Accounting and finance, impact of elastic cloud model on, 175
ACID transactions, 74–75, 89–90
Acme eAuctions (AEA) case study
  business architecture, 43, 61
  business problem statement, 45
  cloud deployment models, 66–67
  cloud service models, 21–22, 48
  data design decisions, 97–98
  dealing with change, 34, 53
  disaster recovery planning, 161
  final architecture, 188–190
  IaaS use case, 66
  logging strategy, 124
  mobile development decision, 51
  monitoring strategy, 146–147
  organization change planning, 178–180
  PaaS use case, 64–65
  pragmatic approach, 46–47
  SaaS use case, 60–62
  security requirements, 103
  service level agreements, 134–135
Active-passive cold model, 154, 155
Active-passive warm model, 154, 156
AEA case study. See Acme eAuctions (AEA) case study
Agility of cloud computing, 169–170
Allspaw, John, 163
Amazon EC2, 65
Amazon Elastic Block Store, 151
Amazon Web Services (AWS)
  availability zones, 120, 151, 152
  compliance road map, 85–86
  Global Start-Up Challenge, 57
  as IaaS, 15
  infrastructure management and, 2
  Netflix and, 9
  outages, 66
  security of, 30, 105
  service level agreement, 32–33
Apigee, 51
API management, 115–116
API SaaS tools, 51
Application layer
  KPIs and, 143
  performance at, 140
  security and, 107
Applications
  cloud, auditing, 78–80
  cost of building in cloud, 39
  legacy, porting to cloud, 3
  migrating to cloud, 23–24, 25, 26, 26–27
  mobile, and PaaS, 187–188
  web, security of, 132
Application stack layer, 141, 151
Architecture
  business architecture diagram, 43–45
  defining, 54
  enterprise, value of, 41
  loosely coupled, 24
  tightly coupled, 24
Archiving use cases, 68
Auditing
  cloud applications, 78–80
  design strategies for, 83–85
  regulations and, 80–83, 81
  security and, 118
Automating
  deployments, 166–167
  infrastructure, 165–166
Automation strategy for security, 110
AWS. See Amazon Web Services
Backup and restore method, classic, 153, 153–154
BASE transactions, 75
Bias, Randy, 173
Big-data PaaS solutions, 188
Business and technical requirements.
  See Customer requirements
Business architecture diagram, 43–45, 44
Business impact of elastic cloud model, 174–178
Business models, 186–187

Case studies
  Instagram, 8
  National Oceanic and Atmospheric Administration, 10
  Netflix, 9
  Obama campaign e-commerce site, 10
  See also Acme eAuctions (AEA) case study
Cash flow, 175
Categories of information, monitoring, 139–145
CD (continuous delivery), 168–170
CDNs (content delivery networks), 96–97
Centralization strategy for security, 109
Centralized logging strategy, 119–125, 121
Change, resistance to, 178, 180. See also Organizational change
Chatter, 82
CI (continuous integration), 168–170
Client-server era, 3–4
Cloud bursting, 68
Cloud computing
  agility of, 169–170
  benefits of, 6–7
  characteristics of, 13n
  evolution of, 6, 11, 183–185
  maturation of, 5
  overview of, 190–191
  security maturation, 7
  use cases, 68–69
  visual model of, 19
See also Case studies; Designing cloud services; Hybrid clouds; Private clouds; Public clouds; Worst practices
Cloud culture, 185–186
Cloud Security Alliance
  IaaS definition, 14–15
  PaaS definition, 16
Cloud service providers (CSPs), 77, 78, 79–80. See also Vendors
Cloud stack
  choosing service model and, 56
  IaaS, 104
  monitoring and, 139
  overview of, 13, 14
  PaaS, 106
  SaaS, 108
Coghead, 32
Column store databases, 96
Commodity clouds, 6
Compliance, monitoring, 144–145
Concur expense management software, 1, 132
Consumer, maturity of, and auditing strategy, 84
Consumer experience, visualizing, 49–51
Content delivery networks (CDNs), 96–97
Continuous delivery (CD), 168–170
Continuous integration (CI), 168–170
Costs
  of downtime, 32–33, 149–151
  expectations for reductions in, 28–29
  of IaaS, 65–66
  managing SLAs, 128
  of ownership, 57–58
  of prototyping, 2–3
  unexpected, 37–39
Criticality of services
  cost of downtime and, 150
  SLAs and, 128–129
CSPs (cloud service providers), 77, 78, 79–80. See also Vendors
Customer requirements/expectations identifying, 48–49
misunderstanding, 36–37
for security, 101–102
SLAs and, 127–129, 130
why, who, what, where, when, and how of, 41–43
Data
characteristics of, 87–92
encryption of, 90, 100, 112–113
government requests for, 100–101
store types for, 95–97
tenancy of system and characteristics of, 92–95
See also Security
Database as a Service (DBaaS)
products, 32
Data mining and analytics use cases, 68
Defining SLAs, 130–132
Delayed time performance, 89
Deployment models
AEA case study, 66–67
overview of, 18–21
PaaS, 105–107, 106
selecting, 69–70
Deployments
automating, 166–167
daily, 185
Designing cloud services
business architecture diagram, 43–45, 44
consumer experience, 49–51
data requirements, 98
for failure, 75–76
pragmatic approach, 45–47
problem statement, 47–48
project constraints, 51–52
state constraints, 52–54
user characteristics, 48
See also Customer requirements
Detection area of focus, 111, 144
DevOps
automating deployments, 166–167
automating infrastructure, 165–166
continuous integration and continuous delivery, 168–170
designing feature flags, 167
developing mind-set, 163–165
measuring, monitoring, and experimenting, 167–168
overview of, 163, 170
Directing logs to isolated storage areas, 120
Disaster recovery planning
cost of downtime, 149–151
hybrid clouds and, 160–161
for IaaS, 151–152
overview of, 149, 162
for PaaS, 157, 159
for primary data center, 152–154, 153, 155, 156, 157, 158
for SaaS, 159–160
Document store databases, 96
Domains to monitor, 139
Downtime, cost of, 149–151
Dynamic data sets, 89–90
Elastic cloud model, 173
Encryption of data, 90, 100, 112–113
Engine Yard, 17
Enterprise architecture, value of, 41
Enterprise clouds, 6
Enterprise management, complexity of, 4
Enterprise model, 172–173
Eucalyptus, 151–152, 160
Expectations, misguided, 27–29
Experimenting and DevOps, 167–168
Failure
designing for, 75–76
planning for, 31–33, 149
prevention of, 137–138
See also Disaster recovery planning; Outages
Fault tolerance with software, 72
Feature flags, 167–168
Fielding, Roy, 72–73
Files, storing data as, 96–97
Financial aspects of service models, 57–58
Force.com, 16, 62, 64
Fragile systems, 164
Functional requirements, 48–49
GitHub, 38
GoGrid, 15
Google
Apps Engine, 16, 31
Gmail, 10
as PaaS solution, 62
Government requests for data, 100–101
Graph databases, 96
Hammond, Paul, 163
HATEOAS, 73–74
Heroku, 17, 132
HIPAA (Health Insurance Portability and Accountability Act), 80
Horizontal scaling, 9, 24, 25, 26
Hosting solutions, 24
Human resources, impact of elastic cloud model on, 177–178
Hybrid clouds
disaster recovery planning with, 151–152, 160–161
overview of, 21, 184
IaaS. See Infrastructure as a Service
Implementing cloud initiatives, 39–40, 54
Infrastructure
automating, 165–166
provisioning, 185
Infrastructure as a Service (IaaS)
auditing cloud applications, 79
cloud stack, 104, 104–105
costs of, 38–39
described, 7
disaster recovery planning for, 151–152
logging strategies, 120–122
monitoring, 146
overview of, 14–15
regulations for, 82–83
selecting, 65–66
Infrastructure layer, performance at, 141
Innovation, resistance to, 5
Instagram, 8, 27, 31, 186
Internet
business operating model with, 172
level of complexity of systems and, 4
Inventory of actors and SLAs, 129
IT, impact of elastic cloud model on, 173–174
Key management and security, 113–114
Key performance indicators (KPIs), monitoring, 143
Layer 7 Technologies, 51
Legacy applications, porting to cloud, 3
Legacy systems, migrating to cloud, 74–75
Legal department, impact of elastic cloud model on, 176
Location of data, 88
Log files, uses of, 119–120
Logging
centralized strategy for, 119–125, 121
security and, 117–118
Loosely coupled architecture, 24
Machine images, standard set of, 166
Mainframe computers, 3, 4
Managing vendor SLAs, 132–135
Mashery, 51
Maturity of product and security, 102
M-Dot Network, 57, 65
Mergers and acquisitions, 186
Metrics to monitor, 138–139
Microsoft Azure, 16, 31, 62
Migrating
applications to cloud, 3, 23–24, 25, 26, 26–27
legacy systems to cloud, 74–75
Minimal viable product, 131–132
Mobile applications and PaaS, 187–188
Monitoring
DevOps and, 167–168
overview of, 137, 146–147
proactive compared to reactive, 137–138
requirements for, 138–139
security and, 118
strategies by category, 139–145
strategies by service level, 145–146
Multitenancy design strategies, 92, 92, 93, 93–94
National Institute of Standards and Technology (NIST)
IaaS definition, 14
PaaS definition, 16
encryption of, 90, 112
security of, 110
SLAs and, 128
Physical characteristics of data, 88
Platform as a Service (PaaS)
auditing cloud applications, 79
costs of, 38
described, 7
disaster recovery planning for, 157, 159
as game changer, 187–188
logging strategies, 122
monitoring and, 145–146
overview of, 15–17
regulations for, 82
security of, 105–108
selecting, 62–65
SLAs of, 132–133
See also Microsoft Azure
Policy enforcement and security, 111
Pragmatic approach for building services, 45–47
Prevention area of focus, 111
Primary data center, disaster recovery planning for
active-active hot, 157, 158
active-passive cold, 154, 155
active-passive warm, 154, 156
classic backup and restore method, 153, 153–154
overview of, 152–153
Private clouds, 17n, 20–21, 183–184
Private keys, 113–114
Private PaaS, 184
Private PaaS service providers, 63
Proactive monitoring, 137–138
Problem statement, 45, 47–48
Product components and SLAs, 129
Production environment and quality monitoring, 142–143
Project constraints, 51–52
Protection area of focus, 110, 144
Prototyping, comparison of costs of, 2–3
Public clouds, 17n, 18–20, 21
Public keys, 113–114
Public PaaS service providers, 63
Python, 31

Quality, monitoring, 142–143

Rackspace, 15, 152
Reactive monitoring, 137–138
Real-time performance, 88
Recovery point objective, 150
Recovery time objective, 150
Redundancy, cross-region and cross-
zone, 151

Regulations
auditing and, 80–83
compliance with, and SLAs, 134
data design decisions and, 90
list of, 81
monitoring compliance with, 144–145
USA Patriot Act, 100
U.S.-EU Safe Harbor, 102

Requirements. See Customer require-
ments/expectations
Resistance to change, 178, 180
RESTful (Representational State Trans-
er) services, 32, 71–74, 91
Retention period for data, 91–92
RFC 5424 Syslog protocol, 123, 123
Risk aspects of service models, 58
Risk tolerance and security, 102

SaaS. See Software as a Service
Sales, impact of elastic cloud model on,
176–177
Salesforce.com, 1, 59, 64, 82, 132
Scaling techniques, 9, 24, 25, 26
Security
areas of focus, 110–118
of AWS, 30, 105
cloud service providers and, 77, 78
maturation of, 7
misinformation about, 29–31
monitoring, 143–144
overview of, 78, 99–100, 118
requirements for, 101–103
service models and, 104–108
skills shortage and, 35–36
strategies for, 108–110
truth about, 100–101
of web, 114–115, 132
Security as a Service (SecaaS), 103
Self-service provisioning, 166
Sensitivity of data and security, 102
Service level agreement (SLA)
defining, 130–132
factors impacting, 127–130
managing, 132–135
monitoring, 138
overview of, 127
Service levels, monitoring, 145–146
Service models
overview of, 13, 14, 55
security requirements for, 104–108
selecting, 31, 56–59, 69–70
See also Infrastructure as a Service;
Platform as a Service; Software as a
Service
Session hijacking, 116
Single tenancy, 92, 92–93, 94
Skills shortage, 35–36
SLA. See Service level agreement
Snowden, Edward, 100–101
Software as a Service (SaaS)
auditing cloud applications, 79–80
cloud stack, 108
costs of, 38
described, 7
disaster recovery planning for,
159–160
logging strategies, 122
monitoring and, 145
overview of, 17–18
regulations for, 83
security of, 107
selecting, 59–62
SLAs and, 133–134
Software escrow, 159
Standardization strategy for security,
109–110
Standardizing log formats, 122–124
State constraints, 52–54
Stateful services, 26–27
Stateless services, 26–27, 32
Static data sets, 89
Storage use cases, 68
Strategic aspects of service models, 58
Systems thinking, 164. See also DevOps

Target industry and security, 101
Technical aspects of service models, 57
Tenancy of systems, 92, 92–95, 93
Test environment use cases, 69
Third-party software solutions and PaaS, 17
Throttling, 63–64
Throughput, monitoring, 141–142
Tightly coupled architecture, 24
Transaction boundaries, 91
Transmission boundaries and security, 102
Tumbler, 186

USA Patriot Act of 2001, 50, 110, 113
User characteristics, 48
User layer
performance at, 140
security and, 107
U.S.-EU Safe Harbor regulations, 102

Value of recovery, and cost of downtime, 150
Vendors
cloud migration services of, 75
leveraging multiple public, 152
lock-in, 32, 33
managing SLAs, 132–135
PaaS, 63
SaaS, 60
security requirements for, 99
selecting, 31
shutdown of, 32, 160
See also Cloud service providers; Outages
Vertical scaling, 24
Volatility of data, 89–90
Volume of data, 90
Web security, 114–115, 132
Workday, 186–187
Worst practices
migrating applications to cloud,
23–24, 25, 26, 26–27
misguided expectations,
27–29
misunderstanding customer requirements, 36–37
outages and out of business scenarios, 31–33
overview of, 23
security misinformation, 29–31
selecting vendors, 31
skills shortage, 35–36
underestimating impacts of change,
33–34
unexpected costs, 37–39