Cloud Contracts – Risks and Mitigation Strategies

Frank Bruno, Director & Senior Business Strategist, Iron Mountain

Rob Scott, Scott Technology Attorneys,
Let’s Talk About

• The Ever-Changing Cloud Computing Landscape
• Need for Due Diligence – “Governance, Risk & Compliance”
• Risk Assessments – Business Impact from “What-if’s”!
• Practical Strategies for SaaS Contingency Planning
• Enabling Strategies with the Right Contractual Terms
• Security & Privacy
• Business Continuity
• 3rd Party Litigation
• Regulation Compliance
• Q&A
The Techtonic Shift in Tech Delivery

**SaaS**
- Application and data hosted by SaaS provider
- User accesses software via the internet (SaaS)
- End user does not have a copy of the object code (executable) and their data.

**On Premises**
- Software developer delivers executable on media to the user
- User accesses software on local system
- End user has a copy of the object code (executable) and their data.
DUE DILIGENCE
“Yes, but what-if? Then what?”

- Bankruptcy (an “Enron-Like Occurrence”)
- M&A (non prevailing products suffer from extinction)
- Contract Breach (Blown SLA’s)
- Force Majeure
- Extended Outage
- Exit Strategy
- Can’t Recover Your Data?
Risk Assessments

Operational Dependencies
✓ Number of users
✓ Customer facing impact/brand
✓ Lost productivity & Revenue
✓ Business Continuity / Disaster Recovery Planning (BC/DRP)
✓ Suitable interim alternatives

Investment of Time
✓ Corporate Tolerance - Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
✓ Availability of substitute SaaS products
✓ Time to identify new product
✓ Time transition and negotiate

Costs
✓ Security Assessments
✓ Monthly Subscription
✓ Retraining and ongoing training
✓ Integration with Legacy Apps
✓ Customization

Vendor Assessment
✓ Vendor stability
✓ Single vs. Multi tenancy
✓ Subcontractor partnerships, i.e. hosting parties
✓ Acquisition Risk/Change in Control

What level of escrow and data protection are needed based on the Risks of SaaS?
CONTINGENCY PLANNING
Practical Strategies for SaaS Contingency Planning

• Marshaling resources & expertise to craft the plan
• Create standards to address the risk of doing business
• Concerns become Triggers to set the contingency in motion
• Means to keep working while you execute (application continuity)
• Trusted, neutral third party administration to execute the plan!
• Successors in waiting to take over
• Testing to verify that the plan works
• Unambiguous contract terms to allow for unencumbered success!
Contingency Trigger Process

What-if Occurs:
- Subscriber contacts Provider

No response:
- Subscriber Contacts 3rd Party Admin

Problem solved:
- Contingency Trigger process invoked
- Access to Recovery Environment provided
- Data Recovered

Desired Outcome:
- Application Continuity Secured

Subscriber contacts Provider

Problem solved!

Contingency Trigger process

Iron Mountain
Establish Standards to Support Contingency Plans

- Deposit Requirements
- Verification (DR) Testing Rights
- Release Conditions (Triggers)
- Demand or Notice Process
- Objection Period
- Contrary Instructions
- Rights Following a Release
- Payment of Fees
- Repeatable Process
Repeatable Process

1. Conduct your due diligence and craft your contingency plan!
2. Communicate contingency requirements up front as a condition of doing business
3. Execute an agreement that includes the contingency solution
4. Test Everything Frequently

Do this before you pay a single vendor invoice!
Questions?

- Frank Bruno
- frank.bruno@ironmountain.com
- +1 303-954-8830

Twitter: @FrankBruno4
LinkedIn: www.linkedin.com/pub/frank-bruno/0/664/691
Cloud Contracts – Risks and Mitigation Strategies

Presented by Robert J. Scott
Managing Partner Scott & Scott, LLP

www.ScottandScottllp.com
Key Provisions in Cloud Contracts

• Intellectual property ownership

• Insurance and indemnity requirements –especially for intellectual property infringement

• Regulatory compliance
Key Provisions in Cloud Contracts

- Subcontractor liability for third party services or software
- Effect of termination – return of customer data
- Service failure corrective action plan
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
Mitigating Risks in the Cloud

Cloud Service Providers

• Ensure providers meet and take some responsibility for your regulatory requirements

• Require cyber risk insurance

• Implement employee Acceptable Use policy to limit exposure on free or low-cost cloud services
Contact Information

Robert J. Scott, Esq.
Managing Partner
Scott & Scott, LLP.
1256 Main Street, Suite 200
Southlake, TX 76092

Phone: (214) 999-2902
Fax: (214) 999-0333

E-Mail: rjscott@scottandscottllp.com