Guide for Evaluating Service & Security of Cloud Service Providers

Introduction

Cloud computing is rapidly transforming the IT landscape. Many Lehigh University Data Owners are showing strong interest in outsourced Cloud offerings that can help reduce costs and increase enterprise agility. These Cloud services offer enormous economic benefits but they also may pose significant potential risks in safeguarding university information assets, and in complying with a myriad education, industry, and government regulations.

The goal of this guide is to provide to units within Lehigh University an ability make pragmatic decisions about where and when to use Cloud solutions by outlining specific issues that should be raised with hosting providers before selecting a vendor, as well as highlight the ways the vendor might respond in any service RFP so that Lehigh Data Owners might conduct business in the Cloud with confidence.

This guide can be used to assist Lehigh University personnel as well as Service Providers in responding to RFP’s and evaluating collocation, managed hosting, Cloud and Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Desktop-as-a-Service (DaaS), and Backend-as-a-Service (BaaS) providers. It is recommended each Data Owner should carefully evaluate every question/requirement to insure it is valid for their specific needs. Additional evaluation criteria, questions, and information may be included to reflect unique requirements and thus certain portions of this content may be eliminated or expanded upon, depending upon those specific requirements.

Cloud Computing: Providing Both New Opportunities and New Security Challenges

To create an organized evaluation template this guide will be broken into nine areas for consideration. Two of these areas include a General Considerations and Data Encryption section. The remaining seven areas will align to areas of security risk services associated with enterprise Cloud computing as defined by Gartner Research. In those areas Gartner recommends that organizations address several key issues when selecting a Cloud hosting provider:

- **Access Privileges** – Cloud service providers should be able to demonstrate they enforce adequate hiring, oversight and access controls to enforce administrative delegation.
- **Regulatory Compliance** – Enterprises are accountable for their own data even when it’s in a public Cloud, and should ensure their providers are ready and willing to undergo audits.
- **Data Provenance** – When selecting a provider, ask where their datacenters are located and if they can commit to specific privacy requirements.
- **Data Segregation** – Most public Clouds are shared environments, and it is critical to make sure hosting providers can guarantee complete data segregation for secure multi-tenancy.
- **Data Recovery** – Enterprises must make sure their hosting provider has the ability to do a complete restoration in the event of a disaster.
- **Monitoring and Reporting** – Monitoring and logging public Cloud activity is hard to do, so enterprises should ask for proof that their hosting providers can support investigations.
- **Business Continuity** – Businesses come and go, and enterprises should ask hard questions about the portability of their data to avoid lock-in or potential loss if the business fails.

To reap the benefits of Cloud computing without increasing security and compliance risks, Lehigh University must ensure they work only with trusted service providers that can address these and other Cloud security challenges. In moving from using just one Cloud-based service to using several from different providers, we also must manage all these issues across multiple operators, each with different infrastructures, operational policies, and security skills. This complexity of trust requirements drives the need for a ubiquitous, highly reliable method to secure your data as it moves to, from and around the Cloud.

Cloud Provider Requirements Sections

**General Requirements**

- A detailed description of the customer data the vendor requires to perform their tasks and an acknowledgement that Lehigh is the data owner.
- Does the provider have an allowance to audit either the application or network infrastructure? What notice is required to do non-intrusive vs. intrusive scans or other vulnerability assessments?
- What allowances does the vendor provide to access or request any security related configuration files, developed application code, or policy or quality assurance and testing documents?
- Are there any customization or customer specific changes allowed for your Cloud services? If so please describe. Are there additional costs?
- What internal software/hardware/infrastructure audits do you perform and what actions do you take upon locating a security issue?
- Do you have an incident response plan and can you describe it? Any incident response history or examples are helpful.
- Explain how you designate a customer contact in the event of a breach or security issue?
- What internal software/hardware/infrastructure audits do you perform and what actions do you take upon locating a security issue?
- Do you use the customer data for any other purposes, whether metadata (in part) or whole for other services?
- Description of scheduled maintenance times and customer notification processes. Any maintenance history provided is helpful.
- Explain your levels of customer support for your Cloud offering beyond self-help, knowledge based or message boards. Are there additional costs associated for this support? If so, note those costs.
- Define your trouble ticket severity levels. How are they assigned and how are they escalated? Is escalation automatic based on a metric or customer initiated?
- Service Level Agreement for uptime. Targets should be 99.99% if possible but may vary. Be wary of any stated level that has disclaimers for “additional subtractions”.

For Lehigh guidance:

- 99.99% uptime translates to less than 53 minutes per year downtime
- 99.9% uptime translates to almost 9 hours per year downtime
- 99.5% uptime translates to almost 44 hours per year downtime
- 99% uptime translates to almost 90 hours (87.6 or 3.65 days) per year downtime
*Outage or disaster subtractions may or may not be tolerable to Lehigh depending on use.

- Any ADA or other accessibility requirements or capabilities.
- Mobile device access capabilities and any security controls for protecting linking to lost or stolen customer mobile devices containing data.
- Explain your employee hire, orientation and security training process and any non-compete or data/customer confidentiality agreements you have them sign.

Encryption Requirements

- Data in transit and file uploads or transfers must be secured with encryption protocols. Those protocols utilized should be explained by the vendor.
- For data in transit Cloud providers should be using SSL from an established, reliable and secure independent CA. The SSL CA needs its authentication practices audited annually by a trusted third-party auditor.
- For data in transit SSL should deliver at minimum 128-bit encryption and optimally 256-bit encryption based on the new 2048-bit global root. And it should require a rigorous authentication process. The SSL issuing authority should maintain military-grade data centers and disaster recovery sites optimized for data protection and availability.
- For data in storage what Encryption technology is utilized for data storage?
- For data in storage how are encryption keys for stored data managed?
- Particularly for data backup and recovery what technology is used to encrypt data backups and how are those keys managed?
- If databases are utilized to what level is encryption applied?

Access Privileges and Controls

- A description of the physical security measures in place within your data centers. Describe both the physical data center access as well as server room and physical host access.
- How are the logical and physical data center services secured from other users and from external threats?
- What level of support does the vendor provide for Single-sign-on (SSO) or authentication utilizing Lehigh identity management infrastructure.
- A detailed description of those authentication methods.
- Any support for two-factor authentication?
- What level of Administrative privileges and controls does Lehigh have over the system or software and its users?

Regulatory Compliance

- What is the vendor’s and any 3rd party’s compliance requirements to SSAE 16/SAS70-II, SOX, PCI-DSS, ISAE3402, SOC1, 2 or 3, Safe Harbor, or other regulatory certification requirements.
- Can the vendor describe the commitment to their and any 3rd party utilized to remain in such compliance?
- Will the vendor attach their latest compliance audit performed by a recognized qualified 3rd party and commit to maintaining that described level of security?

Data Provenance

- A detailed inventory of hardware specifications, including manufacturers, for all Cloud product offerings. Include manufacturer, model numbers, processors, disk drives, database hardware, data center networking components (routers, switches, etc.), security devices (firewalls, etc.), load balancers, and any other hardware relevant to the delivery of the service.
- A description of how often is infrastructure/hardware/software upgraded, hardened and patched and what communications/requirements are there with the customer?
- Describe the automated Information Lifecycle (Configuration Upgrade and Control) Management capabilities of your Cloud offering and the benefits clients receive from this functionality.
- What are any options for dedicated storage, dedicated hardware firewalls and load balancers to connect to the public Cloud offerings in your facilities?
- Can you share networks, VPNs, firewalls and load balancers between your dedicated and public Cloud environments?
- An outline of the size of the network (number of contiguous IP addresses) available to a customer’s Cloud environment.
- Explain your data and sensitive documents handling and destruction practices for customer data.

Data Segregation

- Provide an overview of the dedicated single-tenant and shared (multi-tenant) Cloud services provided by the company.
- Notation if the data center components are provided by you or by another third party and a description of maintenance or transfer of those services.
- As a customer how are we responsible to entering or transferring data?
- Explain how data is either physically or logically separated such that one account cannot see data from any other account.

Data Recovery

- Describe the SAN and/or NAS storage options connected to your Cloud.
- Describe the backup and archival process and length of time backups are available.
- Do you perform test restores?
- Do you have any file or directory versioning capability or capabilities short of restoring from a backup?
- Location of backups and key management and storage for any backup encryption keys.
- What archival backup/restore/versioning is part of the agreement and what actions require any additional service fees?
- Explain any shadowing or redundancy you have across multiple datacenters or repositories and if those data repositories are within the US and controlled by the vendor.
- An explanation of the vendor disaster recovery plan with maximum downtime limits.
- Do you offer persistent Cloud images (longer than 2-week retention) or offer back up in your Cloud longer than 1-month retention?
- Does your Cloud backup allow file based restore, without requiring clients to mount a full historic copy of their virtual machine?

Monitoring and Reporting
• Explain how the vendor monitors and reports upon notification of abuse or investigation. This might include DMCA notices, regulatory violations, criminal or civil investigations and additional requests made by either an outside entity or Lehigh University.
• Explain the dashboards and analytics that are in place for customer use.
• Explain any real-time monitoring that the customer might deploy that the vendor has developed.
• Explain what additional reporting, training, aggregate, industry, research, or other reporting information or data might be available as part of a customer subscription.

**Business Continuity**

• Do you have a formal Risk Analysis plan and review it annually?
• Do you have a Disaster Recovery plan and its details?
• What tests do you perform on your disaster recovery plan?
• What are the contract stipulations potential customer losses or for transfer of data and support to another organization should the business fail?