Recommended Risk Responses for Cloud Computing

Elaborates on recommended risk responses for some of the more significant cloud-related risks

Risk - Unauthorized cloud activity

Risk Response – Cloud policies and controls

Organizations should have policies to establish controls to prevent and detect the unauthorized procurement and use of cloud services, regardless of management's position on venturing into cloud computing. Due to the low cost of initiating cloud services relative to traditional technology purchases, current controls such as expenditure limits may not trigger appropriate attention from management.

Risk – Lack of transparency

Response – Assessments of the Cloud Service Providers control environment

Completing a high-quality and thorough risk assessment of a Cloud Service Providers environment can be challenging when the desired information is incomplete or difficult to obtain. In most cases, a Cloud Service Providers (CSP's) internal control environment is not completely visible to its customers.

Security, compliance, data leakage, and data jurisdiction

Response – Data classification policies and processes

While an organization cannot control exactly where its data is stored when using a public or hybrid cloud deployment model, it can control the type of information that resides in the cloud. From a risk management perspective, it is critical for any organization using public or hybrid cloud computing solutions to have effective data classification policies and processes in place.

Risks – Transparency and relinquishing direct control

Response – Management oversight and operations monitoring controls

In the public or hybrid cloud models, management transfers partial or complete direct control to the Cloud Solution Providers (CSP). In most situations, the CSP is focused on providing a stable and secure platform that meets the control requirements of its customers from a macro perspective. The CSP's solutions are not likely to satisfy every unique need of every cloud customer. It is the responsibility of management to assess the CSP's cloud solution in detail and implement additional controls so that the CSP's cloud solution meets all of the organization's requirements.

Risks – System Failure and High-Value Cyber-Attack

Response – Incident management

An organization needs to evaluate its CSP's capability to provide adequate incident response in addition to its own incident response procedures for system disruption and data theft scenarios.

Risk - Noncompliance with regulations

Response – Monitoring of the external environment

Management needs to monitor for changes in the external environment that would affect its own operations and the operations of its CSP. Changes to regulations or telecommunication providers may have a significant impact on how cloud computing can be used.

Risk – Vendor lock-in

Response – Preparation of an exit strategy

The more an organization uses a CSP's solution and the longer it uses the solution to support its operations, the more it depends on the CSP. Nothing lasts forever; it would be prudent for management to anticipate the future need for changing CSP vendors or moving off a cloud solution. Consequently, management should develop an exit strategy or contingency plan as part of its overall cloud strategy.

Risk – Noncompliance with disclosure requirements

Response – New disclosures in financial reporting

New disclosures may be required of publicly traded companies that rely on CSPs to support their critical business processes. In light of cloud computing solutions' potential impact on business operations and other risk factors, public companies need to remain aware of the disclosures they are required to make as part of their regulatory compliance and transparency obligations.