control) addresses

job accounting, 345, 354
 job rotation, 352
 judgmental sampling, 97

K

Keating, Charles, 4
 Kerberos single sign-on system, 412, 413
 kernels for firewalls, 414
 Key Distribution Centers (KDCs), 412
 key goal indicators (KGIs), 461
 key performance indicators (KPIs), 149, 461
 key wrapping, 430
 keyboard remapping, 357
 keys
 encryption, 427–431, 428–431
 PKI, 434–435
 for relational databases, 302
 in WLANs, 422–423
 Kozlowski, Dennis, 4
 Kreinberg, David, 3

L

labels, security, 401
 labor costs in offshore functions, 134
 labor unions
 policies for, 147
 respecting, 74–75
 steering committee representation, 122
 LANs (local area networks). *See* networks and networking
 laptops
 cables and viewing screens for, 20
 recovering, 351
 lasers
 for fiber-optic cable, 223
 in wireless networks, 236

Latest Copy system, 291
 law of unintended consequences, 300
 lawyers, working with, 20
 Lay, Ken, 3
 leadership duties, 22
 leadership risks in BPR, 163
 learning curves, 151
 least privilege concept, 20, 341
 leftovers in BPR, 165
 legal compliance issues in sourcing, 137
 legal repercussions of asset losses, 372–373
 legal teams
 for business continuity plans, 484
 steering committee representation, 121
 lessons learned meetings, 355
 level of assurance, controls for, 81
 levels, CMM, 141–142, 142, 256
 liability
 inherited, 71
 subcontractor, 137–138
 librarian responsibilities, 332
 libraries, infrastructure, 327–328, 329
 licenses
 mainframe computers, 192
 software, 351
 life-cycle management, 148, 253–254
 centralization vs. decentralization, 309
 change management, 265
 data architecture, 301–306, 303–306
 decision support systems, 307–308, 308
 electronic commerce, 309–310, 310
 evidence, 93–95, 95
 exam essentials, 311–312
 governance, 254–255
 program architecture, 309
 project management, 265–269, 267–268
 quality management, 255–260
 review questions, 313–321
 SDLC. *See* System Development Life Cycle (SDLC)
 steering committee in, 260–265
 summary, 311
 Life Time Fitness, 373
 light-emitting diodes (LEDs), 223, 223
 lights-out operations, 327
 limit checks, 345
 Lincoln Savings and Loan, 4
 liquid nitrogen, 393
 local area networks (LANs). *See* networks and networking
 locking security cables for laptops, 20
 locks, 390, 390
 logic bombs, 378
 logic path monitors, 292
 logical access controls, 343
 logical backups, 356
 logical protection, 399
 login accounts
 maintenance, 343
 privileged, 342
 login IDs and passwords, 402
 logistics teams in business continuity plans, 483
 logs
 managing, 340–341
 reviewing, 438
 Syslog system, 239, 340
 transaction, 345, 353
 long-term planning, 124–125
 low-level flowcharts, 278, 278
 lower CASE tools, 287, 287

M

MAC (Media Access Control) addresses, 205, 205–206, 208–209, 208

- MAC-based VLANs, 225
- machinery insurance, 476
- magnetic media
 - disposal process, 399
 - hard disks, 196–198, 198
 - soft disks, 198
 - tape, 198–199
- mainframe computers, 192, 194, 194
- maintenance accounts,
 - attacks through, 343, 379–380
- maintenance controls, 348–349
- maintenance in business
 - continuity, 484–485, 486
- major problems outside of scope, 102
- major releases, 294
- man-in-the-middle
 - attacks, 382
- man-made disasters,
 - surviving, 454
- Man of the Year
 - movie, 298
- management
 - in BPR risk assessment, 164
 - control methods, 140–143, 142
 - exemption from controls, 80–81
 - in SDLC, 284
- managers, 29
- managing partners, 30
- mandatory access controls (MACs), 400
- mandatory actions, 17
- mandatory compliance, 6
- mandatory controls, 146
- mantraps, 386
- manufacturing representation
 - on steering committees, 121
- marginal processes in BPR, 166–167
- market changes,
 - business continuity for, 455
- marketing campaigns,
 - business continuity for, 456
- marketing teams
 - in business continuity plans, 483
 - steering committee representation, 121
- material relevance of evidence, 90–91
- materiality
 - ISACA standards, 15
 - in risk assessment, 73
- Mattel, 71
- maturity levels in CMM, 141–142, 142
- maximum acceptable outage (MAO), 470
- maximum tolerable downtime (MTD), 470
- mean estimation in testing, 99
- Media Access Control (MAC)
 - addresses, 205, 205–206, 208–209, 208
- media access units (MAUs), 218, 219
- media librarian
 - responsibilities, 332
- media relations teams in
 - business continuity plans, 483
- media tracking, 351
- media transport of records, 398–399
- medieval security design, 370–371, 371
- memory, 184–185, 185, 199
- meshed topologies, 220–221, 220
- message modification
 - attacks, 382
- metrics, 333–334
 - in balanced scorecards, 129
 - developing and selecting, 335–336
 - principles, 334
 - types, 334–335, 335
- metropolitan area networks (MANs), 238
- microcomputers, 193–194, 194
- microwaves in wireless
 - networks, 236
- middle CASE tools, 287, 287
- middleware, 343
- midrange computers, 193–194, 194
- MIME (Multipurpose Internet Mail Extensions), 346
- minicomputers, 193–194, 194
- minor problems outside of scope, 102
- minor releases, 294
- minutes of policy
 - discussions, 26
- minutiae in fingerprints, 404, 404
- MIPS (millions of instructions per second), 193
- mirrored disk drives, 196–197, 198, 471
- mirrored servers, 436, 437, 471
- mission in balanced
 - scorecards, 128–129
- mission objectives, 27
- mitigate risk response, 71
- mobile sites, 473
- mobile software code, 346–347
- modems, 230–231
- modular stages for
 - compliance requirements, 66
- monitoring, 339
 - active content, 346
 - antivirus software, 345
 - change management, 349, 350
 - controls
 - administrative management, 351–352
 - application processing, 344–345
 - compensating, 352–353
 - data file, 343–344
 - maintenance, 348–349
 - system access, 341–343
 - logs, 340–341
 - mobile software code, 346–347

560 Morgan Stanley – open systems

policies for, 146
 in project framework, 38
 system, 339–340
 test environments, 350
 Morgan Stanley, 373
 multicasting, 209
 Multiplexed Information and
 Computing Service
 (Multics), 189
 multiplexors, 231
 multiprocessor computer
 systems, 186–187,
 187–188
 Multipurpose Internet Mail
 Extensions (MIME), 346
 multitasking systems,
 187, 188
 multithreading, 192
 mutual respect, 21
 Myers, David, 4

N

N-1 mesh networks, 221
 National Institute of
 Standards and
 Technology (NIST),
 13, 142–143
 natural disasters,
 surviving, 454
 natural gas-powered
 generators, 393
 negligence, 68
 negotiable instruments, 345
 Nelson, Jody, 4
 netmasking, 207
 network administrators,
 195, 331
 network analysis attacks, 376
 network-based IDS (NIDS)
 systems, 425
 network communications
 teams in business
 continuity plans, 482
 Network layer in OSI model,
 206–212, 207–211
 Network Management
 System (NMS), 240
 network scanning, 438

networks and networking,
 183–184
 cable types, 221–223,
 222–223
 computers in
 architecture, 184–187,
 185–188
 capabilities, 193–194
 classes, 191–193, 194
 data storage, 195–199, 198
 devices, 224–226
 exam essentials, 241–242
 expanding, 230–231, 230
 interfaces and ports,
 199–201, 200
 managing, 239–240
 monitoring, 340
 operating systems,
 188–191, 190
 OSI model. *See* Open
 Systems Interconnect
 (OSI) model
 physical network design,
 215–216, 217
 protecting, 412
 firewalls, 413–416,
 415–417
 Kerberos single
 sign-on, 412, 413
 remote dial-up
 access, 417
 security protocols,
 435, 435
 VPNs, 417–419,
 418–420
 wireless, 419–427
 review questions, 243–252
 routing, 209–212, 210–211
 services, 226–229,
 227–229
 summary, 241
 system control, 194–195
 telephone circuits,
 231–234, 233
 topologies, 217–221,
 217–220
 variations, 237–238
 wireless access solutions,
 234–237, 235
 neural-based learning
 networks, 426

neural weighting
 algorithms, 286
 Nmap utility, 376–377
 noncompetition
 agreements, 147
 nonconformity in test
 results, 100
 noncritical functions in
 business continuity
 strategy, 470
 nonrepudiation, 422
 nonsampling risks, 73
 nonstatistical sampling,
 97–98, 97
 nonvolatile data, 356
 nonworking processes in BPR,
 166–167
 normalization, database, 302
 noteworthy achievements in
 test results, 100
 numeric names, 207

O

object classes, 305
 object code, 289
 object-oriented databases
 (OODBs), 302, 305, 306
 object-oriented structured
 databases (OOSDs), 302
 objectives in metrics, 335
 objectivity, 12, 91
 observations
 for benchmarking, 160
 hypotheses based on, 152
 obstruction, 101
 offshore functions, 134–135
 offsite functions, 134–135
 offsite storage, 398
 omissions and errors
 insurance, 476
 omitted procedures,
 identifying, 104
 onsite functions, 134
 Open Shortest Path First
 (OSPF) protocol, 211
 open systems
 program architecture, 309
 in WLANs, 422

- Open Systems Interconnect (OSI) model, 202–203, 202–203
 - Application layer, 214
 - Data-Link layer, 204–206, 204–206
 - firewall generations
 - compared to, 414, 415
 - Network layer, 206–212, 207–211
 - Physical layer, 204
 - Presentation layer, 213, 214
 - Session layer, 213, 213
 - summary, 215, 216
 - Transport layer, 212, 212
 - OpenNMS tool, 376
 - OpenView tool, 376
 - operating systems (OS), 188–191, 190
 - operation/rollout risks, 164
 - operational audits, 10
 - operational category
 - in business continuity, 462
 - operational delivery, 170
 - operational objectives
 - knowledge in preplanning process, 64–65
 - operational planning, 124–125
 - operational risks, 73
 - operations
 - managing, 169–170
 - sustaining, 169
 - operations manager
 - responsibilities, 330
 - opinions
 - evidence rule for, 25
 - qualified, 103
 - optical drives, 199
 - ordinary care in preplanning audits, 68
 - Organization for Economic Cooperation and Development (OECD), 13
 - organizational control, strategy planning for, 118–120, 119–120
 - organizational plans for strategy implementation, 133, 133
 - Organizational Project Management Maturity Model (OPM3), 140
 - OSI model. *See* Open Systems Interconnect (OSI) model
 - outages, 340
 - output control
 - monitoring, 345
 - outsourcing
 - auditing activities, 74
 - considerations, 136
 - disadvantages, 138
 - IT functions, 337–339
 - managing, 150
 - oversight committees, 28
 - overwriting data in disposal process, 399
 - owners of data, 384
-
- P**
- packet filters, 414
 - packet replay attacks, 381
 - packet sniffers, 239
 - packet-switched circuits, 233–234
 - painting process, 376
 - palm prints, 404, 404
 - paper data disposal, 399
 - parallel operations, 297–298
 - parameter control, software, 195
 - Parmalat dairy scandal, 3
 - partial mesh networks, 220, 220
 - partners, 30
 - passive attacks, 376–377
 - passwords
 - cracking, 438
 - login, 341–342, 402
 - SNMP, 240
 - patch management, 293–294
 - Patterson-UTI Energy, 4
 - Paycheck movie, 282
 - Payment Card Industry (PCI), 5, 276, 276
 - credit card rules, 343, 424
 - and SDLC, 299
 - penetration testing, 438
 - performance
 - ISACA standards, 14
 - managing, 149, 150
 - metric goals, 335
 - in outsourcing
 - contracts, 338
 - policies, 148
 - reviewing, 141–142, 142
 - in SLAs, 337
 - permanent virtual circuits (PVCs), 233
 - perpetrators, 373–376
 - personal area networks (PANs), 238
 - personnel and personnel management, 387
 - in business continuity plans, 484
 - incident handling, 388–389
 - physical access, 387–388
 - in risk management, 145
 - roles and responsibilities, 329–333, 333
 - in SLAs, 336
 - terminating access, 388
 - violation reporting, 389
 - PERT network diagrams, 45–48, 47
 - pervasive IS controls, 81–82
 - pet food contamination, 138
 - Peter Pan peanut butter, 138
 - Peters, Tom, *Re-imagine!*, 153
 - PFSweb company, 455
 - phased changeover, 298
 - phishing attacks, 378, 382
 - photographic data
 - disposal, 399
 - physical controls, 83
 - Physical layer in OSI model, 204
 - physical maps for access paths, 386
 - physical network design, 215–216, 217

562 physical protection of assets – privileged login accounts

- physical protection of assets, 389–391
 - access limitations, 387–388
 - in business continuity plans, 482
 - data processing locations, 391
 - environmental controls. *See* environmental controls
 - storage, 398–399
 - physiological characteristics
 - in biometrics, 403–405, 404–405
 - pico prefix, 236
 - ping command, 376
 - Ping of Death
 - command, 382
 - pipelining, 187
 - plain old telephone service (POTS), 232
 - plan creation practice area in business continuity, 480–484, 480–481
 - Plan-Do-Check-Act cycle, 69, 69, 281, 281
 - planning, 140
 - benchmarking, 159
 - business continuity, 149, 480–484, 480–481
 - human resources, 147–148
 - insurance, 149
 - international standards, 143
 - ISACA standards, 14
 - management control methods, 140–143, 142
 - NIST, 142–143
 - outsourcing management, 150
 - performance management, 149, 150
 - performance reviews, 141–142, 142
 - project management, 38, 143
 - quality management, 143
 - risk management, 144–145, 144
 - standards, 146–147
 - system life-cycle management, 148
 - systematic approach, 68–69, 69
 - plastic data disposal, 399
 - plenum-grade cable, 222
 - policies, 6, 7
 - minutes of discussions, 26
 - specifying, 130–131
 - types, 131
 - policy-based VLANs, 225
 - political risk in BPR, 163
 - Poly Version Control System (PVCS), 291
 - portable software systems, 189–191
 - portfolio management, 165
 - ports
 - network, 199–201, 200
 - port-based VLANs, 225
 - protecting, 387
 - post analysis preservation storage in evidence life cycle, 94–95
 - post evaluation step in BPR, 157–158
 - Postimplementation phase in SDLC, 271, 299–300
 - postincident activity, 355
 - potential emergencies, emergency response for, 477
 - power, electrical, 392–394, 392, 394
 - power transfer systems, 394, 394
 - precision in compliance testing, 98
 - preparation in incident handling, 355
 - preparedness simulation in business continuity, 485
 - preplanning
 - audits, 63–65, 65
 - requirements gathering, 66–68
 - scope restrictions, 65–66
 - systematic approach, 68–69, 69
 - variety of audits, 66
 - emergency response, 478
 - risk management strategy, 70–71, 72
 - traditional audits vs. assessments and self-assessments, 69–70
- presentation in evidence life cycle, 95
 - Presentation layer in OSI model, 213, 214
 - preservation storage in evidence life cycle, 94–95
 - president liabilities, 29
 - pretexting, 372–373
 - Pretty Good Privacy (PGP), 214, 435
 - preventative controls, 82–83, 85, 279
 - price of conformance (POC), 281
 - price of nonconformance (PONC), 280
 - primary keys for relational databases, 302
 - primary trunk lines (T1), 232
 - Prince2 project management model, 31
 - priorities
 - changing, 324
 - setting, 22–23
 - prioritized calling lists, 487
 - Privacy Enhanced Mail (PEM), 434
 - privacy issues
 - CPOs, 383
 - laptop screens, 20
 - RFIDs, 237
 - WLANs, 423
 - private, internal use only classification, 384
 - Private Branch Exchange (PBX), 437
 - private-key encryption, 427, 428
 - private passwords in SNMP, 240
 - privileged login accounts, 342

- proactive controls, 82
 - problem management, 354
 - acquisition phase, 356–357
 - digital forensic investigations, 355–356
 - examination, 357
 - incident handling, 354–355
 - review, 358
 - utilization, 357
 - problem state, 195
 - procedures
 - description, 6, 7
 - vs. work, 352
 - process technique, 68–69
 - processes
 - auditing, 10
 - in BPR, 159
 - controls, 159
 - documentation, 158–159
 - maps, 158
 - understanding, 165
 - processing controls, 344–345
 - procurement management, 44–45
 - product audits, 9
 - professional competence, ISACA standards, 14
 - program architecture, 309
 - program patches, 294
 - program scripts, 289, 290
 - programming languages, 283–286, 285–286
 - progressive elaboration, 33
 - Project Communications Management knowledge area, 43
 - Project Cost Management knowledge area, 41
 - Project Human Resource Management knowledge area, 42–43
 - Project Integration Management knowledge area, 39
 - project management, 31–32
 - approach, 265–266
 - authority in, 36
 - defined, 34–35
 - diagramming techniques, 45–48, 46–47
 - monitoring, 349, 350
 - planning and performance, 143
 - process framework, 36–38, 38
 - project characteristics, 32–34
 - quick reference, 38–45
 - requirements, 35–36
 - steering committee representation, 122
 - traditional, 266–267, 267–268
 - Project Management Institute (PMI), 31–32, 36–38, 38, 157
 - Project Management Office (PMO), 143
 - Project Procurement Management knowledge area, 44–45
 - Project Quality Management knowledge area, 41–42
 - Project Risk Management knowledge area, 44
 - Project Scope Management knowledge area, 39–40
 - Project Time Management knowledge area, 40–41
 - projectized organizations, authority in, 36
 - promotion policies, 148
 - property insurance, 475
 - property teams in business continuity plans, 484
 - proprietary information, loss of, 372
 - protection of assets. *See* information asset protection
 - protection profiles (PPs), 295–296, 295
 - protocol analyzers, 239
 - protocol stacks, 215
 - protocols, 199, 201
 - network security, 435, 435
 - routing, 209–212, 210–211
 - prototypes, 288–289
 - provisioning, 207
 - proxy filters, 414
 - pseudocoding, 285
 - Public Company Accounting Oversight Board (PCAOB), 13
 - public information classification, 383
 - public information officers (PIOs), 479, 487
 - public-key encryption, 427–429, 428–429
 - public-key infrastructure (PKI), 432–433
 - digital certificates, 433–434
 - encryption-key management, 434–435
 - S/MIME, 434, 434
 - public passwords in SNMP, 240
 - purpose
 - auditing, 9
 - business continuity, 454–456
 - metrics, 335
-
- Q**
- qualifications of staff, 76
 - qualified opinions, 103
 - quality and quality control
 - CMM for, 255–256
 - Development phase in SDLC, 283–284
 - ensuring, 77
 - failures in, 280–281, 280
 - ISO for, 256–260
 - managing, 41–42, 143, 255
 - models, 31–32
 - in project management, 34
 - steering committee representation, 121
 - quantum cryptography, 432
 - questionable
 - circumstances, 102
 - questionable payments, 101

R

- Racketeer Influenced and Corrupt Organizations (RICO) Act, 101
- racketeering, 101
- radio frequency identification (RFID), 237
- RAID (Redundant Array of Inexpensive Disks) systems, 196–198, 198, 436, 437
- random access memory (RAM), 184–185, 185
- random sampling, 97
- Rapid Application Development (RAD), 288, 288
- Re-imagine! (Peters), 153
- reactive controls, 83
- read-only copies, 357
- read-only memory (ROM), 199
- rebuilding in disaster recovery, 453–454
- reciprocal agreements, 474
- recommended actions, 16
- reconciliation, 352
- reconstruct step in BPR, 156
- recording test results, 100
- Records Management, ISO 15489, 258–260
- recovery
 - deleted files, 356
 - disaster. *See* business continuity (BC); disaster recovery policies for, 146
 - stolen laptops, 351
- recovery point objective (RPO), 470
- recovery time objective (RTO), 470
- Red Button utility, 374
- redesign step in BPR, 156
- reduce risk response, 71
- redundancy
 - communication, 471
 - design for, 436, 437
 - hardware, 353, 471
 - sites, 472–473
- Redundant Array of Inexpensive Disks (RAID) systems, 196–198, 198, 436, 437
- reengineering, 282
- Reengineering the Corporation (Hammer and Champy), 153
- reference by context DSS, 307
- referential integrity, 303, 303
- reflector attacks, 379
- Registered Communications Distribution Designers (RCDDs), 221
- registration authorities (RAs), 432–433
- regression testing, 292
- regulations
 - for best practices, 16–18
 - international, 136–137
 - violations, 101
- regulatory policies, 131
- relational databases, 302–303, 303
- reliability factor, 99
- remapping, keyboard, 357
- remote access attacks, 380
- remote dial-up access, 417
- Remote Monitoring Protocol version 2 (RMON2), 240
- remote VPN access, 417–418
- remounting backup process, 197
- repeaters, 224, 226
- reports, 103–104
 - configuration, 291
 - exception, 345, 353
 - generation and distribution, 345
 - ISACA standards, 14
 - retention, 345
 - violations, 389
- required actions, 17
- requirements and
 - requirements gathering BPR for, 151
 - data retention, 385–386
 - in preplanning audits, 66–68
- Requirements Definition phase in SDLC, 269, 276–279, 276–278
- Research and Development (R&D) steering committee
 - representation, 122
- research for
 - benchmarking, 159
- residual risks, 73
- resources in project management, 34
- respect, mutual, 21
- responsibilities
 - in audit charters, 61
 - auditor, 10
 - in BPR, 159
 - personnel, 329–333, 333
- restricted user interfaces, 401
- retaining data
 - audit documentation, 21
 - reports, 345
 - requirements, 385–386
- retina scans, 405, 405
- return on investment (ROI)
 - balanced scorecards for, 128
 - for BPR, 165
- return to owner stage, 95
- revenue
 - in business continuity, 454
 - objectives, 27
- Reverse ARP (RARP), 209, 209
- reverse engineering, 282
- review and approval in SDLC phases
 - Development, 293
 - Feasibility Study, 275
 - Implementation, 298–299
 - Requirements Definition, 279
 - System Design, 282–283
- review meetings in SDLC, 300

- Revision Control System (RCS), 291
 - revolutionary software development, 266
 - RFIs (requests for information), 263
 - RFPs (requests for proposals), 263
 - Rigas, John, 3
 - Rigas, Timothy, 3
 - right to audit in
 - outsourcing, 150
 - Right to Work laws, 147
 - Rijmen, Vincent, 427
 - ring topologies, 218–219, 219
 - risk assessment and analysis
 - audit, 73
 - in audit planning, 15
 - in BPR, 158, 162–164
 - in business continuity, 464–467, 464–466
 - physical maps for, 386
 - project, 162–164
 - risk management, 44
 - formulas, 144–145, 144
 - information security
 - risk, 145
 - personnel risk, 145
 - in preplanning, 70–71, 72
 - sampling risk, 73, 97
 - Ritchie, Dennis, 189
 - Robust 802.11i
 - authentication, 422
 - Robust Security Networks (RSNs), 236
 - role-based access control (RBAC), 400
 - roles
 - in BPR, 159
 - in consulting firms, 29–31, 30
 - corporate organizational structure, 27–29
 - personnel, 329–333, 333
 - root kits, 379
 - root users, 195
 - rotation, job, 352
 - routers, 216, 224–226, 229, 229
 - routers of last resort, 212
 - Routing Information Protocol (RIP), 211
 - routing protocols, 209–212, 210–211
 - rows in databases, 304, 304
 - Royce, W. W., 267
 - rule-based VLANs, 225
 - run-to-run totals, 345
 - Rutan, Burt, 35
-
- S**
- sabotage, 372
 - safe cracking, 201
 - safe Storage, 398–399
 - safety teams in business
 - continuity plans, 483
 - salami technique, 381
 - sales representation on
 - steering committee, 121
 - salvage teams in business
 - continuity plans, 483
 - samples, audit, 96–98, 97
 - sampling risks, 73, 97
 - Sarbanes-Oxley Act, 4–5, 19, 62
 - SAS-70 audit reports, 74, 150
 - satellite radio, 236
 - scapegoating, 8
 - scenario approach, 261
 - schedules in SDLC, 284
 - Schwartz, Mark H., 4
 - scope
 - in electronic
 - discovery, 90
 - findings outside of, 102
 - identifying, 65–66
 - managing, 39–40
 - project, 34–35
 - scope creep, 274
 - scope risks in BPR, 163
 - screened subnets, 416
 - script kiddies, 374
 - scripts, 289, 290
 - Scrushy, Richard, 4
 - SDLC. *See* System Development Life Cycle (SDLC)
 - second-generation
 - programming languages (2GL), 284
 - Secure DNS (S-DNS), 227
 - Secure Electronic Transaction (SET) protocol, 435
 - Secure Hypertext Transfer Protocol (HTTPS), 435
 - Secure Multipurpose Internet Mail Extensions (S/MIME), 434, 434
 - Secure Shell (SSH), 418
 - Secure Sockets Layer (SSL), 418, 435
 - Securities and Exchange Commission, 13
 - security
 - asset protection.
 - See* information asset protection
 - mainframe computers
 - for, 192
 - mobile code, 348
 - policies for, 146, 348
 - RFIDs, 237
 - in SDLC, 295–296
 - in SLAs, 336
 - security cables for laptops, 20
 - Security event management (SEM) software, 357
 - security guards, 389
 - security labels, 401
 - security parameter index (SPI), 419
 - self-assessments
 - vs. audits, 69–70
 - for independence, 11–12
 - self-directed hacking, 375
 - self-insurance, 149
 - senior consultants, 30
 - sensitive area protection, 387
 - sensitive classification, 383
 - sensitive functions in business
 - continuity strategy, 470
 - separate test
 - environments, 350
 - separation, subnets for, 207
 - separation of duties, 333, 333, 416, 417
 - server administrator
 - responsibilities, 331

566 server application teams in business continuity plans – standing data controls

- server application teams in
 - business continuity plans, 482
- server-side includes (SSIs), 347
- servers
 - access, 231
 - database, 191
 - mirrored, 436, 437, 471
 - protecting, 388
- service delivery objectives (SDOs), 470
- service-level agreements (SLAs), 336–337
- service ports, protecting, 387
- services, 323–324
 - capacity management, 353
 - exam essentials, 358–359
 - functional objectives, 326–327
 - goals support, 329
 - help desk, 336
 - infrastructure library, 327–328, 329
 - metrics, 333–336, 335
 - monitoring. *See* monitoring
 - nature of, 324–325
 - network, 226–229, 227–229
 - outsourcing, 337–339
 - personnel roles and responsibilities, 329–333, 333
 - problem management, 354–358
 - review questions, 360–368
 - service-level agreements, 336–337
 - summary, 358
- servlets, 347
- session keys, 431
- Session layer in OSI model, 213, 213
- Setser, Gregory Earl, 3
- “shall” actions, 17, 18
- shared costs in strategy selection, 130
- shared keys, 422
- shells, 189
- Shelton, E. Kirk, 3
- Shewhart, Walter, 68–69, 155, 256
- signature-based IDPS systems, 425
- signature detection, 378
- signature dynamics, 406
- signatures, digital, 430–434, 430–431, 433
- Simple Network Management Protocol (SNMP), 240
- single loss expectancy (SLE), 144
- single mirror systems, 197, 198
- single sign-on (SSO) system, 412, 413
- Six Sigma project management, 32
- skill risks in BPR, 163
- Skilling, Jeffrey, 3
- skills matrices, 42, 75–76, 263
- slack space, 356
- SLAs (service-level agreements), 336–337
- smart cards, 402, 402
- Smith, Fred, 456
- Smith, Howard, 3
- Smith, Weston, 4
- smoke detection, 395
- snapshot audits, 88
- social engineering, 377
- sockets, 201
- soft disks, 198
- soft tokens, 403
- software
 - antivirus, 345
 - baselines, 282
 - cost estimation in SDLC, 273–275, 274
 - developing. *See* Development phase in SDLC
 - licenses, 192, 351
 - mobile, 346–347
 - monitoring, 339
 - parameter control, 195
 - releases, 293–294
- Software Engineering Institute (SEI), 256
- Software Escrow, 264
- software loading in business continuity plans, 482
- software ports, 201
- Sorin, William, 3
- source code, 289
- Source Code Control System (SCCS), 291
- Source Lines Of Code (SLOC), 273, 275
- source routing attacks, 381
- sourcing locations, 134–135
 - globalization issues, 136–137
 - in-house operations, 138
 - legal compliance issues, 137
 - methods, 136
 - practices, 135–136
 - subcontractor liability trap, 137–138
- Space Travel program, 189
- spaghetti bowl programming, 283
- spamming, 382
- special locks, 390, 390
- special-purpose devices, 191
- special quality failures, 281
- spiral model, 267–269, 268
- split-horizon feature, 210
- sponsor payments in strategy selection, 130
- sponsorship risks in BPR, 163
- spoofing, 234, 382
- spying on foreign nationals, 145
- staff observations in data collection, 78
- staff workers
 - allocating, 75–76
 - responsibilities, 29
- stakeholders, 34
- standard terms of reference, 23–24
- standard WEP, 423
- standards, 6, 7
 - auditing, 13–16, 16
 - implementing, 146–147
- standards of conduct, 14
- standby generators, 393
- standing data controls, 343

- star topologies, 218, 218–219
 - starting IP addresses, 207
 - stateful inspection, 414
 - Statement on Auditing Standards (SAS), 13, 103
 - statements of work (SOWs), 275
 - static electricity, 395
 - static routing, 210, 210
 - stations (STA) in wireless networks, 235, 420
 - statistical IDS systems, 425
 - statistical sampling, 97
 - steering committees
 - alignment of software to business needs, 261–263
 - critical success factors identification, 261
 - in life cycle management, 260
 - overview, 120–125, 121, 123
 - RFI/RFP process, 263
 - scenario approach, 261
 - vendor proposal reviews, 264–265
 - stockpiling supplies, 476
 - stolen laptops, recovering, 351
 - stop-and-go sampling, 98
 - storage
 - in evidence life cycle, 94–95
 - requirements, 398–399
 - storage area networks (SANs), 238
 - strategic category in business continuity, 462
 - strategic objectives
 - knowledge in preplanning process, 64
 - strategic systems, 255
 - strategies
 - in balanced scorecards, 129
 - in business continuity, 469–476, 476
 - implementing, 131–134, 133
 - for organizational control, 118–120, 119–120
 - planning, 124–125
 - selecting, 129–130, 129
 - stratified mean estimation, 99
 - strong controls, 84–85
 - structured databases, 302
 - structured programming, 283
 - subcontractor liability trap, 137–138
 - subnetworks, 207, 208, 416
 - substantive tests, 13, 99
 - sufficiency of evidence, 100
 - Sullivan, Scott, 4
 - super users, 195
 - supercomputers, 192
 - supervisor review, 353
 - Supervisory Control and Data Acquisition (SCADA), 5
 - supervisory state, 195
 - supervisory users, 195
 - supplies, stockpiling, 476
 - supporting processes in business continuity strategy, 469
 - suppression, 101
 - Surely You're Joking, Mr. Feynman! (Feynman), 201
 - surges, business continuity for, 455
 - surveys for data collection, 79
 - sustaining operations, 169
 - Switched Multimegabit Data Services (SMDS), 234
 - switched virtual circuits (SVCs), 233–234
 - switches, 224–225
 - symmetric-key cryptography, 427–429, 428–429
 - Syslog system, 239, 340
 - system accreditation, 297
 - system audits, 10
 - system availability in SLAs, 336
 - system certification in SLAs, 294–297, 295
 - system control audit review file with embedded audit modules (SCARF/EAM), 88
 - system controls
 - access, 341–343
 - in networking, 194–195
 - parameters, 343
 - System Design phase, 270, 279–283, 280–281
 - System Development Life Cycle (SDLC), 269–272, 270. *See also* life-cycle management vs. BPR, 157
 - Development phase. *See* Development phase in SDLC
 - Disposal phase, 301
 - Feasibility Study phase, 272–276, 274
 - Implementation phase. *See* Implementation phase in SDLC
 - Postimplementation phase, 299–300
 - Requirements Definition phase, 276–279, 276–278
 - System Design phase, 279–283, 280–281
 - system logging (Syslog), 239, 340
 - system monitoring, 339–340
 - system reviews in SDLC, 299–300
 - systematic approach to planning, 68–69, 69
 - systems analysts, 31, 332
 - systems architects, 330
 - Systems Network Architecture (SNA) gateways, 214–215
 - systems programmers, 331
-
- T**
- T1 circuits, 231–232
 - T3 circuits, 231–232
 - tables, database, 304
 - tactical management
 - auditor interest in, 168
 - overview, 139–140, 139

568 tape management systems (TMSs) – triple mirror systems

- tape management systems (TMSs), 196
- target of evaluation (TOE)
 - security functionality, 295–296
- task-based access control (TBAC), 400
- tasks in BPR, 159
- TCP connections, 212
- TCP/IP protocol, 201
- team assignments in business continuity plans, 481–484
- technical category in business continuity, 462
- technical controls, 83
- technical protection of
 - assets, 399
 - application controls, 400–401
 - authentication
 - biometrics. *See* biometrics methods, 401–402
 - types, 402–403, 402–403
 - controls classification, 400
 - encryption, 427–432
 - networks. *See* networks and networking
 - PKI, 432–435, 433–434
 - redundancy, 436, 437
 - security testing, 438
 - telephone security, 437
- technical risks, 163–164
- technological risks, 73
- technology plans, 119, 133
- telephone circuits, 231–232, 233
 - dedicated, 232–233, 233
 - packet-switched, 233–234
- telephone security, 437
- television, closed-circuit, 389
- TeleWall firewall, 380
- templates in biometrics, 408
- temporal keys, 423
- temporary nature of
 - projects, 32–33
- termination
 - employee access, 388
 - policies for, 147
- terms of reference, 23–24
- testing
 - business continuity, 484–485, 486
 - cable, 239
 - compliance, 98
 - independence, 11–13
 - irregularities and illegal acts detection, 101–102
 - penetration, 438
 - results analysis, 100–101
 - results recording, 100
 - in SDLC, 292–293
 - separate environments
 - for, 350
 - substantive, 99
 - tolerable error rate in, 99–100
- theft, 101, 371
- “think big” approach to BPR, 153
- third-generation
 - programming languages (3GL), 284–285
- third party threats, 375
- Thomas, Dave, 456
- Thompson, Ken, 189
- threats
 - defined, 5
 - in risk analysis, 464–467, 464–466
 - security, 370–376, 371
- throughput, 191
 - biometrics, 411
 - mainframe computers
 - for, 192
- time management, 40–41
- time-sharing computer systems, 186, 186
- timing of evidence, 92
- tokens, 403
- tolerable error rate in
 - testing, 99–100
- Top Copy system, 291
- top-down structured
 - programming, 283
- top secret classification, 383
- topologies, network, 217
 - bus, 217, 217
 - meshed, 220–221, 220
- ring, 218–219, 219
- star, 218, 218–219
- total number of items
 - processing controls, 344
- Total Quality Management (TQM), 31
- toys, inherited liability in, 71
- tracking
 - assets and media, 351
 - performance, 169
- traditional audits vs.
 - assessments and self-assessments, 69–70
- traditional project
 - management, 266–267, 267–268
- traditional systems, 255
- traffic analysis, 376–377
- training
 - in business continuity, 484
 - in problem management, 352, 354
 - in SDLC, 297
 - for security, 387
- transaction processing
 - monitors (TP monitors), 306
- transactions
 - controls, 344
 - e-commerce, 310
 - integrity, 306
 - logs, 345, 353
- transborder
 - communication, 145
- transfer risk response, 71
- transfer switches, 394
- transition risks, 163
- Transmission Control Protocol/Internet Protocol (TCP/IP), 202–203
- Transport layer in OSI model, 212, 212
- Transport Layer Security (TLS), 418
- transport mode in IPsec, 418
- trapdoors, 378
- triple constraints in project management, 34
- triple mirror systems, 197, 198

troubleshooting BPR, 167–168

Trump, Donald, 153

Trusted Computer System Evaluation Criteria (TCSEC), 294, 295

trusted routers, 212

TSF security functions, 295

TSP security policy, 295

tumbler locks, 390, 390

tunnel mode in IPsec, 418, 419

tuples, 304, 304

twisted-pair cable, 222–223, 222

Tyco, 4

Type 1 events, 105

Type 2 events, 105

U

unauthorized disclosure, 372

unconfirmed delivery, 212

unicasting, 209

Unified Command System (UCS), 478

uninterruptible power supplies (UPSs), 392–393

unions

- policies for, 147
- respecting, 74–75
- steering committee representation, 122

Uniplexed Operating and Computing System (Unics), 189

uniqueness of projects, 33

United Parcel Service (UPS), 456

United Services Automobile Association (USAA), 166

Unix operating system, 189, 193

unmounting backup process, 197

unqualified opinions, 103

unsatisfactory explanations, 101

unsatisfactory record control, 101

unshielded twisted-pair (UTP) cable, 222–223, 222

unstratified mean estimation, 99

updates

- in SDLC, 300
- software, 294, 295

upper CASE tools, 287, 287

uptime-downtime reporting, 340

US Airways, 454

USB tokens, 403

user acceptance testing, 271

User Datagram Protocol (UDP), 212

user support in business continuity plans, 483

user training

- in business continuity, 484
- in problem management, 352, 354
- in SDLC, 297
- for security, 387

user workstations, 191

users

- data, 385
- identity verification, 400
- interface restrictions, 401
- login management, 341–342

V

validation testing, 292

Value Jet airlines, 137

value of auditors, 24–25

variable sampling, 99

vendors

- in business continuity plans, 484
- proposal reviews, 264–265
- RFI/RFP process, 263

ventilation, 395

ventilation control systems, 284

managing, 289–291

vetting process, 22

vice presidents (VPs), 29

viewing screens for laptops, 20

violation reporting, 389

virtual local area networks (VLANs), 225, 238

virtual machines, mainframe computers for, 192

virtual private networks (VPNs), 417

- IPsec, 418–419, 418–420
- remote access, 417–418

viruses, 345, 378

Visual Basic, 347

Visual Basic Scripting Edition (VBScript), 347

vital functions in business continuity strategy, 470

VLANs (virtual LANs), 225, 238

voice-over-IP networks, 437

voice pattern recognition, 406, 406

volatile data, 356

vulnerabilities, 5

vulnerability scanning, 438

W

wait states, 195

Waksal, Samuel D., 4

war chalking, 380

war dialing, 380

war driving/walking, 380

warm sites, 472–473

water detection, 397, 398

waterfall Model, 267, 267–268

weak controls, 85

web browser functions, 346

website servers, 191

Wendy's company, 456

wet pipe fire suppression system, 395, 396

“what if” questions, 261

white-box testing, 292

white hats, 374–375

Wi-Fi radio, 224, 226, 235

570 wide area networks (WANs) – Yates, Buford

wide area networks (WANs)
description, 238
setting up, 230–231, 230
transmission security,
422–423, 424
willful omission, 101
WiMAX networks, 421
wiping utilities, 356
Wired Equivalent Privacy
(WEP), 236, 421, 423
wireless networks, 419
attacks through, 380
firewalls for, 424,
425–426
IEEE standards, 421

intrusion detection
systems, 424–427
overview, 234–237, 235
setting up, 419–420, 421
WLANs, 422–423, 424
work breakdown structure
(WBS), 42, 159
work effort identification, 262
work of other people
ISACA standards, 15
using, 76
work schedule policies, 148
working papers (WPs), 20
working processes in BPR, 167
workshops for data
collection, 79

workstations, 191
WorldCom, 4
worms, 378
write blockers, 356

X

X.25 standard, 233

Y

Yates, Buford, 4