

/THEORY/IN/PRACTICE

Cloud Security and Privacy

An Enterprise Perspective on Risks and Compliance



O'REILLY®

Tim Mather
Subra Kumaraswamy
Shahed Latif

CONTENTS

	PREFACE	xi
1	INTRODUCTION	1
	<i>"Mind the Gap"</i>	1
	<i>The Evolution of Cloud Computing</i>	2
	<i>Summary</i>	5
2	WHAT IS CLOUD COMPUTING?	7
	<i>Cloud Computing Defined</i>	7
	<i>The SPI Framework for Cloud Computing</i>	11
	<i>The Traditional Software Model</i>	17
	<i>The Cloud Services Delivery Model</i>	17
	<i>Cloud Deployment Models</i>	22
	<i>Key Drivers to Adopting the Cloud</i>	26
	<i>The Impact of Cloud Computing on Users</i>	27
	<i>Governance in the Cloud</i>	30
	<i>Barriers to Cloud Computing Adoption in the Enterprise</i>	30
	<i>Summary</i>	34
3	INFRASTRUCTURE SECURITY	35
	<i>Infrastructure Security: The Network Level</i>	36
	<i>Infrastructure Security: The Host Level</i>	44
	<i>Infrastructure Security: The Application Level</i>	49
	<i>Summary</i>	59
4	DATA SECURITY AND STORAGE	61
	<i>Aspects of Data Security</i>	61
	<i>Data Security Mitigation</i>	65
	<i>Provider Data and Its Security</i>	66
	<i>Summary</i>	71
5	IDENTITY AND ACCESS MANAGEMENT	73
	<i>Trust Boundaries and IAM</i>	73
	<i>Why IAM?</i>	74
	<i>IAM Challenges</i>	76
	<i>IAM Definitions</i>	76
	<i>IAM Architecture and Practice</i>	77
	<i>Getting Ready for the Cloud</i>	80
	<i>Relevant IAM Standards and Protocols for Cloud Services</i>	82
	<i>IAM Practices in the Cloud</i>	92
	<i>Cloud Authorization Management</i>	98

	<i>Cloud Service Provider IAM Practice</i>	99
	<i>Guidance</i>	104
	<i>Summary</i>	107
6	SECURITY MANAGEMENT IN THE CLOUD	109
	<i>Security Management Standards</i>	112
	<i>Security Management in the Cloud</i>	113
	<i>Availability Management</i>	115
	<i>SaaS Availability Management</i>	117
	<i>PaaS Availability Management</i>	120
	<i>IaaS Availability Management</i>	122
	<i>Access Control</i>	124
	<i>Security Vulnerability, Patch, and Configuration Management</i>	130
	<i>Summary</i>	141
7	PRIVACY	145
	<i>What Is Privacy?</i>	146
	<i>What Is the Data Life Cycle?</i>	146
	<i>What Are the Key Privacy Concerns in the Cloud?</i>	149
	<i>Who Is Responsible for Protecting Privacy?</i>	150
	<i>Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing</i>	151
	<i>Legal and Regulatory Implications</i>	155
	<i>U.S. Laws and Regulations</i>	155
	<i>International Laws and Regulations</i>	162
	<i>Summary</i>	164
8	AUDIT AND COMPLIANCE	167
	<i>Internal Policy Compliance</i>	168
	<i>Governance, Risk, and Compliance (GRC)</i>	170
	<i>Illustrative Control Objectives for Cloud Computing</i>	174
	<i>Incremental CSP-Specific Control Objectives</i>	179
	<i>Additional Key Management Control Objectives</i>	180
	<i>Control Considerations for CSP Users</i>	181
	<i>Regulatory/External Compliance</i>	182
	<i>Other Requirements</i>	192
	<i>Cloud Security Alliance</i>	192
	<i>Auditing the Cloud for Compliance</i>	194
	<i>Summary</i>	202
9	EXAMPLES OF CLOUD SERVICE PROVIDERS	203
	<i>Amazon Web Services (IaaS)</i>	203
	<i>Google (SaaS, PaaS)</i>	205
	<i>Microsoft Azure Services Platform (PaaS)</i>	206
	<i>Proofpoint (SaaS, IaaS)</i>	207
	<i>RightScale (IaaS)</i>	208
	<i>Salesforce.com (SaaS, PaaS)</i>	210
	<i>Sun Open Cloud Platform</i>	211
	<i>Workday (SaaS)</i>	213
	<i>Summary</i>	213

10	SECURITY-AS-A-[CLOUD] SERVICE	217
	<i>Origins</i>	218
	<i>Today's Offerings</i>	220
	<i>Summary</i>	223
11	THE IMPACT OF CLOUD COMPUTING ON THE ROLE OF CORPORATE IT	225
	<i>Why Cloud Computing Will Be Popular with Business Units</i>	226
	<i>Potential Threats of Using CSPs</i>	228
	<i>A Case Study Illustrating Potential Changes in the IT Profession Caused by Cloud Computing</i>	230
	<i>Governance Factors to Consider When Using Cloud Computing</i>	235
	<i>Summary</i>	236
12	CONCLUSION, AND THE FUTURE OF THE CLOUD	239
	<i>Analyst Predictions</i>	240
	<i>Survey Says?</i>	242
	<i>Security in Cloud Computing</i>	245
	<i>Program Guidance for CSP Customers</i>	257
	<i>The Future of Security in Cloud Computing</i>	260
	<i>Summary</i>	265
A	SAS 70 REPORT CONTENT EXAMPLE	267
B	SYSTRUST REPORT CONTENT EXAMPLE	273
C	OPEN SECURITY ARCHITECTURE FOR CLOUD COMPUTING	279
	GLOSSARY	293
	INDEX	299