

Contents

Preface	xiii
Chapter 1: Introduction to Cloud Computing	1
History	1
Defining Cloud Computing	2
<i>Elasticity</i>	2
<i>Multitenancy</i>	3
<i>Economics</i>	3
<i>Abstraction</i>	3
Cloud Computing Services Layers	4
<i>Infrastructure as a Service</i>	5
<i>Platform as a Service</i>	5
<i>Software as a Service</i>	6
Roles in Cloud Computing	6
<i>Consumer</i>	6
<i>Provider</i>	6
<i>Integrator</i>	7
Cloud Computing Deployment Models	8
<i>Private</i>	8
<i>Community</i>	8
<i>Public</i>	9
<i>Hybrid</i>	9
Challenges	9
<i>Availability</i>	10
<i>Data Residency</i>	10
<i>Multitenancy</i>	11
<i>Performance</i>	11
<i>Data Evacuation</i>	12
<i>Supervisory Access</i>	12
In Summary	13

Chapter 2: Cloud-Based IT Audit Process	15
The Audit Process	16
Control Frameworks for the Cloud	18
<i>ENISA Cloud Risk Assessment</i>	20
<i>FedRAMP</i>	20
<i>Entities Using COBIT</i>	21
<i>CSA Guidance</i>	21
<i>CloudAudit/A6—The Automated Audit, Assertion, Assessment, and Assurance API</i>	22
Recommended Controls	22
Risk Management and Risk Assessment	26
<i>Risk Management</i>	27
<i>Risk Assessment</i>	27
<i>Legal</i>	28
In Summary	29
Chapter 3: Cloud-Based IT Governance	33
Governance in the Cloud	36
<i>Understanding the Cloud</i>	36
<i>Security Issues in the Cloud</i>	37
<i>Abuse and Nefarious Use of Cloud Computing</i>	38
<i>Insecure Application Programming Interfaces</i>	39
<i>Malicious Insiders</i>	39
<i>Shared Technology Vulnerabilities</i>	39
<i>Data Loss/Leakage</i>	40
<i>Account, Service, and Traffic Hijacking</i>	40
<i>Unknown Risk Profile</i>	40
<i>Other Security Issues in the Cloud</i>	41
Governance	41
<i>IT Governance in the Cloud</i>	44
<i>Managing Service Agreements</i>	44
Implementing and Maintaining Governance for Cloud Computing	46
<i>Implementing Governance as a New Concept</i>	46
<i>Preliminary Tasks</i>	46
<i>Adopt a Governance Implementation Methodology</i>	48
<i>Extending IT Governance to the Cloud</i>	49
In Summary	52

Chapter 4: System and Infrastructure Lifecycle Management for the Cloud	57
Every Decision Involves Making a Tradeoff	57
<i>Example: Business Continuity/Disaster Recovery</i>	59
What about Policy and Process Collisions?	60
The System and Management Lifecycle Onion	61
Mapping Control Methodologies onto the Cloud	62
<i>Information Technology Infrastructure Library</i>	63
<i>Control Objectives for Information and Related Technology</i>	64
<i>National Institute of Standards and Technology</i>	65
<i>Cloud Security Alliance</i>	66
Verifying Your Lifecycle Management	67
<i>Always Start with Compliance Governance</i>	67
<i>Verification Method</i>	68
<i>Illustrative Example</i>	70
Risk Tolerance	72
Special Considerations for Cross-Cloud Deployments	73
The Cloud Provider's Perspective	74
<i>Questions That Matter</i>	75
In Summary	76
Chapter 5: Cloud-Based IT Service Delivery and Support	79
Beyond Mere Migration	80
Architected to Share, Securely	80
<i>Single-Tenant Offsite Operations</i>	
<i>(Managed Service Providers)</i>	81
<i>Isolated-Tenant Application Services</i>	
<i>(Application Service Providers)</i>	81
<i>Multitenant (Cloud) Applications and Platforms</i>	82
<i>Granular Privilege Assignment</i>	82
<i>Inherent Transaction Visibility</i>	84
<i>Centralized Community Creation</i>	86
<i>Coherent Customization</i>	88
The Question of Location	90
Designed and Delivered for Trust	91
<i>Fewer Points of Failure</i>	91
<i>Visibility and Transparency</i>	93
In Summary	93

Chapter 6: Protection and Privacy of Information	97
Assets in the Cloud	
The Three Usage Scenarios	99
What Is a Cloud? Establishing the Context—Defining Cloud	
Solutions and their Characteristics	100
<i>What Makes a Cloud Solution?</i>	101
<i>Understanding the Characteristics</i>	104
<i>Service Based</i>	104
<i>On-Demand Self-Service</i>	104
<i>Broad Network Access</i>	104
<i>Scalable and Elastic</i>	105
<i>Unpredictable Demand</i>	105
<i>Demand Servicing</i>	105
<i>Resource Pooling</i>	105
<i>Managed Shared Service</i>	105
<i>Auditability</i>	105
<i>Service Termination and Rollback</i>	106
<i>Charge by Quality of Service and Use</i>	106
<i>Capability to Monitor and Quantify Use</i>	106
<i>Monitor and Enforce Service Policies</i>	107
<i>Compensation for Location Independence</i>	107
<i>Multitenancy</i>	107
<i>Authentication and Authorization</i>	108
<i>Confidentiality</i>	108
<i>Integrity</i>	108
<i>Authenticity</i>	108
<i>Availability</i>	108
<i>Accounting and Control</i>	109
<i>Collaboration Oriented Architecture</i>	109
<i>Federated Access and ID Management</i>	109
The Cloud Security Continuum and a Cloud Security Reference Model	110
Cloud Characteristics, Data Classification, and Information	
Lifecycle Management	113
<i>Cloud Characteristics and Privacy and the Protection</i>	
<i>of Information Assets</i>	113
<i>Information Asset Lifecycle and Cloud Models</i>	114
<i>Data Privacy in the Cloud</i>	118
<i>Data Classification in the Context of the Cloud</i>	119
Regulatory and Compliance Implications	119
A Cloud Information Asset Protection and Privacy Playbook	121
In Summary	124

Chapter 7: Business Continuity and Disaster Recovery	129
Business Continuity Planning and Disaster Recovery	
Planning Overview	129
<i>Problem Statement</i>	130
<i>The Planning Process</i>	131
<i>The Auditor's Role</i>	133
Augmenting Traditional Disaster Recovery with Cloud Services	135
Cloud Computing and Disaster Recovery: New Issues to Consider	136
<i>Cloud Computing Continuity</i>	136
<i>Audit Points to Emphasize</i>	138
In Summary	139
Chapter 8: Global Regulation and Cloud Computing	143
What is Regulation?	144
<i>Federal Information Security Management Act</i>	146
<i>Sarbanes-Oxley Law</i>	146
<i>Health Information Privacy Accountability Act</i>	146
<i>Graham/Leach/Bliley Act</i>	147
<i>Privacy Laws</i>	147
Why Do Regulations Occur?	148
<i>Some Key Takeaways</i>	149
The Real World—A Mixing Bowl	149
<i>Some Key Takeaways</i>	151
The Regulation Story	151
<i>Privacy</i>	153
<i>International Export Law and Interoperable Compliance</i>	154
Effective Audit	155
Identifying Risk	156
In Summary	156
Chapter 9: Cloud Morphing: Shaping the Future of Cloud Computing Security and Audit	161
Where Is the Data?	162
A Shift in Thinking	164
<i>Cloud Security Alliance</i>	165
<i>CloudAudit 1.0</i>	166
Cloud Morphing Strategies	166
<i>Virtual Security</i>	167
Data in the Cloud	168
Cloud Storage	169

xii ■ Contents

<i>Database Classes in the Cloud</i>	171
<i>Perimeter Security</i>	171
Cryptographic Protection of the Data	172
In Summary	173
Appendix: Cloud Computing Audit Checklist	175
About the Editor	181
About the Contributors	183
Index	191

<http://www.pbookshop.com>