Grant Thornton

Grant Thornton and the Institute of Internal Auditors

A roadmap to auditing cloud security

Executive summary

As organizations expand into hybrid and multi-cloud environments, the speed of adoption often outpaces the maturity of security programs. This issue of Global Best Practices examines how internal audit can strengthen assurance in an era defined by AI-powered workloads and complex third-party ecosystems. It highlights practical strategies for closing the cloud security gap, including unified visibility, stronger identity governance, and proactive risk management. Learn how chief audit executives can build the expertise and frameworks needed to secure agile operations in the cloud era.

Introduction

The adoption of cloud and artificial intelligence (AI)-powered solutions has become a competitive necessity and a source of new risk. Today, most organizations operate in hybrid- and multi-cloud environments, layering on complexity as they integrate innovative technologies and third-party providers. Many organizations struggle to keep pace with the evolving threat landscape.

Recent industry research and practitioner surveys reveal a widening gap between the speed of cloud adoption and the maturity of security programs. Compounding this challenge is a persistent skills gap: Internal audit functions and cybersecurity professionals, alike, report difficulty in developing and maintaining the expertise needed to assess and manage complex, multi-cloud architectures and AI-driven workloads.

This Global Best Practices explores the essential elements of a modern cloud security internal audit program. It offers practical recommendations for chief audit executives to reset their strategies — emphasizing unified visibility, robust identity governance, and proactive risk management as the foundation for secure, agile business operations in the cloud era.

When conducting a cloud security audit, internal audit must evaluate the company's cloud strategy, architecture, and operating environment. This includes distributed responsibilities between the organization and service provider, as well as within the organization, for provisioning tenets and migrating software to the cloud, along with product, application, and data development, maintenance, and security aligned to evolving cybersecurity threats. An effective cloud security internal audit program identifies key opportunities and challenges, defines internal audit's role within the cloud environment, and applies agile risk management and testing to develop and sustain a robust cloud security program.

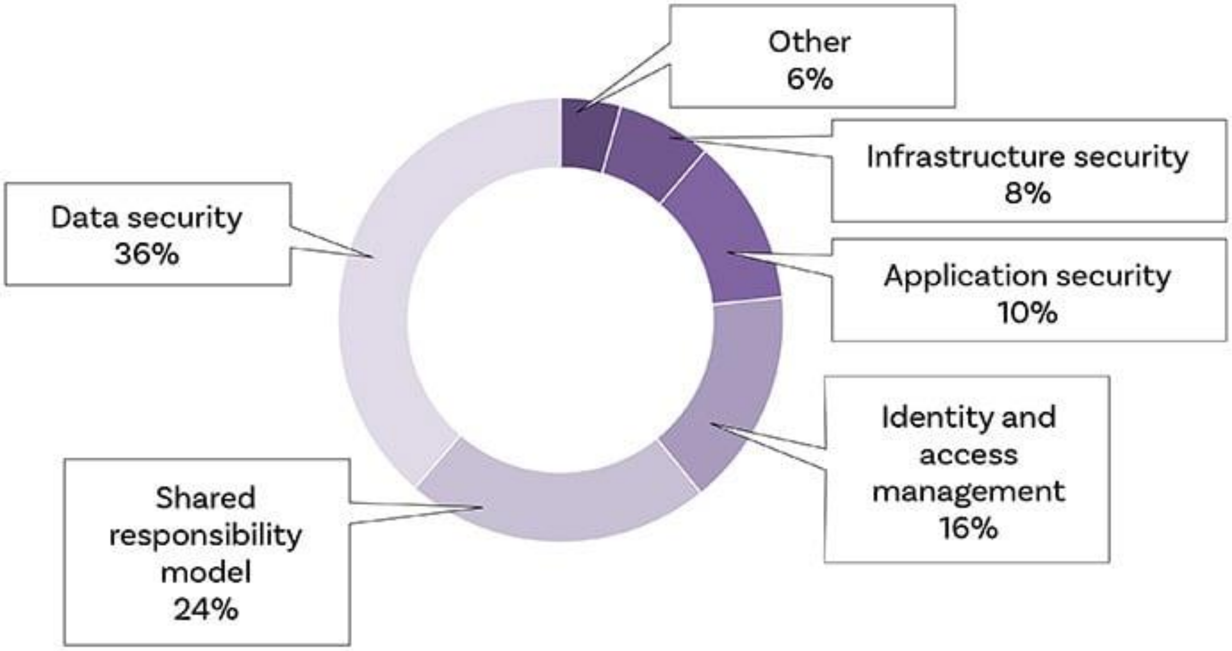
Challenges in cloud security audits

A cloud environment presents tremendous opportunities and several risks. Internal auditors must understand the environment from both a functional and technical perspective, including configuration management, says Vikrant Rai, managing director, Risk Advisory, at Grant Thornton Advisors LLC.

Common challenges include:

- Limited/informal governance and understanding of the shared responsibility model within the organization and the cloud service provider.
- Suboptimized use of available security tools and configurations.
- Credential “sprawl” as unmanaged user permissions and credentials accumulate.
- Limited visibility into data flow.
- Weak access controls.
- Insecure Application Programming Interface (API) integration.

In a recent Grant Thornton webinar on cloud security audits, a survey of approximately 1,200 attendees indicated that data security and shared responsibility were the biggest challenges.



Understanding the complexity of a cloud environment can be challenging. Internal audit needs to ensure the security and transparency of roles, capabilities, and other factors as organizations integrate existing and new technology, solutions, and providers.

"Due to the immense computational demands, high data throughput, and specialized hardware requirements of modern AI workloads, traditional infrastructure or even a single cloud environment no longer meets the needs," Rai says. "This has further accelerated the adoption of a complex cloud computing environment."

> The global cloud computing market is projected to reach approximately $2.3 trillion by 2030, growing from an estimated $752 billion in 2024. The expected compound annual growth rate from 2025 to 2030 is 20.4%.
>
> Source: Grand View Research

Technological advancement and rapidly changing service automation adds complexity and requires internal audit to leverage advanced technical test methods to audit cloud security programs, including cloud strategy, architecture, and the operating environment. Grant

Thornton's cyber risk internal audit team has identified three areas of audit focus and the challenges they present.

Cloud Program Governance

- **Transparency & Ownership** – There is often limited governance which is key to a successful cloud enabled business.
- **Multiple environments and shadow IT** – Unmanaged IT can spiral quickly out of control due to a distributed cloud model.
- **Shared responsibility model** – Lack of clearly defined roles and responsibilities between Cloud Service Providers (CSPs) and Cloud Service Customer (CSC) can leave gaps in overall cloud security posture.

Data Security Posture Management

- **Limited visibility into data assets** - Scalability in cloud environment can make it challenging for organizations to have visibility into data assets (e.g, shadow data stores, forgotten databases).
- **Inaccurate data flows leading to risk of regulatory non-compliance** – Cloud hosted data assets are at a risk of increased exposure as more linked data is migrated to the cloud.
- **Unknown attack paths** - There is a significant risk of undiscovered weaknesses in identity, access, misconfigurations and vulnerabilities that lead to data breaches and Cyber incidents.

Cloud Security Posture Management

- **Challenges with exponential growth** – Managing security in cloud is a continuous battle that requires a strong foundational security architecture.
- **Auditing key cloud security functions** – Auditing services/functions such as access management, application security, encryption & key management can be technically challenging to audit.
- **Limited visibility of cloud resources** – There is limited visibility and control of cloud resources, fragmented approaches to detecting and preventing misconfigurations leading to increased number of security incidents and inability to maintain compliance.

Elements of a cloud security audit

Internal audit can help organizations maintain strong cloud security posture management (CSPM) and data security posture management (DSPM). “It’s crucial for management to establish a process that maintains control over security posture in a changing environment,” Rai says. “For a comprehensive assessment, internal audit should evaluate the design and operating effectiveness of the procedures and controls related to cloud strategy, architecture, and operating environment leveraging established frameworks.” (See “Cloud Security Frameworks.”)

> 76% of organizations have at least one public-facing cloud asset that enables lateral movement, which can allow attackers to reach high-value targets.
> 32% of cloud assets are neglected, either running unsupported operating systems or going unpatched for over 180 days. Attackers can use them to broaden their attack surfaces.
> 38% of organizations have databases with sensitive data that are exposed to the public.
>
> Source: Detect, Prioritize, Annihilate: Hunting Threats in the Age of Relentless Risk, Orca Security 2025 State of Cloud Security Report

Cloud Program Governance A cloud security audit program should begin with an understanding and assessment of governance and strategy — management’s approach, roles and responsibilities, policies, and third-party oversight — while also considering applicable federal, state, and local regulations. “The security team cannot secure a cloud environment if there is improper governance or it lacks a cohesive strategy,” says Rohan Singla, chief information security officer and head of IT at ChargePoint, an electrical equipment manufacturer. As part of this effort, internal audit should determine whether the organization has an established cloud security strategy and implementation roadmap and how often it is updated.

Another important aspect of cloud security is understanding how it aligns to the organization’s overall security and privacy strategy and posture. Determining how cloud security supports the achievement of organizational goals and objectives should be considered.

Determining Responsibility The shared responsibility model sets forth responsibilities held by the cloud service provider and customer — including the customer’s approach for shared responsibilities within the organization — in areas that can include hardware, infrastructure, data, applications, operating system, network controls, and access management. Cloud security audits should determine whether respective responsibilities are documented, understood, and performed.

The ultimate responsibility for risk management and compliance lies with the cloud service *customer*. Internal audit should determine if the organization obtains and evaluates cloud service provider system and organizational control (SOC) reports to evaluate the control environment.

Cloud Security Posture Management (CSPM) "Organizations must ensure that good security practices are built into cloud software, enabling appropriate implementation and management," Rai says. While cloud technology platforms often provide tools and services to help manage cloud security posture, including identifying and addressing vulnerabilities, it remains the customer's responsibility to ensure those services and tools are appropriately configured and leveraged. Internal auditors should understand how the organization, in partnership with its cloud service providers, monitors and manages cloud security risks associated with the cloud deployment model (SaaS, IaaS, PaaS).

An initial step when assessing CSPM is to evaluate monitoring activities performed by the cloud customer and service provider over the cloud environment to determine if the scope and boundaries address the current cloud implementation. Consideration should be given to the capacity and capabilities of those responsible for monitoring to ensure potential risks are identified, escalated, and responded to timely and appropriately based on criticality. In subsequent phases of the audit program, internal auditors can evaluate security processes and configurations, and then data protection and management within the cloud environment, Rai says.

Data Security Posture Management (DSPM) "If you don't have appropriate data governance and adopt a defined framework, you may expose yourself to several data security issues, such as integrity, unauthorized access, and availability," says Aadesh Gandhre, managing director and general auditor at DTCC, which provides clearing, settlement, and trade reporting services to financial market participants. As a result, cloud and data security "need to be integral to the organization's response posture."

When businesses transfer data from their in-house data centers to the cloud or from one cloud platform to another, the security of that data may be overlooked, according to Rai. Companies must be able to identify the structured and unstructured datasets involved and evaluate the controls that will protect data privacy and confidentiality when it is at rest and in motion. Data should be:

- Accessible to authorized users when needed.
- Protected so that data integrity is ensured.
- Managed in compliance with applicable laws and regulations.

Other essential considerations in a cloud security audit include:

- **Identity and access management.** This encompasses issues such as encryption and key management. Some organizations use multiple cloud environments, Singla notes, so internal auditors should consider whether the organization has a defined strategy for authenticating users and what guidelines are involved.
- **Threat detection event monitoring.** Gandhre says AI tools can be used to enhance necessary log analysis.
- **Third-party risk management.** This includes addressed risks associated with the shared responsibility model.
- **Logging and monitoring.** Key considerations here are whether critical alerts — notifications of threats or suspicious activity in a cloud environment — are being logged and how they are addressed, Singla says.

Cloud security frameworks

Internal auditors have several choices when considering the best framework to audit against in a cloud security audit, including:

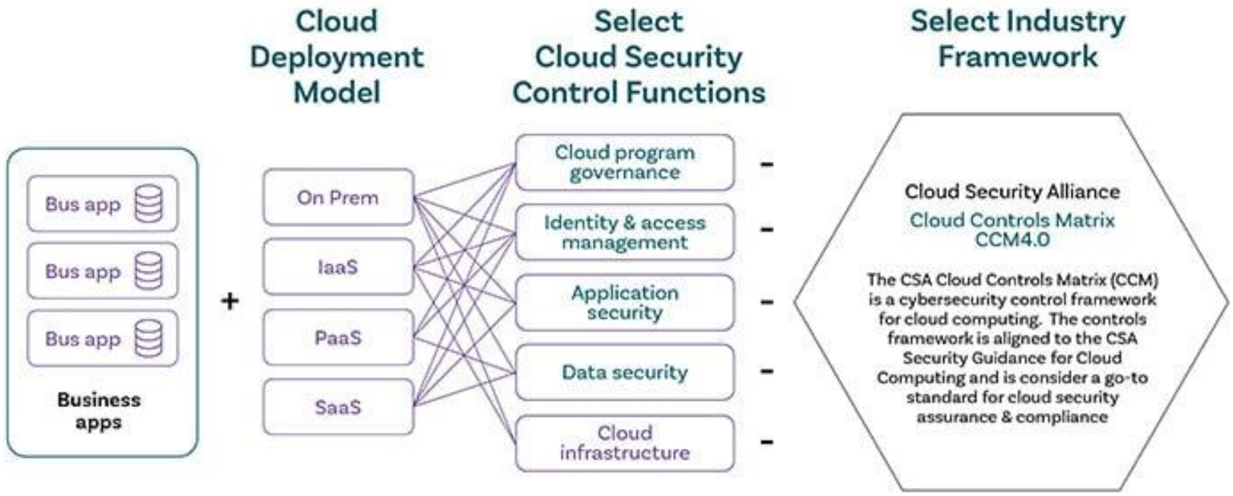
- The CSA Cloud Controls Matrix.
- The NIST Cybersecurity Framework.
- The Amazon Web Services Cloud Adoption Framework.
- The European Securities and Markets Authority Final Report on the Guidelines on Outsourcing to Cloud Service Providers.
- ISO/IEC 27000 family of standards on information security management.

An assessment of cloud security should be a key component of internal audit plans, notes Gandhre, whose company conducts continuous monitoring as frequently as monthly to identify emerging security issues.

Consistency and comparability

Understanding business applications and categorizing them by cloud providers, deployment, and service model (e.g., SaaS, IaaS, PaaS) helps identify the appropriate security controls from relevant frameworks that can be leveraged for control testing. This approach can then be used to drive consistency and comparability when evaluating security controls across the applications in the cloud.

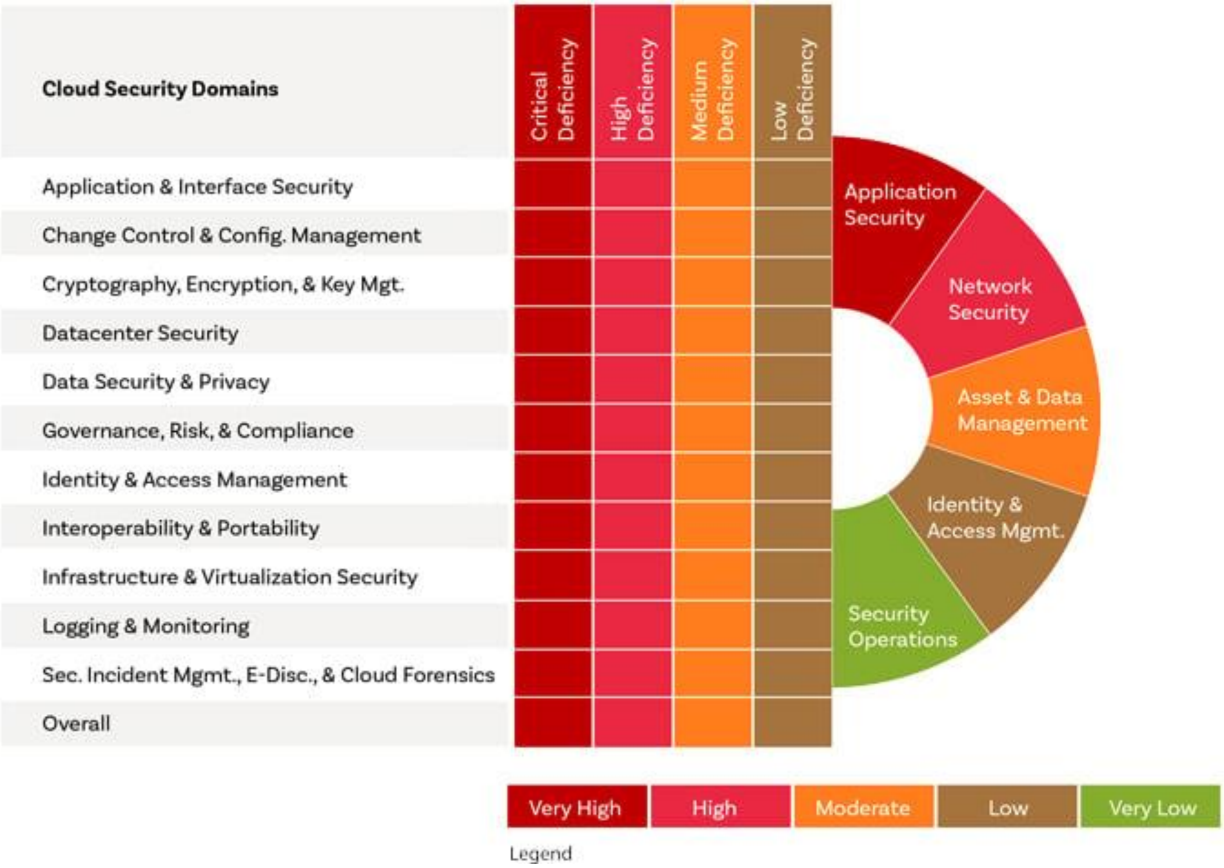
The IIA Global Technology Audit Guide (GTAG), Auditing Identity and Access Management, 2nd Edition, describes key terms and how to approach an audit engagement to ensure the organization's identity and access management protocols mitigate potential security risks. It enables internal auditors to provide assurance that controls for managing access to IT resources are well designed and effectively implemented.



The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing. The controls framework is aligned to the CSA Security Guidance for Cloud Computing and is consider a go-to standard for cloud security assurance & compliance

Evaluate Controls Against CIS Benchmark / Selected Framework

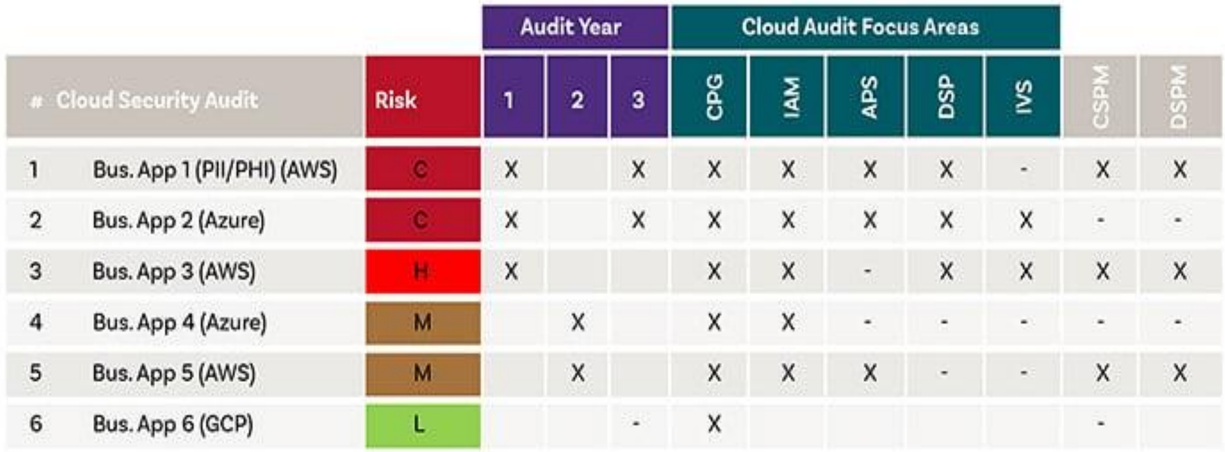
- Provide detailed current and targeted maturity models with peer benchmarking.
- Deliver cloud security assessment based on identified improvement opportunities.



Cloud Security Domains	Critical Deficiency	High Deficiency	Medium Deficiency	Low Deficiency
Application & Interface Security				
Change Control & Config. Management				
Cryptography, Encryption, & Key Mgt.				
Datacenter Security				
Data Security & Privacy				
Governance, Risk, & Compliance				
Identity & Access Management				
Interoperability & Portability				
Infrastructure & Virtualization Security				
Logging & Monitoring				
Sec. Incident Mgmt., E-Disc., & Cloud Forensics				
Overall				

Creating a multi-year cloud security audit program starts with understanding the core business environment. Internal auditors must first evaluate business priorities and existing and future business applications that are expected to be migrated to the cloud environment. A pre- and post-cloud migration strategy should be considered to enable secure, on-going business operations.

Multi-Year Cloud Security Audit Plan (Sample)



			Audit Year			Cloud Audit Focus Areas						
#	Cloud Security Audit	Risk	1	2	3	CPG	IAM	APS	DSP	IVS	CSPM	DSPM
1	Bus. App 1 (PII/PHI) (AWS)	C	X		X	X	X	X	X	-	X	X
2	Bus. App 2 (Azure)	C	X		X	X	X	X	X	X	-	-
3	Bus. App 3 (AWS)	H	X			X	X	-	X	X	X	X
4	Bus. App 4 (Azure)	M		X		X	X	-	-	-	-	-
5	Bus. App 5 (AWS)	M		X		X	X	X	-	-	X	X
6	Bus. App 6 (GCP)	L			-	X					-	

"Much goes into defining a cloud security audit program, and maturing it can take time," Rai says. He recommends organizations take a phased approach, beginning with evaluating governance components. A measured approach enables internal audit to quickly understand and assess governance, operating model(s), and the shared responsibility model.

"It's important to break the large topic of cloud security into sizable portions by cloud environment, topical area, or the intersection of the two when building your cloud security audit program, making the audits manageable in scope and giving management time to implement, enhance, and enforce controls," he says. Auditors can use established frameworks to evaluate the applicable maturity elements and controls, whether they are dealing with governance, configuration, or data protection elements.

Internal audit's role

Internal audit is responsible for assessing governance, risk management, and controls necessary to mitigate cloud security risk and advance its maturity, providing transparency and support to the board and senior management.

Examples of the many areas in which internal audit can play an important role include:

- Assess the organization's implementation of CSPM and DSPM security solutions, policies around them, and whether they are aligned to the organization's needs and leading practice.

- Interview leadership on issues such as major updates to security strategy, architecture, or operating environment.
- Assist management with identifying internal controls that management can implement to develop a strong security baseline and guidelines.
- Assess whether third-party controls, policies, and procedures are aligned with company expectations.
- Encourage management to ensure the right individuals are involved in reviewing and negotiating contracts. Contractual considerations that are paramount to protecting the organization and working productively with a provider include, but are not limited to:
    - A commitment to issuing SOC reports within a defined timeframe.
    - Formal service level agreements for identifying, escalating, and responding to threats within an agreed upon timeframe based on severity.
    - Clear articulation of responsibilities between service provider and customer.
    - Understanding the service provider's rules on data ownership and access, audit rights, etc.
- Perform advisory engagements to provide management with leading practices based on widely adopted frameworks.

An integrated approach

Much of the technology landscape is shifting toward the cloud, Rai notes, with many AI and machine learning solutions being built on the cloud. "The challenges will continue to grow," he says.

Auditing cloud security is a journey, according to Gandhre, and collaboration is important. "Just having a separate program for cloud security doesn't cut it," he says. Cloud security should be aligned with the internal audit risk assessment and the organization's enterprise risk management framework.

Internal audit should be involved in cloud security considerations from the outset so that auditors can ask questions and offer advice before decisions are made, including how risks are assessed, Gandhre says. "Independence doesn't mean isolation."

This paper was a collaboration of Grant Thornton and the Institute of Internal Auditors.

Contacts:

Adam Ross

Principal, Risk Advisory Services

Grant Thornton Advisors LLC

+1 215 558 6530

Vikrant Rai

Managing Director, Internal Audit Cybersecurity Practice

Grant Thornton Advisors LLC

+1 212 624 5212