



Adding Cloud Solutions to Customer Contracts

Robert J. Scott

MSP vs. Cloud

- Who owns the hardware?
- Where does the data reside?
- Dedicated vs. Multi-tenant?
- Who contracts with 3rd parties?
- How are services billed?
- Who is responsible for software licensing?
- What happens if there is a data breach?
- How does the legal risk differ?

Key Provisions in Cloud Contracts

- Intellectual property ownership
- Insurance and indemnity requirements— especially for intellectual property infringement
- Regulatory compliance
- Subcontractor liability for third party services or software
- Effect of termination—return of customer data
- Service failure corrective action plan

Risk Overview

Business Continuity Risks

- Service Interruption
- Post-termination
Data Rights

Regulatory Compliance Risks

- Data Privacy and
Security Statutes

Intellectual Property Risks

- Use and Disclosure of
Information
- Ownership of Software
- IP Ownership at
Termination

Liability Risks

- Risk Balancing

Business Continuity Risks

Service Interruption

- Define service levels, metrics, and remedies in the SLA

Termination of the Agreement

- Ensure data is owned by and returned to customer in a usable format upon termination

Intellectual Property Risks

Use and Disclosure of Information

- Ensure both parties understand the nature of the data stored in the cloud
- Specifically personally identifying information and trade secrets

Intellectual Property Ownership

- Define ownership of any software customizations
- Exclusivity of customizations during term of engagement

IP Ownership at Termination

- Work for hire or vendor-owned code

Regulatory Compliance Risks

Industry-specific Regulation

- Gramm-Leach-Bliley Act – Financial
- HIPAA & HITECH – Healthcare
- PCI Compliance – Payment Systems

State Laws

- Data Privacy
- Safeguards

Common Regulatory Requirements

Privacy and Security Policies

- Regular risk assessment
- Access and audit controls
- Enforcement of policies

Encryption

- Data in transmission and in storage
- Does not address every regulatory requirement

Breach Notification

Regulatory Compliance in Cloud Contracts

Risk involved in reselling public cloud

- Cloud service providers attempt to offload regulatory and liability risk
- Click-wrap contracts
- No opportunity to negotiate

Regulatory Compliance in Cloud Contracts

Large-scale, integrated services

- Negotiated contracts
- Storage of specific data types defined
- Regulatory requirements addressed
- Risks balanced with indemnity and insurance

Healthcare & Financial Services

- Create your own BAA for Healthcare
- Use GLBA attachment for Financial Services Clients
- Clearly define roles and responsibilities for affect of termination & data breach

Liability Risks

Risk Balancing

- Vendors disclaim all liability—this is unacceptable to the customer
- Insurance as a tool for risk balancing
- Indemnity as a tool for risk balancing

Striking the Balance

- Specifically address liability issues specific to the type of data being stored in the cloud
- Risk should be commensurate with the value of the cloud service

Mitigating Risks in the Cloud

Cloud Service Providers

- Understand industry/region regulatory requirements
- Use indemnity provisions
- Obtain cyber risk insurance
- Encrypt data in motion and in storage

The background features a blue-to-white gradient with a faint, semi-transparent grid of rounded squares and binary code (0s and 1s) overlaid. The word "Questions?" is centered in a bold, dark blue font.

Questions?

Contact Information

Robert J. Scott

rjscott@scottandscottllp.com

Managing Partner

214.999.2902

Scott & Scott, LLP

ScottandScottllp.com

1256 Main Street

Suite 200

Southlake, TX 76092