Cloud Security Assessments – Identifying the Peskiest Risks!

- Published on February 10, 2020
- **Edit article**
- **View stats**

Sarbari Gupta

Founder and CEO, Electrosoft
5 articles

Modern software applications and IT infrastructures are complex. Most are constructed using building blocks, components and layers that other vendors and service providers contribute. Thus, when conducting an assessment to determine whether the system implements an appropriate level of security, the security assessor must determine the subset of security controls that each building block/component/layer implements and those that the final system owner must implement.

This task is difficult. For cloud-based information systems, the security assessor must clearly identify the boundary of responsibility for security control implementation between the end customer and one or more cloud providers that may comprise the information system.

As a person who has been watching, working on and talking about cloud security and cloud security assessments for many years, I've given some thought to the specific areas that should be a focus of security audits/assessments of cloud-based information systems. Below are a few thoughts (not in any particular order) on where I believe cloud security auditors need to pay special attention.

Common Controls – Many cloud customers mistakenly identify controls as being "common" and inherited from the cloud service provider. However, the AT (Awareness and Training) controls cannot be fully inherited from a cloud service provider. The cloud customer must implement an appropriate level of AT controls. Similarly, the Policy and Procedures control for each family cannot be inherited from a cloud service provider. The cloud customer must develop individual policies and procedures for each control family. The auditor needs to analyze the common controls claimed to be inherited from the cloud service provider to ensure that it is an appropriate allocation of controls.

Cloud Customer Responsibility Matrix – The cloud service provider's security authorization package needs to include a list of controls that the cloud customer is expected to implement. Cloud customers need to review this list, consider the context in which the cloud service is being used and prepare a list of security controls that are the full or partial responsibility of the cloud customer. Cloud auditors need to review the cloud customer responsibility matrix to validate it against the cloud provider's security authorization package and focus on auditing the controls that are identified as the cloud customer's responsibility.

Cloud System Configuration – Often, cloud services offer many "options" to configure security to meet the needs of diverse groups of cloud customers. However, in order to activate these options, the cloud customer must configure the system appropriately. Auditors need to pay special attention to the "configurations" that the cloud customer has made and audit these configurations and their security implications. In addition, these "configurations" need to be managed by the cloud customer in accordance with the CM (Configuration Management) family of controls.

Identity Management – Auditors need to pay special attention to the techniques used for user authentication and the assurance level of the digital identities – the IA (Identification and Authentication) family. Every cloud system user is a "remote" user authenticating over a shared medium. Thus, it is critical to utilize multi-factor authentication mechanisms leveraging digital identity credentials with assurance commensurate with the criticality of the cloud application.

Key Management – For cloud systems that store PII (personally identifiable information) or other sensitive data, the cloud customer must demonstrate that the data is encrypted at rest and in transit and that the encryption keys are managed in a manner commensurate with the risk of exposure of the data. For example, for highly sensitive data, the encryption keys should not be managed by the same cloud service provider that provides the storage service.

Incident Response and Contingency Planning – The cloud customer must have an incident response plan that delineates actions to be taken when a possible event occurs on their cloud system implementation. Further, the auditor needs to locate and review the cloud customer’s contingency plan.

Risk Assessment – The cloud auditor needs to find and review a risk assessment of the cloud system from the cloud customer’s perspective. In other words, the cloud customer needs to have conducted a comprehensive analysis of the risks of the cloud-based information system from its own business and mission context. The cloud auditor needs to ensure that the risk assessment was adequately done, the risks have been categorized and that the high and moderate impact risks have been addressed through specific corrective actions.

Continuous Monitoring – Since a cloud-based information system relies on the security posture of its constituent cloud service(s), the cloud customer must demonstrate that continuous monitoring of the security status of the cloud service is occurring and analysis is conducted of any service changes that might have security implications. This would include obtaining vulnerability analysis and penetration testing reports from the cloud service provider and reevaluation of the cloud customer’s risk assessment as the business or mission context evolves.

In some ways, the security assessment of a cloud-based information system and a hosted information system share many similarities. However, it is the differences that drive where the security auditor needs to prioritize attention in order to yield the best results and identify the most impactful and potentially devastating risks for the cloud customer’s organization.

I welcome your thoughts and suggestions. To contact me directly, please email sarbari@electrosoft-inc.com.