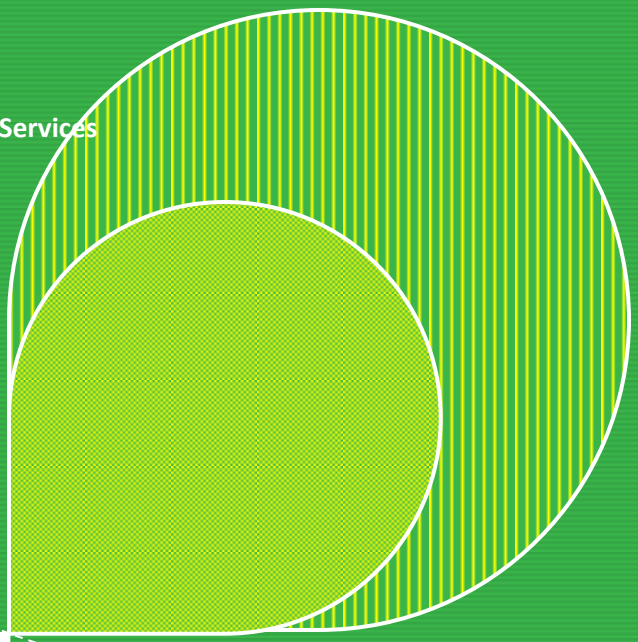
Moving to Clouds? Simplify your approach to understand the risks and protect your data

By Thiruvadinathan
Happiest Minds,
Infrastructure Management and Security Services



happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

How to work with your Cloud vendor to secure sensitive and critical data on the cloud?

Engaging with a vendor especially one who provides some sort of Information and/or technology based services is necessary for many global organizations. Managing risks related to vendors presents its own challenges particularly if they are high technology companies such as Cloud Service Providers (CSP).

Cloud based services add to the complexities of managing traditional security & compliance risks. Identifying and addressing risks associated with moving your data, applications and services are not the only thing that an organization has to consider. An organization also needs to think about and plan for vendor related risks, legal, regulatory and contractual risks. This spectrum of risks continues to expand particularly when dealing with customers and vendors who are operating in different geographies governed by different regulations, data protection laws, culture and operating models.

The following sections discuss some of the challenges involved in assessing those risks.

Are risks in the Cloud different?

The answer is yes and no. Clouds bring in both traditional information security risks such as malicious users, malware, etc. as well as lack of control over and visibility into your data in terms of who has access, where the data is located, how it is secured, etc. Some of the common lacunae in addressing the risks in the Cloud are

- Lack of or inadequate security and compliance risk evaluation of CSPs due to:
    - Business pressures and deadlines
    - Lack of involvement from information security, risk and internal audit teams or specialists during evaluation
    - Inadequate knowledge about cloud security risks, mitigation and monitoring technologies
    - Legal complexities.

- Complexities involved in evaluating risk, security and compliance aspects of engaging with a CSP since risks and requirements can vary widely depending on the type of Cloud service(SaaS, IaaS, etc.) and model (Public, Private, etc.)
- Finding CSPs that treat all customers equally when it comes to risk, security and compliance
- Lack of a formal contract or inadequate service contracts
    - Lack of awareness on what need to be addressed in the contract such as
    - Ownership & confidentiality of data

- Compliance with your security policies based on mapping your controls to CSP's capabilities
- Data classification and corresponding security requirements for transmission, storage, handling/usage, sharing, back-up, retention, geographical restrictions on data movement within the cloud, disposal and e-discovery
- The right to audit and actual audit of CSP' security controls

There are many other areas that need to be addressed in a contract. An article by a New York business law firm provides insights into what needs to be addressed in a contract. The article can be read at http://bit.ly/xMZNx6. Another article published on The Financial Times details about the grey areas in a Cloud service contract, http://on.ft.com/N89J3Z.

This list of such lacunae could easily expand into other areas such as risks related to CSP's staff in terms of their background credentials, operational risks such as inadequate change management, errors and omissions, failed back-ups and so on.

However, there is help available to address these challenges. No matter what standards you use among ISO27001, PCI-DSS, NIST SP 800-53, CoBIT, etc., you can leverage your experience on those and bring value to your assessment Cloud & Vendor risks. To know more about how, read on…

Simplify your approach to assess Cloud vendor risks

The Cloud Security Alliance (CSA) provides a security controls framework that can be used by CSPs as well as Cloud consumers both. The assessment tools namely, the Consensus Assessment Initiative Questionnaire (CAIQ) and Cloud Controls Matrix (CCM) are specifically designed for Cloud environment to assess the associated risk and security requirements.

The rigor of going through multiple and long security assessment questionnaire can be quite challenging both for the Cloud consumers as well as CSPs. Vendor risk assessment tools would typically span multiple security domains requiring the involvement of staff from various functions within the organization. The process takes considerable time, resources and skills to go through. Smaller organizations may require additional resources and skills to do the evaluation of CSP.

Using CSA STAR in Cloud security assessments

To assist potential Cloud consumers and CSPs, the Cloud Security Alliance has come up with an initiative known as STAR (CSA **S**ecurity, **T**rust & **A**ssurance **R**egistry). STAR is a program participated by many of the leading CSP. Participants of this program voluntarily prepare a self-assessment of their controls and compliance posture in a format specified by CSA.

CSPs can make use of either CAIQ or CCM to perform self-assessment of their Cloud security controls. The self-assessment reports are published by the respective CSPs and are made available. The reports are free to download from https://cloudsecurityalliance.org/star/

The STAR program also encourages participating vendors to be available for any question from the consumers.

The advantage of this report is that the format provides for mapping with international standards and best practices such as IS027001, COBIT, NIST, etc. This can simplify the overall assessment in terms of rigor and also improve the focus on the controls that require more attention. The CSA also provides a GRC stack those organizations that are willing to integrate CAIQ and CCM into their GRC management solution.

The following section provides a simplified approach to assess the Cloud related risks.

Steps 1 – Prepare yourselves

- Determine what type of Cloud service (SaaS, PaaS, and IaaS) and Cloud model (Public, Private, etc.) you require.
- Many CSPs are very likely to have implemented ISO27001. It is important to understand the scope of such certification and to understand what controls have either been implemented or omitted.
- If CSP have implemented ISO27001, then ask for their Statement of Applicability and have a dialogue with them to understand how the applicable controls are implemented. For CSPs that have not implemented ISO27001, ask for any other standard or regulatory compliance that's been implemented. Even a SAS70 Type 2 or SOC 2 report can be a very good starting point.
- Determine if the CSP has undergone a self-assessment and obtain the report from CSA website.
- Shortlist potential CSP vendors based on the above, check for credible references from existing customers of the CSPs you are going to evaluate.

Step 2 – Perform an Analysis

- Perform a detailed analysis of the self-assessment reports from the CSPs. Evaluate the controls in line with your data security and compliance requirements.
- Speak to their references to understand how their needs relates to your business
- Provide weightage to the CSP that is willing co-operate fully with your requirements
- Involve your legal, IT, security, risk and audit teams throughout the process
- Have a list of your regulatory compliance requirements to understand how the CSP would help

Step 3 – Prioritize your requirements

- Based on your analysis, narrow down and prioritize risk areas that remain to be addressed.

- Use CAIQ to extract those areas as to how you need to prepare yourself for further analysis
- Prepare your assessment questionnaire and have your shortlisted vendors respond to them.
- Plan a site visit where you can get evaluate the responses you received as to how they have been implemented
- During your visit, observe, inspect and document the controls implemented and practiced as you would understand.

Step 4 - Prepare a risk and control plan

- Develop a plan that identifies the risks and controls that would address the risks.
- Make this plan as the basis for preparing your contractual terms and conditions in conjunction with your shortlisted vendors
- Sensitize your users on on-going basis about the risks and controls

The huge advantage of this approach is that it can certainly help save a lot of time for the consumer as well as provider. The actual assessment can effectively be reduced significantly depending on the other factors such as availability of relevant skills and so on.

Depending on your organization's unique cloud computing needs, security and compliance requirements, your assessment must be tailored accordingly. A good understanding of the various types of Cloud services and models would be required. For example, SaaS based model offers very little room for control of data by the Cloud consumer, whereas IaaS offers the most flexibility. An assessment for a SaaS service should cover infrastructure security, IT operational security, application & data security as all these are fully under the control of CSP. The contract for a SaaS service shall also be designed to address security risks in these areas. Physical and environmental security is to be addressed anyway irrespective of the Cloud service, which determines the nature and extent of any Cloud security assessment and contractual requirements.

Conclusion

As Cloud based services evolve along with the associated technologies, the standards for cloud based risk management and assurance framework will have to evolve. The good news is existing standards such as PCI DSS, ISO27001, etc. can be judiciously leveraged for initial as well as on-going assessment of risk exposure and compliance status in conjunction with CSA's initiatives. The key is to keep updating your risk assessment framework and continuously engage with the CSP who's partnered with you to improve its services.

To learn more about the **Happiest Minds Cloud Security Offerings,** please write to us at **business@happiestminds.com**

About Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

About the author

Thiruvadinathan A (thiruvadinathan.a@happiestminds.com) is the Technical Director and Practice Lead for IT Governance, Risk Management, Security & Compliance services. He credits his rich experience in the field to his global clientele across industry verticals gained in the last 16 years. One of his recent achievements is having successfully led Happiest Minds Technologies to meet the stringent requirements of ISO27001 global standard.