

# Index

- Abstraction, 3, 9, 101, 113, 114
- Abuse of cloud computing, 38, 39, 148, 152, 154
- Access control, 12, 17, 18, 24–26, 39, 41, 82–88, 93, 94, 108, 109, 135, 163, 168, 169, 173
- Accounting criteria and controls, 109
- Agile innovation, 163
- Amazon, 5, 93, 164
- American Recovery and Reinvestment Act (2009), 146
- Anti-malware scanning, 163
- Application as a Service. *See* SaaS (Software as a Service)
- Application programming interface (API), 22, 39, 152, 166
- Application servers, 5
- Application service providers, 80–82, 87, 88
- Atomic security continuum
  - elements, 111–114, 122–124
- Atomicity, principle of, 111, 121
- Attestation of controls, 66, 69, 77
- Audit logs, 11, 16, 38, 39, 84, 85, 104, 138
- Audit trail, 171, 173
- Auditability, 45, 102, 103, 105, 106, 115–117, 125, 143, 169, 172
- Auditors
  - audit process, 16–18
  - business continuity and disaster recovery audit questions, 138, 139
  - challenges, 30
  - control frameworks, use of, 18–20
  - external, 69, 70, 72
  - independent, 69, 166
  - role of in business continuity and disaster recovery planning, 133–135
- Audits
  - about, 16–18, 29, 30
  - audit trail, 171, 173
  - automated, 22
  - cloud architecture and traditional systems infrastructure differences, 17, 18
  - control frameworks, 16, 18–22
  - controls recommended, 22–26
  - data access, 162, 163, 173 and data storage, 172–174 and deployment model, 18
  - hypervisors, 167

- Audits (*Continued*)
- regulatory compliance, 143, 145, 148–150, 152, 154–156, 162
  - reports, 18, 72, 172. *See also* SSAE
    - 16 (Type II) audits
  - right to audit, 23, 70, 72, 138
  - risk assessment, 26–29
  - risk management, 26, 27
  - scope of audit, 16, 17
  - and service model, 18
  - standards, 124
  - virtual machines, 167
- Authentication, 17, 23–25, 38–40, 71, 87, 108, 135, 166
- Authenticity, 103, 108
- Authorization, 16, 18, 25, 30, 39, 108, 163
- Autonomic response, 3
- Availability issues, 8, 10, 28, 29, 38, 39, 65, 104, 108
- Backups, 23, 75, 117, 133–138
- Bechtel Corporation, 92
- Benchmarks, security, 144, 145, 149–152
- Best practices. *See also* Regulatory compliance, Standards
  - audits, 16
  - COSO framework, 149. *See also* COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  - security benchmarks, 144, 145, 149–152
  - and security design, 38, 111, 144, 165
- Blobs, 170
- Botnets, 17, 39
- BPaaS (Business Process as a Service), 101
- Brokers, 7
- BS 25999 (British Standards Institute), 137
- Business continuity. *See also* Disaster recovery
  - availability issues, 10
  - and cloud deployment model, 59
  - and data level security, 172
  - planning. *See* Business Continuity Planning (BCP)
- Business Continuity Planning (BCP)
  - auditor's role, 133–135
  - planning process, 131, 132
  - problem statement, 130, 131
  - purpose of, 130
  - senior executive support, 130, 131
  - team, 130, 131
- Business impact analysis, 131, 132
- Business Process as a Service (BPaaS), 101
- Business processes
  - and Business Continuity Planning, 130–133. *See also* Business Continuity Planning (BCP)
  - change, 80
  - cloud solutions, 101
  - and IT governance, 46, 80, 84
  - morphing, 162
  - and SOX compliance, 162
- CCSK (Certificate of Cloud Security Knowledge), 166
- Center for Internet Security (CIS), 144, 147
- Certificate of Cloud Security Knowledge (CCSK), 166
- Certifications

- business continuity, 137
- CSA Certificate of Cloud Security Knowledge (CCSK), 166
- CSA Trusted Cloud Initiative, 165
- FedRAMP program, 20
- FISMA, 20, 146
- international issues, 150
- ISO 27001/27002, 70, 90
- multi-tenant environments, 90
- standards, 70
- trust certification, 45
- and verification of controls, 69, 74
- Challenges of cloud computing, 9–13, 164
- Change control, 23, 64
- Change management, 47
- Chekov, Anton, 118
- Chief information officer (CIO), 34, 35, 46
- CIAAAAA (Confidentiality, Integrity, Availability, Authentication, Authorization, Accounting, and Audit), 123
- CIS (Center for Internet Security), 144, 147
- Client-server architecture (C/SA), 36
- Clobs, 170
- Cloud architecture, 17, 18
- Cloud characteristics, 98, 101–109, 113–117
- Cloud computing, overview
  - and agile innovation, 163
  - benefits of, 1, 13, 15, 52, 164
  - challenges, 9–13, 164
  - cloud characteristics, 98, 101–109, 113–117
  - continuity issues, 136, 137
  - defined, 2, 3, 100
  - deployment models, 8, 9, 37, 101
  - described, 34, 36, 37
  - history, 1, 2, 164
  - migration to, 80
  - providers. *See* Providers
  - roles of consumer, provider, and integrator, 6, 7
  - service layers, 4–6, 36, 37, 101.
    - See also* BPaaS (Business Process as a Service); IaaS (Infrastructure as a Service); PaaS (Platform as a Service); SaaS (Software as a Service)
  - top threats to cloud computing, 38–41, 152
  - as a utility, 164, 165
- “Cloud Computing Management Audit Assurance Program” (ISACA), 21
- “Cloud Computing Risk Assessment” (ENISA), 20
- Cloud morphing, 162, 166–168, 170
- Cloud Security Alliance (CSA)
  - about, 19, 30, 158, 163–166
  - Certificate of Cloud Security Knowledge (CCSK), 166
  - chapter organizations, 166
  - CloudAudit initiative (2010) (A6 group), 22, 164, 166
  - Consensus Assessments Initiative, 165
  - Controls Matrix, 66, 67, 137, 165, 166
  - formation of, 161, 165
  - and regulatory compliance, 152, 153, 158
  - Security Guidance for Critical Areas of Focus in Cloud Computing, 21, 165

- Cloud Security Alliance (*Continued*)
  - top threats to cloud computing, 38–41, 152
  - Trusted Cloud Initiative (TCI), 165, 166
- Cloud Security Continuum, 110–112
- Cloud storage, 169–171. *See also*
  - Data storage
- CloudAudit initiative (2010) (A6 group), 22, 164, 166
- COBIT (Control Objectives for Information and related Technology), 16, 19, 21, 48, 62, 64–66, 145, 146
- Code, custom, 29, 89
- Code base, 88, 90, 92, 93
- Collaboration Oriented Architecture (COA), 103, 109, 124
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 21, 145, 146, 148, 149
- Communications controls, 18, 40, 41
- Community clouds, 8, 18, 37, 101
- Complexity and risk, 17, 28, 35, 67, 73, 74, 79, 80, 94, 149
- Compliance. *See also* Regulatory compliance
  - auditing, 16–18, 107
  - control environment, 67, 68
  - control frameworks, 19–22, 30, 68
  - controls, 22–26, 69
  - governance, 43, 44, 46, 47, 51, 67
  - by inclusion, 77
  - multi-tenant environments, 11
  - organizations developing guidance for, 19
  - protection and privacy of information, 119–122
  - risk management, 27
  - service level agreements, 40, 44
  - service policies, 107
  - standards, 20, 30, 70
- Confidentiality, 12, 29, 45, 103, 104, 108, 116, 117, 123–125
- Connection points, 68, 69, 71, 72, 80
- Consensus Assessments Initiative, 165
- Consumer, defined, 6
- Control attestations, 66, 69, 77
- Control environment
  - compliance, 67, 68
  - CSA Controls Matrix, 66, 67, 137, 165, 166
  - effectiveness, validating, 67–74
  - providers, 69, 73–75
- Control frameworks
  - and audit process, 16, 18–22
  - Cloud Security Alliance (CSA), 21. *See also* Cloud Security Alliance (CSA)
  - CloudAudit/A6, 22
  - COBIT, 16, 19, 21, 48, 62, 64–66, 145, 146
  - compliance, 19–22, 30, 68
  - COSO framework, 149. *See also* COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  - ENISA, 20. *See also* ENISA (European Network and Information Security Agency)
  - FedRAMP, 20, 21
  - ISO 27001, 19

- ITIL, 19. *See also* ITIL (Information Technology Infrastructure Library)
- NIST, 16, 19. *See also* NIST (U.S. National Institute of Standards and Technology)
- regulatory compliance, 144, 145, 148–154, 156–158
- vendors, compliance program support, 19
- Control Objectives for Information and related Technology). *See* COBIT (Control Objectives for Information and related Technology)
- Controls
  - attestations, 66, 69, 77
  - control environment. *See* Control environment
  - CSA Controls Matrix, 66, 67. *See also* Cloud Security Alliance (CSA)
  - evaluating importance of, 62
  - frameworks. *See* Control frameworks
  - lifecycle methodologies, 62–67
  - recommended, 22–26
  - testing, 68, 69
- Controls Matrix (CSA), 66, 67, 137, 165, 166
- Corporate Governance Task Force, 43
- COSO (Committee of Sponsoring Organizations of the Treadway Commission), 21, 145, 146, 148, 149
- Costs
  - considerations, 16
  - cost/benefit analysis, 52
  - and Moore’s Law, 164
  - private clouds, 8
  - and regulatory compliance, 143, 144
  - single-tenant offsite operations, 81
- Credit card fraud, 39
- Criminal penalties, 154
- Cross-cloud deployments, 73, 74
- Cryptographic keys, 73, 134, 168, 172. *See also* Encryption
- CSA. *See* Cloud Security Alliance (CSA)
- Custom applications, 17, 88, 89
- Cyber crime, 37, 147, 150, 151. *See also* Security
- Data
  - assurance, 45
  - attributes and database classes, 171
  - encryption. *See* Encryption
  - logging of interactions, 84
  - in multi-tenant systems, 84
  - partitioned, 82
  - privacy. *See* Privacy and protection policies
- Data access, 168, 169. *See also* Access control
- Data at rest, 17, 25, 98, 108, 110, 115, 119, 123, 162, 169
- Data breaches, 17, 18, 65, 100, 150, 168, 169
- Data centers, 10, 18, 28, 75, 76, 133–135, 163, 172
- Data classification, 23, 106, 119, 120, 124
- Data evacuation, 12

- Data in flight (in transit), 17, 25, 98, 108, 110, 115, 117, 119, 123, 124
- Data location, 9–11, 29, 90, 91, 107, 119, 168, 173
- Data loss/leakage, 38, 40, 75, 136, 152
- Data privacy, 118, 119. *See also* Privacy laws; Protection and privacy of information assets
- Data processing, 147, 148, 162–163, 169
- Data protection, legal agreements, 29
- Data residency. *See* Data location
- Data storage, 12, 35–36, 40, 44, 68–75, 136, 147, 169–174. *See also* Media storage
- Database management, 162, 163, 169–171
- DB2 database, 5
- Defense Information Security Agency (DISA), 144, 147
- Demand, unpredictability of, 3, 102, 105
- Demand and Capacity Management, 64
- Deployment models
  - community cloud, 8, 18, 37, 101
  - described, 8, 9, 37
  - hybrid cloud, 9, 18, 101
  - private cloud. *See* Private clouds
  - public cloud, 9, 18, 37, 101
- DISA (Defense Information Security Agency), 144, 147
- Disaster recovery
  - and cloud deployment model, 59
  - and data level security, 172
  - planning. *See* Disaster Recovery Planning (DRP)
- Disaster Recovery Planning (DRP)
  - audit questions, 138, 139
  - auditor's role, 133–135
  - cloud computing continuity issues, 136, 137
  - cloud services, use of, 135, 136
  - phases of, 132, 133
  - problem statement, 130, 131
  - senior executive support, 130
  - team, 130
  - traditional strategies for IT recovery, 133, 135
- DMTF, 2
- Due diligence, 9, 41, 75, 98, 99
- E-mail. *See* Electronic mail systems
- EC2 IaaS (Amazon), 5, 116
- Economies of scale, 3, 9, 10, 80, 164
- ECPA (Electronic Communications Privacy Act), 147
- Education, privacy issues, 120, 121
- Elasticity, 2, 3, 10, 63, 101, 102, 104, 105
- Electronic Communications Privacy Act (ECPA), 147
- Electronic mail systems, 15, 91, 92, 120, 147, 163
- Electronic Patient Health Information (ePHI), 86
- Electronic Transactions Act (Cap. 88) (Singapore), 148
- Elements, atomic security
  - continuum, 111–114, 122–124
- Encryption, 12, 17, 25, 39, 40, 69, 71–73, 90, 124, 134, 153, 166, 168, 169, 171–173
- ENISA (European Network and Information Security Agency), 19, 20, 28, 150, 158

- ePHI (Electronic Patient Health Information), 86
- EPIC, 120
- European Network and Information Security Agency (ENISA), 19, 20, 28, 150, 158
- European Union (EU)
  - Data Protection Directive, 120, 148, 153
  - Privacy Directive, 157
  - privacy laws, 10, 11, 148, 153, 154
  - safe harbor programs, 120, 125, 153
- Everything as a Service, 36. *See also* IaaS (Infrastructure as a Service)
- Export laws, 154, 155, 157
- Fail fast (agile innovation), 163
- Failure points, 10, 17, 91, 92, 94, 109
- FAIR, 120
- Family Educational Rights and Privacy Act (FERPA), 120
- Family Policy Compliance Office (FPCO), 120
- Federal Information Protection Standards (FIPS), 120, 145
- Federal Information Security Management Act (FISMA), 19–21, 23, 26, 146, 153, 154
- Federated access, 109
- Fees, 106
- FERPA (Family Educational Rights and Privacy Act), 120
- Financial Management, 64
- FIPS (Federal Information Protection Standards), 120, 145
- Firewalls, 11, 17, 87, 91, 134, 167, 168, 171
- FISMA (Federal Information Security Management Act), 19–21, 23, 26, 146, 153, 154
- Frameworks
  - control frameworks. *See* Control frameworks
  - NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, 65, 66
  - regulatory compliance, 144, 145, 148–154, 156–158
- Gall, John, 86
- GLBA (Gramm/Leach/Bliley Act), 147, 152
- Global regulation. *See* International laws and regulations; Regulatory compliance
- Google, 2, 6, 93, 100, 116
- Governance
  - corporate, 41, 47
  - Information Technology (IT). *See* IT governance
- Governance in risk and control (GRC), 44
- Governmental controls, 23
- Graham/Leach/Bliley Act (GLBA), 147, 152
- Granular privilege assignment, 82–84. *See also* Access control
- Guidelines
  - NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, 65, 66
  - OECD guidelines, 120

- Guidelines (*Continued*)
  - protection and privacy of
    - information assets, 121–124
  - Security Hardening Guidelines, 145
  - Security Technical Information Guides (STIG), 144
  - STIG (Security Technical Information Guides), 144
- Hacking and hackers, 17, 38, 39, 45
- Health Insurance Portability and Accountability Act (HIPAA), 11, 84–86, 121, 146, 147, 152, 153
- Hijacking, 40, 152
- HIPAA (Health Insurance Portability and Accountability Act), 11, 84–86, 121, 146, 147, 152, 153
- HITRUST CSF, 66
- Host intrusion detection systems (HIDS), 11
- Hot sites, 133, 135, 136
- Hybrid clouds
  - about, 9, 101
  - audit process, 18. *See also* Audits
- Hypervisors, 11, 39, 167
- IaaS (Infrastructure as a Service)
  - about, 5, 36, 37
  - Amazon EC2, 5
  - as cloud computing service, 4
  - and disaster recovery, 135–137
  - integration of providers, 7
  - providers, 5
  - security issues, 38, 41
- Identity management, 17, 19, 25, 109, 166, 169. *See also* Access control; Authentication
- Implementation methodology for IT governance
  - about, 46
  - adoption of, 48, 49
  - application to cloud computing, 49–52
  - preliminary steps, 46–48
- Implementing and Continually Improving IT Governance (ISACA), 48, 49
- In Search of Excellence (Peters and Waterman), 52, 53
- Incident management and response, 25, 26, 45, 85, 150, 168, 173, 174
- Information asset lifecycle
  - management (ILM), 114, 118
- Information Security Governance (InfoSec), 41, 43, 44, 46–52
- Information Security Management Systems Requirements (ISO/IEC 27001), 21, 66, 70, 90, 145
- Information Services (IS), 8
- Information Technology (IT)
  - governance. *See* IT governance
  - as private cloud provider, 8
- Information Technology
  - Infrastructure Library (ITIL), 19, 62–64
- InfoSec (Information Security Governance), 41, 43, 44, 46–52
- Infrastructure as a Service (IaaS). *See* IaaS (Infrastructure as a Service)
- Insiders, malicious, 39, 152
- Integrator, 7
- Integrity, 108, 124

- Intellectual property
  - legal agreements, 29
- International issues, 107
- International laws and regulations
  - export law, 154, 155
  - regulatory compliance, 148, 150, 152–158, 168
- Intrusion management, 167, 168
- ISACA (Information Systems Audit and Control Association), 19, 21, 30, 47–50, 64, 66, 158
- ISMS (Information Security Management Systems), 21, 66, 70, 90, 145
- ISO 27001 Information Security Management Systems (ISMS), 21, 66, 70, 90, 145
- ISO/IEC 27001:2005, 145
- Isolated-tenant application services (application service providers), 81, 82
- IT governance
  - about, 41–43
  - board, 46, 47
  - and cloud computing. *See* Cloud computing, overview
  - defined, 42
  - implementation, 46–52
  - Information Security Governance (InfoSec), 41, 43, 44, 46–52
  - need for, 34, 35
  - policy, 42
  - risk and control, 44
  - and risk management, 52, 53
  - and security issues, 35
  - service agreement management, 44–46
  - service-oriented architecture (SOA) approach, 42
- ITIL (Information Technology Infrastructure Library), 19, 62–64
- Japan, 148
- Java Runtime Environment (JRE), 5
- Jericho Forum, 109, 111, 118
- JSOX, 148
- Key success factors (critical success factors), IT and InfoSec governance, 47, 48
- Kumar, Nikhil, 110
- Legacy models, 80, 82, 86, 87, 94
- Legal agreements
  - risk assessment, 28, 29
  - service contracts, 45
  - service level agreements. *See* Service level agreements (SLAs)
- Lewis, Mark, 37
- Licensing issues, 5, 81, 134, 151, 154, 168
- Lifecycle management
  - control environment, verifying effectiveness of, 67–74
  - control methodologies, 62–67
  - controls, evaluating importance of, 62
  - cross-cloud deployments, 73, 74
  - handoff, 57, 59
  - IaaS responsibilities, 58, 59, 67, 73, 74
  - information asset lifecycle management, 114, 118
  - onion model, 61, 62
  - PaaS responsibilities, 58, 59, 73, 74

- Lifecycle management (*Continued*)
- policy and process conflicts,
    - dealing with, 60, 61
  - provider's perspective, 74, 75
  - questionnaires for providers, use of, 75, 76
  - responsibilities of provider versus customer, 58, 59
  - risk tolerance, 72, 73
  - SaaS responsibilities, 58, 59, 64, 67, 73, 74
  - stages of lifecycle, 62
  - and tradeoffs, 57–59
- Location independence, 101, 103, 107, 116, 117, 119–120, 122
- Location of data, 9–11, 29, 90, 91, 107, 119, 168, 173
- Lost business, restitution for, 45
- Managed service providers (single-tenant offsite operations), 81
- Managed shared service, 105
- McCarthy, John, 1, 2
- Media storage, 132–135. *See also* Data storage
- Medical records, 86, 109. *See also* Personal health information (PHI)
- Metadata-based design, 88–90, 92, 93
- Metadata links, 87
- Microsoft
  - operating systems, 89
  - Windows Azure platform, 5
- Middleware, 4, 5
- Migration to cloud, 10, 51, 80
- Monetary Authority of Singapore, 148
- Monitoring
  - for abuse, 39
  - and audit trails, 173
  - communications, 18, 153
  - controls, 21, 69, 144, 155
  - performance, 11, 12, 59, 63
  - policy monitoring points (PMPs), 111
  - service policies, 106, 107
  - use, 106, 168, 169
- Moore, Gordon E., 2
- Moore's Law, 2, 164
- Morphing, 162, 166–168, 170, 173, 174
- Multi-tenancy
  - challenges, 11
  - and cloud computing, 3–5, 153, 164, 167
  - data location, 90, 91
  - perimeter security, 171, 172
  - privacy and data protection issues, 107, 120
  - service delivery and support, 82–94
  - trust concerns, 91–93
  - and virtual security, 167, 168
- Mundie, Craig, 92
- National Electric Reliability Council (NERC), 145
- National Fire Protection Association (NFPA), 137
- National Institute of Standards and Technology (NIST). *See* NIST (U. S. National Institute of Standards and Technology)
- National Security Agency (NSA), 145
- Nefarious use, 10, 38, 39, 152

- NERC (National Electric Reliability Council), 145
- Network access, 102, 104
- NFPA 1600 (National Fire Protection Association), 137
- NIST (U.S. National Institute of Standards and Technology)
  - characteristics of cloud solutions, 101–103
  - cloud computing definition, 100
  - control frameworks, 16, 30
  - guidance, 19
  - NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, 65, 66
  - NIST 800-53 (rev.3), 20
  - and regulatory compliance, 145, 146, 148, 152, 153, 158
- Non-repudiation, 108, 124
- NSA (National Security Agency), 145
  
- OASIS, 2
- Object-oriented database
  - management, 170, 171, 173
- OECD guidelines, 120
- Off-the-shelf software, 88, 165, 172
- Offsite media storage, 75, 132–135
- On-demand self-service, 102, 104
- Open Group, 2, 101, 124
- Operating systems, 3–5, 34, 36, 37, 39, 41, 59, 67, 76, 89, 134, 167, 168
- Outages, 10, 45, 65, 131, 133, 136–138
- Outsourcing
  - to cloud, 15, 18, 34, 37, 65, 91, 151, 161, 162, 164
  - cloud computing contrasted, 80, 161, 162
  - by cloud provider, 29
  - compliance, 67, 77, 151
  - and core competencies, 53
  - legal agreements, 29
  - as risk management, 65
  - security issues, 37. *See also* Security
- PaaS (Platform as a Service)
  - about, 5, 36
  - as cloud computing service, 4
  - and disaster recovery, 137
  - as provider, 6
  - security issues, 38, 41, 171, 172
  - Windows Azure, 5
- Passwords, 25, 38, 39, 41, 83
- Patch management
  - auditing, 24
  - cloud servers, 17
  - provider services, 76
  - responsibility for, 67
  - and virtualization, 92
- Payment Card Industry (PCI), 19, 66, 136, 145, 148, 149, 151, 152, 154, 157
- PCI. *See* Payment Card Industry (PCI)
- Performance levels, 11, 12, 59, 63, 65. *See also* Service level agreements (SLAs)
- Perimeter security, 171, 172
- Personal health information (PHI), 11, 120
- Personally identifiable information (PII), 11, 106, 120, 125
- Peters, Tom, 52
- Physical security, 19, 26, 39, 51, 134, 163

## 202 ■ Index

- Platform as a Service (PaaS). *See* PaaS (Platform as a Service)
- Policies, conflicts between provider and customer, 60, 61
- Policy enforcement points (PEPs), 111
- Privacy and protection policies, 107, 109, 111. *See also* Protection and privacy of information assets
- Privacy laws, 120, 121, 125, 147, 148, 150, 152–154, 156, 157, 168
- Private clouds
  - about, 8, 37, 101
  - audit process, 18. *See also* Audits
  - availability issues, 10
  - multi-tenancy, 3
- Professional negligence, 29
- Protection and privacy of information
  - assets
  - about, 97–99, 124, 125
  - access control. *See* Access control
  - and cloud characteristics 104–109, 113–117
  - Cloud Security Continuum (security reference model), 110–112
  - cloud solutions described, 100–104
  - compliance issues, 119–121
  - consumer perspective, 99
  - data classification, 119
  - data privacy, 118, 119, 168
  - encryption. *See* Encryption
  - guidelines for (playbook), 121–124
  - information asset lifecycle management, 114, 118
  - perspectives on, 99, 100
  - regulatory issues, 119–121
- Providers
  - application service providers (isolated-tenant application services), 81, 82
  - cloud computing, 6, 7
  - customer concerns, addressing, 91–93
  - Information Systems (IS) department, 8
  - Information Technology (IT) department, 8
  - managed service (single-tenant offsite operations), 81
  - and policy conflicts, 60, 61
  - privacy issues, perspective on, 99, 100
  - questionnaires on security practices, 75, 76
  - risk management and security practices, 40, 41
  - visibility and transparency, 93
- Public clouds
  - about, 9, 37, 101
  - audit process, 18. *See also* Audits
- Public Company Accounting Oversight Board (PCAOB), 148, 149
- Quality of service (QoS)
  - challenges, 9–13
  - community clouds, 8
  - and demand servicing, 105
  - hybrid clouds, 9
  - and integrity, 108
  - and PaaS, 5
  - payment based on, 106
  - policy enforcement points (PEPs), 111

- privacy and protection policies, 111, 112
- private clouds, 8
- public clouds, 9
- and SaaS, 6
- scalability, 105
- service-based cloud solutions, 104
  
- Rackspace, 10
- Ramleth, Geir, 92
- Recovery Point Objective (RPO), 132, 137
- Recovery Time Objective (RTO), 132, 135, 137
- Regulatory compliance
  - about, 143–145, 156–158
  - auditing, 143, 145, 148–150, 152, 154–156
  - and best practices, 144, 145, 147, 149–152, 158
  - and Cloud Security Alliance (CSA) 152, 153, 158. *See also* Cloud Security Alliance (CSA)
  - criminal liability, 154
  - early adoption measures, 150, 151
  - export laws, 154, 155, 157
  - frameworks, 144, 145, 148–154, 156–158
  - international laws and regulations, 148, 150, 152–158
  - issues with, 10, 11, 149–151
  - need for regulations, 148, 149
  - and NIST, 152, 153, 158. *See also* NIST (U.S. National Institute of Standards and Technology)
  - privacy laws, 147, 148, 150, 152–154, 156, 157
  - regulatory programs, evolution of, 151, 152
  - and risk assessments, 147, 150, 155, 158
  - and risk identification, 156, 157
  - risk mitigation, 144, 150, 155–157
  - security benchmarks, 144, 145, 149–152
  - standards, 144–146, 149–154, 156–158
  - U.S. laws and regulations, 146, 147, 152, 153
- Resource management, 64, 65
- Resource pooling, 101, 102, 105
- Right to audit, 23, 70, 72, 138
- Risk and complexity, 17, 28, 35, 67, 73, 74, 79–80, 94, 149
- Risk assessment
  - Business Continuity Planning, 131
  - controls, 26–29
  - and regulatory compliance, 147, 150, 155, 158
- Risk identification, 94, 131, 156, 157
- Risk management
  - and cloud computing, 80, 94
  - controls, 26, 27
  - and governance, 52, 53
  - outsourcing to provider, 65
  - tradeoffs, 57–59
- Risk mitigation, 27–29, 40, 62, 68, 111, 125, 130, 131, 144, 150, 155–157
- Risk tolerance, 68, 72, 73
- Rollback, 102, 106
- Rumsfeld, Donald, 91
- Runtime environments, 5

- SaaS (Software as a Service)
  - about, 6, 36
  - as cloud computing service, 4
  - and disaster recovery, 137
  - Google Apps, 6
  - and integration of services, 7
  - as provider, 6, 7
  - Salesforce.com, 6, 83, 85, 93
  - security issues, 41, 171, 172
  - and service layers, 3
- Safe harbor provisions, 120, 125, 153
- Saint-Exupéry, Antoine de, 79
- Salesforce.com, 6, 83, 85, 93
- Sarbanes-Oxley Act (SOX), 19, 21, 145, 146, 148, 149, 151, 153, 154, 157, 162
- SAS 70, 19, 66, 69–72, 90, 155
- Scalability, 63, 102, 105, 166, 169
- Schmelzer, R., 38
- Schmidt, Howard, 37, 38
- Security
  - auditability of, 45
  - benchmarks, 144, 145, 149–152
  - CSA Controls Matrix, 137. *See also* Controls Matrix (CSA)
  - data evacuation, 12
  - frameworks, 145. *See also* Regulatory compliance
  - Infrastructure as a Service (IaaS), 41
  - issues with, generally, 15, 16, 37–41, 165
  - and legacy models, 79, 80
  - multi-tenancy models, 11, 82–90, 171, 172
  - perimeters, 171, 172
  - physical access, 39
  - Platform as a Service (PaaS), 41
  - protection and privacy. *See* Protection and privacy of information assets
  - public clouds, 9
  - Software as a Service (SaaS), 41
  - virtual security, 167, 168
- Security Guidance for Critical Areas of Focus in Cloud Computing, 21, 165
- Security Hardening Guidelines, 145
- Security reference model (Cloud Security Continuum), 110–112
- Security Technical Information Guides (STIG), 144
- Self-service, on-demand, 102, 104
- Sensitive information, 12, 13, 23, 60, 69, 84, 91, 106, 153, 168. *See also* Protection and privacy of information assets
- Servers, 6, 10, 17, 19, 34, 36, 45, 77, 86, 92, 100, 144, 147, 154, 163, 164, 168, 172
- Service-based aspect of cloud solutions, 102, 104
- Service delivery and support
  - isolated-tenant application services (application service providers), 81, 82
  - and legacy models, 79, 80
  - migration contrasted, 80
  - multitenant applications and platforms, 82–94
  - and risk, 79, 80, 93, 94
  - single-tenant offsite operations (managed service providers), 81
  - and transformation of technology stack, 80
- Service layers
  - about, 4–6

- and abstraction, 3
- categories of cloud computing
  - services, 4, 36. *See also* BPaaS (Business Process as a Service); IaaS (Infrastructure as a Service); PaaS (Platform as a Service); SaaS (Software as a Service)
- traditional versus cloud model, 4
- Service level agreements (SLAs)
  - and control methodologies, 62, 63
  - described, 45
  - and elasticity of cloud services, 105
  - failure to meet performance levels, recourse for, 11, 12
  - management, 44, 45
  - physical security, 39
  - provisions of, 45
  - public clouds, 9
  - and risk management, 27
  - security standards, 44
  - testing, 156
- Service Level Management, 64
- Service models
  - BPaaS (Business Process as a Service), 101
  - Infrastructure as a Service. *See* IaaS (Infrastructure as a Service)
  - Platform as a Service. *See* PaaS (Platform as a Service)
  - Software as a Service. *See* SaaS (Software as a Service)
- Service-oriented architecture (SOA), 42, 66, 100, 101, 110, 164
- Service Portfolio Management, 63
- Service reliability, 63
- Service termination, 106
- Service Validation and Testing, 64
- Shared technology, 39, 40, 152
- Short, 118
- Singapore, 148
- Single-tenant offsite operations (managed service providers), 81
- SNIA, 118
- Software as a Service (SaaS). *See* SaaS (Software as a Service)
- Software stack, 5
- SOX (Sarbanes-Oxley Act), 19, 21, 145–146, 148, 149, 151, 153, 154, 157, 162
- SSAE 16 (Type II) audits, 19, 66, 69–72, 90, 155
- SSL, 41, 68
- SSL/TLS, 68
- Stakeholders, identifying, 46
- Standard of due care, 44
- Standards. *See also* NIST (U.S. National Institute of Standards and Technology)
  - audits, 124
  - BS 25999 (British Standards Institute), 137
  - certifications, 70. *See also* Certifications; ISO 27001 Information Security Management Systems (ISMS)
  - development of, 2
  - FIPS (Federal Information Protection Standards), 145
  - lack of, 34
  - NFPA 1600 (National Fire Protection Association), 137
  - privacy, 120
  - and regulatory compliance, 144–146, 149–154, 156–158
  - service level agreement security standards, 44

- Standards for Attestation
  - Engagements (SSAE) 16. *See* SSAE 16 (Type II) audits
- State laws, 147
- Statement on Auditing Standards (SAS) 70. *See* SAS 70
- STIG (Security Technical Information Guides), 144
- Student information, 120, 121
- Supervisory access by cloud provider, 12
- Systems administrators, 42, 76, 87
- SysTrust, 90
  
- Termination of service, 106
- Terrorism, 153
- Testing
  - audit considerations, 17, 18, 63, 156
  - business continuity plan and disaster recovery, 132–135, 137, 138
  - controls, 68–70
  - custom applications, 17, 89
  - service level agreements, 156
- Tokens, 39, 90, 91
- Top threats to cloud computing, 38–41, 152
- Traffic Light Protocol (TLP), 120, 125
- Training, business continuity, 130, 132
  
- Trust certification, 45
- Trusted Cloud Initiative (TCI), 165, 166
  
- United Kingdom (UK), 148
- United Nations, declaration of Human Rights, 120
- Unknown risk profile, 38, 40, 41, 152
- Upgrades, 80, 89, 92, 93
- U.S. laws and regulations. *See also* specific laws
  - regulatory compliance, 146, 147, 152, 153
  - safe harbor provisions, 120, 125, 153
- U.S. National Institute of Standards and Technology (NIST). *See* NIST (U.S. National Institute of Standards and Technology)
- “Vector Theory of Systems” (Gall), 86
- Vendors, cloud computing. *See* Providers
- Virtual private networks, 82
- Virtualization, 3, 10, 19, 44, 81, 92, 151, 164, 167, 168
- VMware, 151
  
- Waterman, Bob, 52
- Web Services (Amazon), 93
- Williams, Paul, 33

<http://www.pbookshop.com>

<http://www.pbookshop.com>