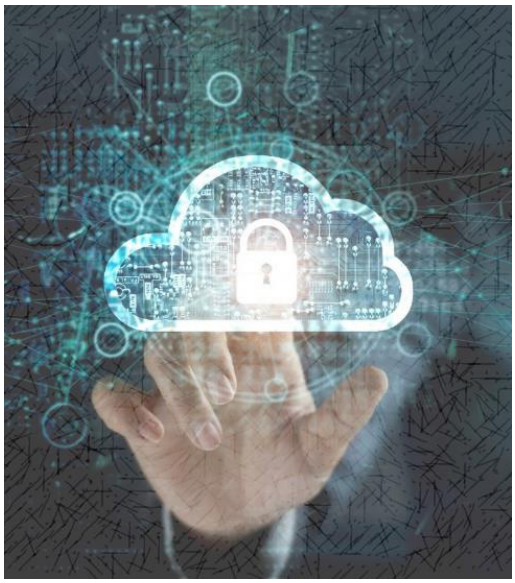
IIA Bulletin

The Institute of Internal Auditors

Perspective for internal auditors on today's most urgent issues

August 2019

Cloud Security, Insider Threats, and Third-Party Risk



Yet another major bank is in the news because of a data breach, the kind that not only endanger the personal information of millions of consumers, but also undoubtedly damage organizational reputations. The breach also will fuel intensified scrutiny from boards and increase shareholder and public demand for accountability. But organizations are not helpless. There is much they can do to mitigate cyber risks and deter and detect attacks, and internal audit must position itself to help.

Internal audit leaders should have a strong understanding of their organizations' cloud security controls and be prepared to educate their boards and audit committees.

10 QUESTIONS CAES SHOULD BE READY TO ANSWER

While the following list of questions is not exhaustive, it provides a strong beginning to the information CAEs should be able to provide boards and audit committees about cloud security, insider threats, and third-party risks.

01. Does the organization rely on cloud services? What does that mean?

02. What sensitive information does the organization house in the cloud?

03. Is there an inventory of all the access points for customer data?

04. What steps does the organization take to ensure data in the cloud is secure?

05. Who else has access to data – vendors, consultants, other outside personnel/organizations?

06. Is cloud-related exposure included in the organization's risk assessment, and, if so, what are the biggest cyber risks?

07. How are insider threat risks assessed, managed, and monitored?

08. How are cloud vendors/hosts risks managed from a third-party risk management perspective?

09. What is internal audit's role in evaluating cloud programs, and does the organization have a contractual right to audit its data in the cloud as well as the interfaces between its web applications?

10. Does the audit activity have the knowledge and resources required to perform assurance engagements including complex cybersecurity risks?

IIA Resources

GTAGs

- *Information Technology Outsourcing.*
- *Assessing Cybersecurity Risks*
- *Auditing Insider Threat Programs*

Practice Guides

- *Auditing Third-party Risk Management*
- *Engagement Planning: Assessing Fraud Risks*

INTERNAL AUDIT FOUNDATION™

Internal Audit Foundation

- *The Future of Cybersecurity in Internal Audit*

Training/CPE

- *Auditing Third Party Risk*

IIA Global Website

- *The IIA Cybersecurity Resource Exchange*

ABOUT THE IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla. For more information, *visit www.theiia.org.*