Kevane
Grant Thornton

Advisory

Businesses

Cloud security

Internal audit in the cloud

August 17, 2021

The critical role of internal audit in cloud security.

As organizations increasingly migrate to and rely upon cloud-based solutions, internal audit (IA) is uniquely positioned to play a critical role in the adoption of a cloud security program. IA's independence and objectivity can provide insights that enhance the ability for management and the board to oversee and control risks. IA bolsters cloud security by:

- assessing cloud security strategy and its alignment with risk and compliance
- understanding cloud security architecture, service types and associated risks and challenges
- identifying areas for improvement and communicating them to the board and management
- collaborating with the cloud service provider, IT, IS and leadership to translate enterprise risk management objectives

Cloud migration and related cybersecurity risks

Cloud computing has seen rapid adoption because of its speed, agility, and affordability. Benefits include a scalable infrastructure, flexibility in access to computing resources and reduced expenses associated with maintaining infrastructure like data sources, network components and, in some cases, even physical data centers.

However, the cloud also presents challenges. Studies suggest that more than 70% of companies had a cloud data breach in the previous 12 months, which has intensified the need for cloud security. A Sophos News survey revealed that organizations have been confronted with a variety of cloud data breaches. About 34% faced a malware attack, 29% had exposed data and 28% suffered a ransomware strike.

How IA provides perspective on cloud security

IA plays a critical role in assessing and enhancing your cloud security by:

- helping management understand cloud security architecture, with associated risks and challenges
- identifying areas for improvement and communicating them to management and the board
- supporting collaboration among the cloud service provider, IT, IS, and leadership

IA's assistance is also vital in helping to bring leading practices to a cloud security strategy, with a focus on the risk and control elements primarily driven by people, process, and technology:

People

- address risks from a lack of skilled cloud security experts
- identify key dependencies on the cloud service provider and critical third-party providers
- evaluate clearly defined roles and responsibilities, ensuring that risks are collectively mitigated

Process

- evaluate alignment of cloud security against business goals and objectives
- assess non-standard processes introduced through migration to the cloud
- evaluate processes for risk mitigation as responsibilities transition from one business function to the other
- examine adoption of cloud controls, and how they impact risk and compliance efforts

Technology

- address risks related to privilege access, data storage, and security
- evaluate risks that protect against shared responsibilities from third-party service providers that provide cloud services

Focus on these cloud security areas

When your organization has accepted its responsibility to ensure strong cloud security, it can move forward to develop a program that identifies key focus areas and an action plan to audit those functions. Concentrate on the most important areas, including:

- **cloud program governance**: Policies, procedures and risk-based planning and assessment; for compliance with standards, regulations, legal, contractual, and statutory requirements
- **policies and procedures**: Identification and assessment of how identity inventory, password policies, and other information is managed
- **application security**: Secure application design and development, such as access code, logic, and secure coding practices
- **data security**: Data inventory, classification, storage, ownership, and privacy
- **key management and encryption**: Policies, procedures, roles and responsibilities, and encryption requirements on classified data

Management needs to ensure that the cloud security program is built into the overarching enterprise resiliency architecture. That means, environment aside, you need to ensure you are following the security controls and requirements that can help reduce the risk to your organization.

A strong cloud security audit program must develop a "cadence," or a regular review cycle of cloud security, configuration, and other factors. In addition to an annual audit, cloud security should be reviewed with each change in strategy or with the introduction of a new application. As the cloud strategy evolves and major applications are being moved to the cloud, it's important to perform a pre-implementation review.

Cloud security isn't optional

Creating a strong cloud security program requires identification of not only key IA focus areas, but also a thorough understanding of your operational objectives, risks, and processes. It also requires the integration of program enhancements to prepare for inevitable risks

Grant Thornton library articles:
[Internal audit in the cloud]

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.

Marta Rodríguez
Advisory Senior Manager
E marta.rodriguez@pr.gt.com

Neysha Otero
Advisory Manager
E neysha.otero@pr.gt.com

Jorge Paredes
Advisory Manager
E jorge.paredes@pr.gt.com

Jorge Oquendo
Advisory Manager
E jorge.oquendo@pr.gt.com

Kevane Grant Thornton

grantthornton.pr

DISCLAIMER: This update and its content do not constitute advice. Clients should not act solely on the basis of the material contained in this publication. It is intended for information purposes only and should not be regarded as specific advice. In addition, advice from proper consultant should be obtained prior to taking action on any issue dealt with this update. Information provided in this publication may change in the future and such change may be applied retroactively. Kevane Grant Thornton LLP does not assume the responsibility to update this communication if the applicable laws change.