Cloud Service Provider Risk Assessment

Barry Ribbeck
Director SAI-CSI
brr@rice.edu

Need to Tweet #EDU14

© 2014
Located in Houston, Texas
101 years old
Private – R1
13,000 Faculty, Staff & Students
Unabashed bragging

Because we are a bit proud and after all we are in Texas

- Princeton Review – #1 Best value colleges in 2014, #2 student life
- Kiplinger’s Financial - #1 Best Value
- US News top 20
- Leiden #1 for Natural Sciences and engineering & #6 for all sciences
- #5 Athletic Academic rating by NCAA
- #7 US News Biomedical Engineering
Why we’re here

By David February 17, 2011 7:32 am
4 Things to Remember

What a cloud risk assessment is to Rice

• Our Method
• Our Tools
• Our Stakeholders
• Our Results
Aversion, Mitigation, Denial

It's been announced our company is moving to the cloud. How's your fear of heights?

By David May 2, 2014 9:36 am
Definitions

• Cloud Risk Assessment Protocol: A step by step repeatable process used to produce an understanding of risk associated with relinquishing control of data or management of services to an external party.

• External party: any entity that does not fall under an institutions direct management.
Risk Factors

- Enumerate Scope and Scale
- Contract and Practice
- Cost of non-compliance
- Cost of service
- Defined support boundaries
- data security management
- BC/DR planning
Graphic Flow Chart

Cloud Request

IT-Legal Review

Assess and discuss with client & vendor

Issues?

Yes

Complete contract, Document, Sign Off, Implement, Support and Post for future Review

No
1. Stakeholder requests review for purchase of services
2. OGC and IT review the contract. IT reviews the TOS and risk
3. Risk Assessment begins
   - Documentation review
   - Discussion with Stakeholder
   - Questions to vendor
Risk Assessment Concludes with a document and checklist that is issued to and reviewed with the stakeholder and OGC stating any risks and recommendations.

Review with OGC if require or it is blessed to proceed.
– Security (data protection, authX)
– Data Compliance Identification (PII, FERPA, HIPAA, PCI, SOX, GLB, NCAA ..)
– Workflow analysis
– Data Management
– Back out plan
– Recent breach search
– Vendor review (financial, news, leadership)
– Periodic Review of TOS by stakeholder
- Cloud Security Alliance Security Trust Assurance Registry (STAR) 7/14
- Breach reporting sites
- Rice review checklist
- HIMSS Healthcare Cloud Risk Assessment
- Cloud Risk Analysis Frameworks
- Google
- $\text{Risk} = \text{Value of Loss} \times \text{probability of loss}$
Break for questions
Reading the fine print

By David May 9, 2014 9:24 am
You have to read the contract(s)

- Establish responsibility
- Assess if the contract is skewed in favor of?
- Determine Service warranty (AS IS?)
- SLAs linked to the contract
- Referenced security (data center audits)
- What will you pay for vs what you expect
- Key word searches (see key word list)
Questions for Stakeholder

– Why this product?
– Who is using it, how and why they chose it?
– What data is exposed, how and what will you do if there is a breach?
– What will you do if this service is unavailable?
– Will this be mission critical?
– How many people will be affected if the service is unavailable
Set Expectations

I can't listen to some soothing music while I wait for the net to come back on, I uploaded it all to the cloud!!!
Documents to Review

• Terms of Service
• Security Policy
• Privacy Policy
• Web Site (About Us)
• Data Center Audit Reports
• Web Site (Investors section)
Contract Key Words

- Indemnification (hold harmless)
- Warranty – what is the warranty if any?
- Export – export controls requirements
- Third Party – both upstream and downstream
- Liability – who pays for what when something goes wrong
- Termination – how does this all end
- Jurisdiction or Governing Law - Who’s back yard do we fight in
- Suspension – when service is halted
- Dispute – when you don’t agree what are the rules of engagement
- Service Level – IF ANY
- Discovery – how do you handle subpoenas
- Infringement – patents, intellectual property and copyright
- Privacy – what is done with your data
- ANY Hyperlinks – to other documents
- Notification – when are you notified of change or problem
Other Terms

- Commercially reasonable
- Intellectual Property
- Limits of Liability
- Force Majeure
- Equitable Relief
IT has reviewed X and has found that except where noted above, X has demonstrated through successful audits and controls what we would consider industry-standard or better levels of security and operational best practices within their operation. However, regardless of the protections employed, no one is immune from all attacks. IT recommends periodic reevaluation of the term of service, development and testing of a back out plan that includes data recovery and a business continuity plan that would account for loss of access to the services provided by X.
Break for Questions
Summary of the 4 things

• What a cloud risk assessment is to Rice
• Method – how Rice does it
• Tools – Due Diligence
• Stakeholders – get them involved
• Results – risk assessment and better understanding of business process
Seed Questions

- How long does a risk assessment like this take?
- How much man power is required?
- Do you charge fees to customers for this service?
- Have you had any cloud services go bad?
- How many cloud services do you currently support?
- What do you find is the real value in doing this work?
- Where do you think cloud services will go in the future?
- Are their standards being developed for cloud services?