Index

• Numbers •

12V DC power, 224
80/20 rule
  applying, 48–49
  defined, 289
  Scrum programming, 170
  SSO projects, 105

• A •

abstraction, 172
acceptable-use policy, 72
acceptance strategy, 89
access, root, 13
access control, 96, 123–124, 289
access rights, assigning, 108
access token, 98–99, 289
accessibility
  in closed source software, 36
  defined, 289
  in FOSS, 35
  hardware for, 45
  including in application development, 173–174
  Rehabilitation Act of 1973 (Section 508), 83
ad-hoc replacement, 239–240
administrative access, 13, 72
Administrative management permissions, 107
Adobe Device Central emulator, 186, 187
Advanced Encryption Standard (AES), 252
aggregation, content, 124
agile programming, 169, 289
alt tag, 173
alternative data center locations, 60
alternative energy, 222–223, 287
alternative sites, 268–270
American Recovery and Reinvestment Act of 2009 (ARRA), 221
announce-only lists, 131
anti-malware software
  choosing solution, 250–251
  and cost saving, 284
  defined, 289
  fixing security vulnerabilities, 285
  in security policy, 73
anti-virus updates, 62
AoE (ATA over Ethernet), 155
API (application programming interface), 172, 289
application
  effects of choosing, 14
  incompatibility due to standardization, 54
  virtualization of, 197, 203–204
  vulnerabilities in, 249
application architect, 21–22
application architecture
  multitiered architecture, 171–172
  overview, 171
  SOA, 172–173
application development
  accessibility, including, 173–174
  addressing vulnerabilities in, 251
  application architecture, designing, 171–173
  overview, 163
  RAD strategies, 168–171
  SDLC, 164–168
  as source of complexity, 45–46
application programming interface (API), 172, 289
application rights, 107
application stack, 44, 289
aquatic heat transfer systems, 221
Arbitrated Loop topology, 154
architect, 20–22
ARRA (American Recovery and
Reinvestment Act of 2009), 221
asymmetric encryption, 252–253, 289
asynchronous communication,
127–128, 290
ATA over Ethernet (AoE), 155, 290
attack. See specific attack by name
attacker, 247
auditing, IAM, 112
authentication
boundaries, 109
central, 103–104
cross-realm, 105–106
defined, 290
directory, 103
federated, 104
IAM, 96
overview, 102
within portals, 123–124
portals, 123–124
review of before IAM implementation,
110–111
SSO, 104–105
standards for, 102–103
authorization, 106–107, 111, 290
authorized software, 73
automated system, 63
automation
of backup systems, 63
of data center, 61–63
update/patch management, 283–284
availability, 159, 290
avoidance strategy, 89

• B •
backup
automatic solutions, 63
data storage protection, 158–159
including media in storage surveys, 144
physical protection of media, 159
RPO, 263
testing, 63
of virtual machines, 198
backward-compatibility of open
standards, 38
bandwidth, 183
basic input/output system (BIOS), 241
batteries, 184–185, 224
BCP (Business Continuity Planning),
264, 291
behavioral identification, 101–102
Beowulf, 213
Berkeley Open Infrastructure for
Network Computing (BOINC),
216–217
BES (Blackberry Enterprise Server), 57
BIA (business impact analysis),
261–264, 291
biometrics, 99–101, 290
BIOS (basic input/output system), 241
Blackberry Enterprise Server (BES), 57
bleeding edge technology, 237, 278, 290
blog, 133, 290
Blue Waters supercomputer, 209
Bluetooth, 177, 290
BOINC (Berkeley Open Infrastructure for
Network Computing), 216–217
booster, 179–181
bot, 85, 290
bot herder, 129
botnet
  defined, 291
electronic threats, 85
IRC, 129
  overview, 248–249
processing power used for, 211
bottlenecks, virtualization, 200
breach, data, 66–67, 293
bricked device, 241
broadcast communication
  overview, 138
  podcasting, 139
  RSS, 139–140
  streaming media, 140
browser-based application, 182
brute-force attack, 97, 291
bulk discounts on licenses, 30
business architect, 22
business continuity
  business impact analysis, 262–264
  overview, 261–262
  risk assessment, 264
Business Continuity Planning (BCP), 264, 291
business impact analysis (BIA), 261–264, 291
business intelligence tools, 126
business staff, 16

• C •
CA (Certificate Authority), 252, 254, 291
caching, 58, 60
CAS (Central Authentication Service),
  103–104
case sensitivity, 54
cellular phone, 132, 177
cellular signal booster, 179, 180
central authentication, 103–104, 110–111
Central Authentication Service (CAS), 103–104
centralized data center, 61, 282, 283
Certificate Authority (CA), 252, 254, 291
character set, 35
chat, 128–129
checklist testing, 267
chief architect, 20–21, 27–28
Chief Information Officer (CIO), 20, 275
Children’s Online Privacy Protection Act
  (COPPA), 82–83
CIO (Chief Information Officer), 20, 275
circuitry-embedded keys, 98
Cisco Network Management, 260
classification, data, 18, 72
clearing, 159, 291
client hosting, 203
client protocols, 130
client-server architecture, 291
closed source software
  benefits of, 36–37
  defined, 291
drawbacks, 37–38
  versus open source, 276–277
  overview, 33, 36
cloud computing, 77, 204–206, 291
cluster
  computing, 212–214
defined, 291
  load-balancing, 300
  visualization, 214–215
CMMI (Capability Maturity Model
  Integration), Carnegie Mellon’s, 15
CMS (Content Management System), 124
COBIT (Control Objectives for Information and related Technology), 24–25, 291
cold site, 268–269, 292

**collaboration solutions**
- groupware, 120–122
- networks of trust, establishing, 113–116
- overview, 113
- portals, 123–126
- social media, 116–120
- technology, 76

**collective intelligence**, 118–119, 292

Columbia supercomputer, 212, 213

**commercial off-the-shelf (COTS) software**, 33, 276–277, 292

**commercial open-source software**, 33, 34

**communication**
- about automation of systems, 63
- about opposition to consolidation projects, 56
- asynchronous, 127–128, 290
- during disasters, 270–271
- effective, 19
- eliminating resource silos, 277
- ensuring with IT governance, 24
- importance of in receiving support, 276
- networks of trust, developing, 115
- in RAD strategies, 168
- synchronous, 127–128, 307

**communication technology**
- broadcast communications, 138–140
- classes of communication, 127–128
- collaboration in portals, 124
- community sites, 132–135
- conferencing, 135–138
- groupware, 120–122
- messaging, 128–132
- overview, 127
- community sites, 132–135
- compatibility, 54, 111

**complexity**
- application development, 45–46
- application stack, 44
- connectivity, 46
- hardware, 44–45
- identity management, 45
- legislative and regulatory mandates, 46
- overview, 44
- of password, 97, 99
- as security measure, 68
- in security systems, 72

**complexity reduction**
- complications of complexity, 46–47
- consolidation, planning for, 47–52
- data center automation, 61–64
- data center consolidation, 56–61
- with IAM, 109
- overview, 43
- sources of complexity, 44–46
- standardization concerns, 53–56
- compliance, 109–110, 278–279, 292
- components, updating, 240–241
- compute cluster, 292
- compute farms, 217
- compute grid, 216, 292
- computer system recycling, 227
- computing cluster, 212–214
- concentric-ring security, 69
- conferencing technology
- overview, 135
- videoconferencing, 135–136
- virtual reality, 136
- VoIP, 137
- Web conferencing, 137–138
- confidentiality, 159, 292
- confidentiality, integrity, and availability (CIA), 159
- connection broker, 202
- connectivity, 46, 183
- consolidation
- 80/20 rule, 48–49
- economies of scale, 49
- funding for, 55
- help desk functionality, 51
- overview, 47–48
skill concentration, 51–52

technology end of life, planning for, 49–50
consumables, reducing, 223–224, 286–287
content aggregation, 124
content filtering, 292
content management, 124
Content Management System (CMS), 124
contingency plan, 91, 292
continuity of operations. See business continuity
Control Objectives for Information and related Technology (COBIT), 24–25, 292
convergence, 110
cooling requirements, data center, 61, 201, 220–221, 287
COPPA (Children’s Online Privacy Protection Act), 82–83
cost
full replacement cycle, 233
increases in with complexity, 46–47
of open-source software, 36
of standardization, 31, 33
sunk, as factor in purchase decisions, 47
cost benefit analysis, 92
cost-saving opportunities
anti-malware solutions, 284
automated update/patch management solutions, 283–284
centralized data center, 282
data center consolidation, 283
green IT practices, 286–287
with groupware, 121, 122
with IAM, 109
overview, 281
resource silo elimination, 281
risk assessment, 285
virtualization, 286
workstation replacement, 285
workstation standardization, 282
COTS (commercial off-the-shelf) software, 33, 276–277, 292
countermeasure
for common threats, 90–91
data loss prevention, 251
defined, 292
encryption, 252–254
firewalls, 254–256
intrusion detection and prevention, 256–257
malware protection, 250–251
NAT, 257–259
network monitoring, 260
overview, 250
secure application development, 251
Cray Jaguar supercomputer, 209
Cray X-MP supercomputer, 207
credentials, IAM, 96
cross-platform SSO services, 105
cross-realm authentication, 105–106
customization of commercial software, 37
cutting-edge replacement, 236–237
cutting-edge technology, 293
cyclic replacement, 50, 293
d • D •
daemon, 107, 293
DAS (direct attached storage), 153, 294
data
breaches, 66–67, 293
categories, 145–149
disposal of, 73
protection of, 66–67
requirements, identification of, 18
RPO, 263
data architect, 22–23
data breach notification laws, 66–67, 76
data center
  alternative locations, 60
  automation, 61–63
  centralized, 61
  cooling requirements,
    61, 201, 220–221, 287
  defined, 293
  location and environmental impact,
    220–221
  planning for centralized, 61
  using alternative energy for, 222–223
data center consolidation
  additional benefits, 59
  implementing desirable redundancy, 60
  improved document recovery, 58
  improved resource use, 57–58
  improved security, 58–59
  overview, 56–57, 283
  planning the centralized facility, 61
  reducing complexity through
    virtualization, 59
data classification, 18, 72
data de-duplication, 156–157, 293
data loss prevention (DLP), 251, 293
data mining, 293
data processing, outsourcing of, 78
data removal, 159–161
data storage
  with cloud computing, 206
  data categories, identifying, 145–149
  overview, 143
  protecting data, 157–161
  redundancy in, 60
  storage policy, creating, 149–152
  storage requirements, determining,
    143–145
  storage system design, 152–157
data warehouse, 293
database, 146–147
database rights, 106
DDoS (distributed denial of service),
  249, 294
dead zone, 179–181
de-duplication, 156–157, 293
defense in depth, 69
degaussing, 160, 293
deleted items, removing, 150
Demilitarized Zone (DMZ), 254, 255, 293
deployment, 62–63, 243–244
design phase, SDLC model, 164
desirable redundancy, 60
deskside computer system, 209
desktop computing, 208–209, 217–218
desktop
  remote, 184, 203, 304
  sharing, 138
  virtual, 202–203
destruction methods, 160
destruction policy, 160–161
device driver, 240, 241–242, 293
device interaction, 179
device locking, 187
dictionary attack, 97, 293
digital certificate, 293
digital signature, 253, 294
direct attached storage (DAS), 153, 294
directed network attack, 250
directly applied access tokens, 98
directory, 103, 294
directory services, 45
disaster recovery
  alternative data center locations for, 60
  alternative sites, 268–270
  in closed source software, 36
  communicating during disaster,
    270–271
  cost of, 47
  data storage protection, 158–159
  overview, 262–263
  recovery plan, preparing, 264–268
Disaster Recovery Planning (DRP), 264, 294
discoverability, 172
discovery, 83, 294
discussion board, 133–134
discussion list, 131
disk mirroring, 158
disposal practices, 226–227
distributed computing,
   210–211, 216–217, 294
distributed denial of service (DDoS), 249, 294
distributing storage policy, 151–152
DLP (data loss prevention), 251, 293
DMZ (Demilitarized Zone), 254, 255, 293
DNS (Domain Name Service), 182
document management, 124–125
document recovery, 58
Domain Name Service (DNS), 182
draft-mode printing, 286
driver, device, 240, 241–242, 293
DRP (Disaster Recovery Planning),
   264, 294
duplex printing, 286

• E •

EAP (Extensible Authentication Protocol), 103, 295
EC2 (Amazon Elastic Computer Cloud), 205
economy of scale
   as benefit of standardization, 30, 49
   with consolidation, 59
defined, 294
Security as a service model, 78
   strategies to obtain, 278
efficiency, 30
Electronic and Information Technology Accessibility Standards, 174
electronic threats. See threat e-mail
   issues related to selection of platform, 13–14
   kill pills, 188
   overview, 129
   phishing, 85
   planning use in enterprise, 129–130
   protocol, choosing, 130–131
   spam, 249, 306
   storage requirements, 147–148
   embedded system, 18, 294
   emulators, 186, 187
encryption
   asymmetric, 289
   of backup media, 159
defined, 294
   in mobile device data, 183
   on-device, 187–188
   public-key, 303
   secret-key, 252, 305
   in security policy, 73
   in security systems, 67, 68
   symmetric, 252, 307
types of, 252–254
ENERGY STAR, 221–222, 287, 294
energy tax credits, 221
enterprise, defined, 9–10, 294
enterprise architect, defined, 295
enterprise architecture certification, 25
enterprise architecture, defined, 295
enterprise architecture framework
   defined, 295
   FEAF, 26
   Gartner Enterprise Architecture Framework, 26–27
   overview, 25
   TOGAF, 26
   Zachman Framework, 26
enterprise planning
  defining enterprises, 9–10
  defining success, 14
  finding best solutions, 10
  issues in enterprises, 11–13
  overview, 9
  preventing failure, 15–16
  providing leadership, 10–11
  technological connections, 13–14
  using maturity models, 15
enterprise-level storage strategies, 153–155
environmental threat, 85
error message, 70, 249
Ethernet, 295
executives
  commitment to security policy, 74
  lack of support from, 16, 275–276
  understanding of security program, 68
expiration, password, 97–98, 99
exploit, 295
extended replacement cycle, 220
Extensible Authentication Protocol (EAP), 103, 295
Extensible Markup Language (XML), 295
extension of trust, 114
extranet, 182, 295
extreme programming, 170, 295

● F ●

facial recognition, 101
factor, 295
failover, 60, 295
farm, 217, 296
fault tolerance, 158, 296
FCIP (Fibre Channel over IP), 154
FEAF (Federal Enterprise Architecture Framework), 26
feature creep, 165, 168
Federal Educational Rights Protection Act (FERPA), 82
Federal Enterprise Architecture Framework (FEAF), 26
Federal Information Processing Standards, 71
federated authentication, 104
feedback, prototype model, 166
FERPA (Federal Educational Rights Protection Act), 82
Fibre Channel, 154, 296
Fibre Channel over IP (FCIP), 154
file repository, 145–146, 296
file rights, 106
file versioning, 58, 146, 296
fingerprint test, 100
fire suppression system, 61
firewall, 68, 73, 254–256, 296
firmware, 241, 296
floating-point operations per second (FLOPS), 209, 296
font, 286
forum, 133–134, 296
FOSS (free open-source software), 33–36, 296
framework, enterprise architecture, 25–27, 295
framework-specific certification, 25
free open-source software (FOSS), 33–36, 296
full interruption testing, 267
full replacement, 233–234, 296
functionality, effect of standardization on, 53–54
funding, consolidation project, 55
• G •
gait identification, 101
Gartner Enterprise Architecture Framework, 26–27
Gartner Research, 118, 296
general purpose computing on graphics processing units (GPGPU), 210
geothermal cooling, 221
gigaflop, 209
GLBA (Gramm-Leach-Bliley Act), 82–83
global positioning system (GPS), 296
GPGPU (general purpose computing on graphics processing units), 210
GPS (global positioning system), 296
GPU (graphical processing unit), 297
Gramm-Leach-Bliley Act (GLBA), 82–83
graphical processing unit (GPU), 224, 297
green IT
  alternative energy, 222–223
data center location, 220–221
defined, 297
disposal practices, 226–227
ENERGY STAR certification program, 221–222
energy tax credits, 221
extended replacement cycles, 220
hardware, selecting green, 224–225
overview, 219–220
reducing consumables, 223–224
reducing cost from consumables with,
  286–287
settings, configuring green, 225–226
telecommuting, 220
telework, 220
virtualizing hardware, 226
grid computing, 215–216, 297
grid tools, 216
groupware, 120–122, 297

• H •
HAL (hardware abstraction layer), 198, 297
hand geometry identification, 100
hardware
  discounts on licenses, 30
disposal practices, 226–227
ENERGY STAR certification,
  221–222, 287
extended replacement cycles, 220
failover capability of servers, 60
firewalls, 254
lease or warranty replacements, 161
personally owned equipment, 279–280
platforms, 12–13
power saving options, 225–226
green, selecting, 224–225
as source of complexity, 44–45
tech refresh planning, 199–200
theft of, 66
updating in virtual environments, 200
VPNs, 184
hardware abstraction layer (HAL), 198, 297
hardware update strategy
  ad-hoc replacement, 239–240
  cutting-edge replacement, 236–237
  defined replacement cycles, 232–236
  keeping systems until failure, 232
  overview, 231–232
  surplus technology, relying on, 238
technology as rewards, 238
  trickle-down replacement, 237–238
hazardous waste, 227
Health Information Technology for Economic and Clinical Health (HITECH) Act, 67, 76
Health Insurance Portability and Accountability Act (HIPAA), 46, 82–83
help desk functionality, 51
hidden obsolescence, 50
high-availability cluster, 297
high-performance computing
  compute farms, 217
  computing clusters, 212–214
  defined, 297
desktop, 217–218
grid computing, 215–216
overview, 207
supercomputers, 207–211
visualization clusters, 214–215
volunteer computing, 216–217
HIPAA (Health Insurance Portability and Accountability Act), 46, 82–83
HITECH (Health Information Technology for Economic and Clinical Health) Act, 67, 76
homeostasis, risk, 91
host server, 197
host-based IDS, 256
hosting
  client, 203
  of groupware, 122
  virtual machines (VM), 198–199
hot site, 269, 297
hotfixes, 245
hotspot, 177–178, 191, 297
human threat, 86
Hypertext Transfer Protocol (HTTP), 130–131, 297
hypervisor, 198, 199, 203, 265, 297

I

IAM (Identity and Access Management).
  See also identification
authenticating users, 102–106
authorizing access, 106–107
creating strategy, 108–109
defined, 298
implementing, 110–112
overview, 95–96
icons, explained, 4–5
identification
  access tokens, 98–99
  behavioral, 101–102
  biometric, 99–101
defined, 297
overview, 96
passwords, 97–98
Identity and Access Management (IAM).
  See also identification
authenticating users, 102–106
authorizing access, 106–107
creating strategy, 108–109
defined, 298
implementing, 110–112
overview, 95–96
identity management, 45, 298
IDS (intrusion detection system), 35, 256–257, 299
IEEE 802.11, 298
iFCP (Internet Fibre Channel Protocol), 154
image-based deployment, 62–63, 244
IMAP (Internet Messaging Access Protocol), 130–131, 298
implementation phase, SDLC model, 164
incident management, 73
industrial espionage, 86
infected computer, 247
information security planning
  layered frameworks, using, 68–70
  overview, 65, 67–68
protected enterprise data, 66–67
security policy, developing, 72–75
security standards, implementing, 70–71
simplicity, 71–72
technology, using to support security, 75–79
viewing as program versus project, 71
workable programs, designing, 68
Information Technology Infrastructure Library (ITIL), 25, 298
information technology (IT) governance, 24–25, 298
informational token, 98
initiation and planning phase, SDLC model, 164
input, unsanitized, 249
insourcing, 79
instant messaging (IM), 131–132, 298
instruction detection software (IDS), 35
instruction set, 241
integrity, 159, 298
intellectual property identification, 35
interface, portal, 125
internal IP address, 298
international character set, 35
International Organization for Standardization (ISO), 298–299
Internet
accessibility technologies, 173
defined, 298
open standards on, 38
sustained connections for groupware, 122
Internet Fibre Channel Protocol (iFCP), 154
Internet Messaging Access Protocol (IMAP), 130–131, 298
Internet Protocol address. See (IP) Internet Protocol) address
Internet Protocol Security (IPSec), 103, 299
Internet Relay Chat (IRC), 129, 248
Internet Small Computer System Interface (iSCSI), 154, 299
intranet, 299
intrusion detection system (IDS), 256–257, 299
intrusion prevention system (IPS), 256–257
inventory, 144
IP (Internet Protocol) address, 250, 257–259, 298
IPS (intrusion prevention system), 256–257
IPSec (Internet Protocol Security), 103, 299
IRC (Internet Relay Chat), 129, 248
iris detection, 101
iSCSI (Internet Small Computer System Interface), 154, 299
ISO (International Organization for Standardization), 299
ISO/IEC 27000 series, 70
IT governance, 24–25, 298
ITIL (Information Technology Infrastructure Library), 25, 298, 299

• J •
justification of changes, 19

• K •
Kerberos, 103, 105–106, 299
kill pills, 188
Kryder’s Law, 155, 299

• L •
L2TP (Layer 2 Tunneling Protocol), 299
LAN (local area network), 300
laptop
ad-hoc replacement strategy, 239–240
cutting-edge replacement strategy, 236–237
full replacement cycle, 233–234
laptop (continued)
LoJack, 188–189
overview, 176
partial/staged replacement cycle, 234–236
trickle-down replacement strategy, 237–238
using technology as employee rewards, 238
Layer 2 Tunneling Protocol (L2TP), 299
layered framework, 68–70
LCD system, 225
LDAP (Lightweight Directory Access Protocol), 103, 299
lead architect, 21
leadership, 10–11, 16, 280
leased equipment, 161
legacy system
integrating, 277–278
layered security around, 70
planning for technology end of life, 50
tech refresh, 232
using encryption with SOA, 68
legal mandate. See mandate
liability for loss of mobile devices, 190
licensing, 30, 201, 206
life cycle of technology, 37, 49–50
lighting, 224
Lightweight Directory Access Protocol (LDAP), 103, 299
limitations, recognition of, 280
line-of-business (LOB) applications, 299
link to master copy, 156–157
load balancing, 60, 198, 300
LOB (line-of-business) applications, 299
local area network (LAN), 300
locking, mobile device, 187
log
files, storage requirements, 148
IM, 132
purpose of, 72
regulatory mandates for, 82
reviewing, 63
logical unit number (LUN), 153
Logon permission, 107
LoJack, laptop, 188–189
long-range wireless technology, 177–178
LUN (logical unit number), 153

M

mailing list, 131
maintenance phase, SDLC model, 164
malware. See also botnet
defined, 300
electronic threats, 85
overview, 247–248
protection against, 250–251
security policy for, 73
spyware, 248, 306
Trojans, 248
viruses, 248
worms, 248
Managed security services model, 78
mandate
compliance with, 278–279
discovery and retention, 83
generalized, 83–84
identity management, 108–109
increase in complexity from, 46
legal requirements, 82–83
overview, 81–82
man-in-the-middle attack, 189, 252, 300
mapping data resources, 83
matrix, risk, 89
maturity models, 15
Message Passing Interface (MPI), 213
messaging technology, 128–132
metadirectory, 104
Metcalfe’s Law, 115–116, 301
microblogging, 133, 300
microwaving optical media, 227
mirroring, disk, 158
mitigation, risk, 92
mitigation strategy, 89
mobile access policy, 189–191
Index

mobile technology
- Bluetooth, 177
- boosters, 179–181
- cell phones, 177
- dead zones, 179–181
- device interaction, 179
- fixed stipend for, 279–280
- laptops, 176
- long-range wireless, 177–178
- mobile access policy, 189–191
- mobile network access to
  organizational resources, 182–185
- netbooks, 176
- overview, 175
- security, 178–181
- smartphone computing, 186–189
- synching media files and storage issues, 150, 151
- tablets, 176–177
- modernization of technology, 50
- monoculture, technology, 55, 307
- Moore’s Law, 155, 235, 300
- MPI (Message Passing Interface), 213
- multimedia files, 147
- multiplexing, 259, 300
- multitiered architecture, 171–172, 300

N

- Nagios, 260
- naked hypervisor, 198, 199
- NAS (network attached storage), 153, 301
- NAT (network address translation), 257–259, 300
- National Association of State Chief Information Officers (NASCIO) Enterprise Architecture Maturity Model v1.3, 15
- National Vulnerability Database, 62, 86
- natural threat, 85
- navigation in extended network, 182
- netbook, 176

network. See also collaboration solutions
- attacks on, 250
- culture, developing with portals, 126
- image based deployment over, 244
- mobile access to, 182–185
- monitoring, 260
- nursery, 244
- stateless packet filtering, 255–256
- test, 242
- network address translation (NAT), 257–259, 300
- network attached storage (NAS), 153, 301
- network interface card (NIC), 200
- network mapper, 35
- network of trust, 113–116
- network-based IDS, 256
- New object creation permission, 107
- news feed, 139
- NIC (network interface card), 200
- notebook, 176
- notification laws, data breach, 66–67, 76
- n-tier application architecture,
  171–172, 173, 301
- nursery, 244, 259

O

- obscurity of password, 97
- obsolescence, 49–50
- offshoring, 23, 79, 301
- on-device encryption, 187–188
- Open Group Architecture Framework (TOGAF), 26
- Open Records requests, 190
- open source software
  - benefits of, 34–35
  - versus closed source, 276–277
  - defined, 301
  - drawbacks, 35–36
  - overview, 33–34
  - open standards, 38–39, 301
  - operating cycle speed, 225
operational planning, 48, 301
outsourcing
alternative site management, 269–270
defined, 301
destruction of media, 160
risk management, 92
of security, 78–79
of supporting architect roles, 23
overwriting, 159, 160, 301

• P •

packet, 301
packet-filtering firewall, 255–256
pair programming, 168
palm sensor, 100
PAN (Personal Area Network), 301
pandemic, planning for, 265
paper, use of, 223–224
parallel processing, 210, 301
Pareto Principle
applying, 48–49
defined, 289
Scrum programming, 170
SSO projects, 105
partial replacement, 234–236, 301
partner organizations, 32, 77–78
password
frequent changes in, 71
identification systems, 97–98
management with IAM, 112
minimum standards for, 99
in security policy, 73
PAT (port address translation), 302
patch
automated management of, 283–284
defined, 301
management of, 62
regular application of, 251
software maintenance, 245
Payment Card Industry Data Security Standards, 46
PDA (personal digital assistant), 302
permission
assigning within portals, 124
user account, 107
Personal Area Network (PAN), 301
personal digital assistant (PDA), 302
personal sites, 125
personalization features, portal, 125
personalized portal interfaces, 125
personally identifying information (PII), 83
personally owned equipment, 279–280
petaflop, 209
phased implementation of groupware, 122
phishing e-mail, 85
physical-to-virtual (p2v) process, 201
PKI (public-key infrastructure), 253, 303
planned obsolescence, 49–50
planning, enterprise. See enterprise planning
planning levels, 48
platform
defined, 302
excess of, 12–13
platform architecture, 29–30, 302
platform standardization
benefits of, 30–31
closed source software, 33, 36–38, 276–277
consideration of business needs, 39–40
open source software, 33–36, 276–277
open standards, 38–39
overcoming challenges in, 31–33
overview, 29–30
PMO (Project Management Office), 27
podcasting, 139, 302
PoE (Power over Ethernet), 224
Point of View ray-tracing (POV-Ray)
application, 213
Point to Point topology, 154
Point-to-Point Tunneling Protocol (PTPP), 302
policy. See specific policy by name
POP (Post Offi ce Protocol), 130–131, 302
port address translation (PAT), 259, 302
portable computer, 175–176
portal
authentication and access control, 123–124
business intelligence tools, integrating, 126
collaboration and communication technologies, 124
content aggregation, 124
content management, 124
defi ned, 302
document management, 124–125
topology, 123
enterprise search, 125
file storage requirements, 152
network culture, developing with, 126
overview, 123
personalization, 125
portfolio management, 28
portlet, 123, 302
Post Offi ce Protocol (POP), 130–131, 302
POV-Ray (Point of View ray-tracing) application, 213
power consumption, 219
Power over Ethernet (PoE), 224
power requirements, data center, 61
power settings, hardware, 225–226
power supply, mobile device, 184–185
power-saving features, 287
Preboot eXecution Environment (PXE), 196, 201
preventing failure, 15–16
printing, 286–287
prioritizing threats, 89–90
privacy laws, 84
privacy-related certification, 122
private cloud, 205
private IP address, 257–259
probability
  defi ned, 302
determining, 88
  reducing for threats, 90–91
of threat, 87
processing speed, 209
processor, upgrading, 240–241
product stack, single-vendor, 30
productivity, eff ect of standardization on, 54
profile, user, 125
program, 28, 71
programming
  agile, 169, 289
  extreme, 170, 295
  Scrum, 170–171, 305
programming language
  eff ects of choosing, 14
  reducing complexity in use of, 45
  source code, 33
programming phase, SDLC model, 164
project management, 27–28, 303
Project Management Offi ce (PMO), 27
protection, data, 66–67, 157–161
protocol, client, 130
prototype, 303
prototype iterative model, 166–167
proxy server, 60
PTPP (Point-to-Point Tunneling Protocol), 302
public-key encryption, 252–253, 303
public-key infrastructure (PKI), 253, 303
purging, 160, 303
PXE (Preboot eXecution Environment), 196, 201
qualitative analysis, 88, 303
quality settings, printing, 286
quantitative analysis, 87, 303

RAD (rapid application development), 169–171, 303
radio-frequency identification (RFID) proximity cards, 98
RAID (redundant array of independent disks), 60, 158, 304
rapid application development (RAD), 169–171, 303
RCRA (Resource Conservation and Recovery Act), 221
reactionary replacement strategy, 239–240
Really Simple Syndication (RSS), 139–140, 303
real-time collaboration, 120
recovery plan
developing scenarios, 264–265
overview, 264
testing, 267
updating, 267–268
virtualization strategies, 265–267
recovery point objective (RPO), 263, 303
recovery time objective (RTO), 263–264, 304
recycling, 226–227
Red Hat Network (RHN), 284
redesign challenges
compliance, 278–279
hardware replacement, 278
lack of executive support, 275–276
legacy systems, integrating, 277–278
opposition to change, 276
overview, 275–280
personally owned equipment, 279–280
platform standardization, 276–277
recognition of limitations, 280
resource silos, eliminating, 277
separate revenue streams, 279
redundancy, 18, 47, 60, 304
redundant array of independent disks (RAID), 60, 158, 304
registration, software, 240
regulatory mandate. See mandate Rehabilitation Act of 1973 (Section 508), 83, 174
reliance on technology, 31–32
Remember icon, 4
remote access policy, 190
remote desktop, 184, 203, 304
removable media, 144
render grid, 216
replacement, hardware
ad-hoc, 239–240
cutting-edge, 236–237
cyclic, 50
defined cycles for, 232–236
extended cycles, 220
overview, 231–232
surplus technology, relying on, 238
technology as rewards, 238
trickle-down, 237–238
upon failure of system, 232
replacement, warranty, 161
repository, file, 145–146
requirements analysis and definition phase, SDLC model, 164
resource, integration of existing, 18
resource allocation, 249
Resource Conservation and Recovery Act (RCRA), 221
resource silo
defined, 304
eliminating, 57, 277, 281
excess of, 12
retention, 83
retinal detection, 101
reuse of password, 99
revenue stream, 279
RFID (radio-frequency identification) proximity cards, 98
RHN (Red Hat Network), 284
risk, defined, 304
risk acceptance, 304
risk assessment
business continuity planning, 264
defined, 304
impact, determining, 88–89
overview, 87–88
probability, determining, 88
results, using to find vulnerabilities, 285
risk matrix, 89
tool in security policy approval, 74
risk avoidance, 304
risk homeostasis, 91, 305
risk management
addressing risk, 89–92
assessing risk, 87–89
defined, 305
threats, identifying, 84–86
vulnerabilities, identifying, 86–87
risk matrix, 89
risk mitigation, 92, 305
risk transference, 305
roles, 20–23
root access, 13
RPO (recovery point objective), 263, 303
RSS (Really Simple Syndication), 139–140, 303
RTO (recovery time objective), 263–264, 304

• S •

SaaS (Software as a Service) model, 122
SAN (storage area network), 153–155, 306
Sarbanes-Oxley Act (SOX), 82
scale, economy of. See economy of scale
scale of need, 32
SCCM (System Center Configuration Manager), 283
scenario, 264–265
schema, 111
Scrum programming, 170–171, 305
SDLC (Software Development Life Cycle), 164–168, 306
search, portal, 125
search engine, 182
secret-key encryption, 252, 305
Section 508 of Rehabilitation Act of 1973, 83, 174
secure application development, 251
Secure Sockets Layer (SSL), 183–184, 253, 305
security. See also information security planning
application development, 251
backup and recovery, 159
CIAs, 159
of cloud computing, 205
in community-created code, 35
consolidation, improving with, 58–59
data loss prevention, 251
defined, 305
diversity as factor in, 55
in embedded systems, 18
encryption, 252–254
firewalls, 254–256
IAM, 109
identifying data users, 18
intrusion detection and prevention, 256–257
malware protection, 250–251
mandates, 46
mobile device, 187–188
NAT, 257–259
network monitoring, 260
overview, 247
reducing complexity in identity management, 45
remote desktops, 184
security (continued)
  SaaS providers, 122
  threats, identifying, 247–250
  wireless transmission systems, 179, 180
Security as a service model, 78
security policy, 72–75
security standards, 70–71
security update, 245, 251
security utilities, FOSS, 35
self-serve recovery, 58
self-service mechanism for password resets, 112
sensitive data
  in e-mail, 130
  encryption of, 252
  improved security with consolidation, 58
  layered security around, 70
  limitations in offshoring, 23
  multiple firewall protection for, 254
server
  ad-hoc replacement strategy, 239–240
  cutting-edge replacement strategy, 236–237
  data center consolidation, 283
  failover capability, 60
  five-year replacement cycle for, 236
  full replacement cycle, 233–234
  load balancing, 60
  partial/staged replacement cycle, 234–236
  proxy, 60
  security policy for installations, 73
  TFTP, 196
  trickle-down replacement strategy, 237–238
  updating, 231
  VDI, 202–203
  virtualization of, 59, 149–152, 197–201
service, 305
service pack, 245
service rights, 107
service set identifier (SSID), 305
service-oriented architecture (SOA), 68, 111, 172–173, 305
shared account, 109
SharePoint Unified Logging Service (ULS) logs, 148
sharing
  desktop, 138
  of resources, 57–58
  Shibboleth standards, 103
Short Message Service (SMS), 132, 306
shutdown permission, 107
signature identification, 102
Simple Mail Transfer Protocol (SMTP), 306
Simple Object Access Protocol (SOAP), 306
simulation testing, 267
single sign-on (SSO), 104–105, 123–124
site survey, 179–180
skill concentration, 51–52
smartphone
  device locking, 187
  familiarity with, 186
  kill pills, 188
  laptop LoJack, 188–189
  on-device encryption, 187–188
  overview, 186
  planning ahead, 186–187
SMS (Short Message Service), 132, 306
SMTP (Simple Mail Transfer Protocol), 306
snapshot, copying, 62
SOA (service-oriented architecture), 68, 111, 172–173, 305
SOAP (Simple Object Access Protocol), 306
social engineering, 73, 97, 306
social media, 73, 116–120, 132–135
software. See also anti-malware software; application development; closed source software; open source software
authorized, 73
cost compared to complexity, 47
development, 45–46, 78
firewalls, 254
fixing vulnerabilities in, 62
groupware, 120–122
image-based deployment, 62–63
incompatibility due to standardization, 54
licenses, 30
malware, 247–249
patch management, 62
platforms, 12–13
registration issues with component upgrades, 240
settings, configuring green, 225–226
tech refresh planning, 199–200
updates, 62, 200, 242–245
virtualization, 203–204
VPNs, 184
software architect, 21–22
Software as a Service (SaaS) model, 122
Software Development Life Cycle (SDLC), 164–168, 306
solar energy, 223, 287
solid-state drive (SSD), 225
source code, 33
SOX (Sarbanes-Oxley Act), 82
spam, 249, 306
spiral model, 167–168, 306
spoofing, IP address, 250
spyware, 248, 306
SSD (solid-state drive), 225
SSID (service set identifier), 305
SSL (Secure Sockets Layer), 183–184, 305
SSO (single sign-on), 104–105, 123–124
stack, single-vendor product, 30
staged replacement, 234–236, 306
Stallion visualization cluster, Texas Advanced Computing Center, 214–215
standard base deployment strategy, 243
standardization. See also platform standardization
in closed source software, 37
cyclic replacement of technology, 233
for data center automation, 62
decreased productivity, 54
and desire for bleeding edge technology, 278
incompatibility with existing applications, 54
of open-source software, 36
overview, 53–56
of platforms, 12–13
preparing for opposition, 55–56
reduced functionality, 53–54
requirement for image-based deployment, 62
risk of technology monoculture, 55
standards
authentication, 102–103
cloud computing, 205
defined, 306
defining technical, 18–19
open, 38–39, 301
security, 70–71
Startup permission, 107
stateful packet filtering, 256, 306
stateless packet filtering, 255–256, 306
stipend for mobile device use, 279–280
storage area network (SAN), 153–155, 306
storage configuration, 152–153
storage grid, 215–216, 306
storage policy, 149–152
storage survey, 144, 307
strategic planning, 48, 307
streaming media, 140, 307
strength, password, 97–98
subnet, 307
sub-system update, 240–242
supercomputer, 207–211, 307
superuser access, 13
supervisor access, 13
support skill alignment, 52
surplus technology, relying on, 238
survey, storage, 144
Switched Fabric topology, 154
symmetric encryption, 252, 307
synched media files, 150, 151
synchronous communication, 127–128, 307
System Center Configuration Manager (SCCM), 283
system memory, upgrading, 240–241
Systems Development Life Cycle (SDLC).
See Software Development Life Cycle (SDLC)
Systems Security Engineering Capability Maturity Model, 70

T

tablet, 176–177
tactical planning, 48, 307
tasks, 17–19
tax credit, energy, 221
TCP/IP (Transmission Control Protocol/Internet Protocol), 307
team creation, 114
tech refresh, 199–200, 231, 285, 307
technical standards, defining, 18–19
Technical Stuff icon, 5
technology. See also specific types of technology
collaborative, 76
effect of change on connected, 13–14
life cycle of, 37, 49–50
monoculture, 55, 307
reviewing for IAM strategy, 108
as rewards strategy, 238
using to support security, 75–79
technology architect, 21
technology stack, 44, 308
telecommuting, 220, 308
teleworking, 220, 308
terrorism, virtual, 136
test network, 242
testing phase, SDLC model, 164
tethering, 308
text messaging, 132, 308
TFTP (Trivial File Transport Protocol) server, 196
Thawte, 254
theft of hardware, 66
thick client, 202, 308
thin client, 202, 308
threat
application vulnerabilities, 249
countermeasures for, 90–91, 250
defined, 308
directed network attacks, 250
electronic, 85
human, 86
malware, 247–249
mitigation, 92
natural or environmental, 85
overview, 84–85, 247
prioritizing, 89–90
reducing impact of, 91
reducing probability of, 90–91
risk assessment, 87–89
three-tier architecture, 171
three-user network, 115–116

tiered data storage, 156, 157, 308
timebox, 308
Tip icon, 4

together, 308

Tip icon, 4

TOGAF (Open Group Architecture
Framework), 26
token, access, 98–99, 289
topology, 154
Toxic Substances Control Act (TSCA), 221
training, employee, 75, 117
transference strategy, 89
Transmission Control Protocol/Internet
Protocol (TCP/IP), 307
transparency, 206
trickle-down replacement, 237–238, 308
Trivial File Transport Protocol (TFTP)
server, 196
Trojan, 248, 256, 308
trust, network of, 113–116
TSCA (Toxic Substances Control Act), 221
tunneling, 309

V

VDI (virtual desktop infrastructure)
server, 202–203
vendor, virtualization, 198
vendor-specific certification, 25
vendor-specific protocol, 130
versioning, file, 58, 124–125, 146
video card upgrade, 240–241
videoconferencing, 135–136, 309
virtual desktop, 202–203
virtual desktop infrastructure (VDI)
server, 202–203
virtual machine, 197, 198–199, 309
virtual private network (VPN), 183–184, 309
virtual reality, 136
virtual server, 149
virtual terrorism, 136
virtualization
applications, 203–204
cloud computing, 204–206
and cost saving, 286
defined, 309
in disaster recovery planning, 265–267
of hardware for environmental
reasons, 226
overview, 195–197
reducing complexity through, 59
servers, 197–201
update deployment strategies, 244
workstation, 201–203
virtualization host, 309
virtualized application, 309
virtualized desktop, 309
virus, 71, 248, 309
virus creation kit, 248
visualization cluster, 214–215
voice analysis, 102

ULS (SharePoint Unified Logging Service)
logs, 148
unsanitized input, 249
update
automated management, 283–284
disaster recovery plan, 267–268
management of, 62
security software, 251
update strategy. See also hardware
update strategy
overview, 231
software updates, 242–245
sub-system updates, 240–242
upgrades, software, 37, 38
USB fingerprint biometric reader, 100
user account, 107, 109, 112
user feedback, prototype model, 166
Voice over Internet Protocol (VoIP), 137, 310
volunteer computing, 216–217
VPN (virtual private network), 183–184, 309
vulnerability
in applications, 249
defined, 310
identifying, 86–87
using risk assessment to find, 285

Wi-Fi (Wireless Fidelity), 179, 185, 310
Wi-Fi Protected Access (WPA/WPA2), 183, 311
wiki, 134–135, 311
WiMAX (Worldwide Interoperability for Microwave Access), 177
wind turbine power generation, 223, 287
Windows Server Update Services (WSUS), 283–284
wiping mobile devices, 188, 189
Wired Equivalent Privacy (WEP), 311
wireless access point, 189, 311
Wireless Fidelity (Wi-Fi), 179, 185, 310
wireless local area network (WLAN), 311
wireless transmission, 177–178, 183, 189
wireless use policy, 191
workable program, designing, 68
workflow, IAM, 112
workstation
ad-hoc replacement strategy, 239–240
cutting-edge replacement strategy, 236–237
full replacement cycle, 233–234
high-performance computing cycle, 217–218
partial/staged replacement cycle, 234–236
replacement, 285
security policy for installations, 73
standardization, 282
trickle-down replacement strategy, 237–238
updating, 231
virtualization, 201–203
Worldwide Interoperability for Microwave Access (WiMAX), 177
worm, 311
WPA/WPA2 (Wi-Fi Protected Access), 183
WSUS (Windows Server Update Services), 283–284

wake-on-LAN functionality, 226
walkthrough testing, 267
WAN (wide area network), 310
wardriving, 189
warm site, 269, 310
Warning icon, 5
warranty replacement, 161
waste disposal, 73
water consumption, 220
water cooling, 287
water microturbine power generation, 223
waterfall model, 165, 310
Web conferencing, 137–138, 310
Web feed, 139
Web service, 310
Web Services Description Language (WSDL), 310
Web site
accessibility technologies, 173
Chief Information Officers Council, 26
community sites, 132–135
containing warnings about software flaws, 249
point of contact, 270–271
social networking, 117–119
wiki, 134
webinar, 138, 310
wide area network (WAN), 310
• X •
X.500 suite, 102
XML (Extensible Markup Language), 295

• Z •
Zachman Framework, 26
zero-day threat, 311
zettaflop, 209