NIST Interagency Report
NIST IR 8613 ipd

# Multi-Cloud Architecture Challenges

*Security and Compliance Implications*

Initial Public Draft

Michaela Iorga
Ned Goren
Joyce Hunter
Chris Carpenter
Brian Ruf
Sanjiev Chattopadhya
Katie Digon
Larisa Gabudeanu

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8613.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

**NIST Interagency Report**
**NIST IR 8613 ipd**

# Multi-Cloud Architecture Challenges

*Security and Compliance Implications*

Initial Public Draft


Dr. Michaela Iorga
Nedim Goren
*Computer Security Division*
*Information Technology Laboratory*

Brian Ruf
*Ruf Risk LLC*

Chris Carpenter
*Cloud Security SME*

Joyce Hunter
*Mission Critical Inc.*

Sanjiev Chattopadhya
*Cloud Security SME*

Katie Digon
*Cloud Security SME*

Larisa Gabudeanu
*Cloud Security Alliance*
*Romanian Chapter*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8613.ipd

August 2026




U.S. Department of Commerce
*Howard Lutnick, Secretary*

National Institute of Standards and Technology
*Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology*

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.



**Publication History**
Approved by the NIST Editorial Review Board on YYYY-MM-DD
Supersedes NIST Series XXX (Month Year) DOI

**How to Cite this NIST Technical Series Publication**
Iorga M, Goren N, Hunter J, Carpenter C, Ruf B, Chattopadhya S, Digon K, Gabudeanu L (2026) Multi-Cloud Architecture Challenges: Security and Compliance Implications . (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8613 ipd. https://doi.org/10.6028/NIST.IR.8613.ipd

**Author ORCID iDs**
Michaela Iorga: 0000-0001-7880-6045
Nedim Goren: 0009-0009-3578-2958
Joyce Hunter: 0009-0009-0759-8766
Chris Carpenter: 0009-0001-2183-8422
Brian Ruf: 0009-0004-1920-5353
Sanjiev Chattopadhya: 0009-0007-6689-6830
Katie Digon: 0009-0002-6815-4973
Larisa Gabudeanu: 0000-0002-2562-5344

**Public Comment Period**
August 21, 2026 – October 5, 2026

**Submit Comments**
ir8613-comments@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

## Abstract

Working group participants submitted challenges, which were aggregated and reviewed. The challenges were first categorized as either security- or authorization-related, and then as functional or technical. Multi-cloud environments present unique security challenges arising from using multiple CSPs and/or CSOs, each with their own security models, tools, configurations, and shared responsibility frameworks. Authorization in a multi-cloud environment introduced challenges that differed from those in a single-system ATO process. Authorizations depend on clearly defined system boundaries, comprehensive security documentation, and the consistent enforcement of controls. In a multi-cloud environment with multiple Cloud Service Providers (CPSs) providing services to the Cloud Service Consumer (CSP), it may be difficult to identify system boundaries, network architecture, and security processes due to differing systems or proprietary information.

## Keywords

Analysis; authorization; authorization challenges; Authorization to Operate (ATO); cloud service customer (CSC); cloud service provider (CSP); multi-cloud; multi-cloud architecture; security challenges; system security plan.

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

## Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: ir8613-comments@nist.gov

## Table of Contents

## List of Figures

## Acknowledgments

The authors of this document thank all of their peers for contributions to the research, discussions, and documentation that made this publication possible: Austen Bryan, Defense Unicorns; Annie Sokol, NIST (retired); Nida Davis, Microsoft; and Ed Kandel, Warner Bros. Discovery.

## Executive Summary

This NIST Interagency Report (IR) by the NIST Multi-Cloud Security Public Working Group (MCSPWG) identifies, categorizes, and analyzes the security and compliance challenges that are unique to — or significantly amplified by — multi-cloud architectures. The analysis relates challenge areas to existing NIST guidance (e.g., SP 800-145 [1], SP 800-207 [1], SP 800-53 [3], SP 800-37 [7]) and highlights areas where additional community research could meaningfully reduce risk.

The MCSPWG identified 23 consolidated challenge areas that represent novel friction points and architectural misalignments that emerge when orchestrating control across autonomous cloud silos. The most significant structural challenge areas are:

- Security-significant differences in cloud-native services across providers
- Organizational logistics and staffing complexity across heterogeneous environments
- Difficulty in implementing centralized security capabilities across provider boundaries

These structural gaps are most acute in five areas where providers need alignment: (1) identity and access management, (2) telemetry and logging, (3) configuration and change management, (4) data protection, and (5) compliance and authorization. The challenges arising at these seams directly affect the confidentiality, integrity, and availability of multi-cloud workloads and complicate adherence to recognized security principles, including zero trust, least privilege, defense in depth, and authorization to operate (ATO).

# 1. Introduction

As cloud service offerings (CSOs) and architectures have grown in both capability and complexity, cloud service consumers (CSCs) increasingly meet their business and mission requirements by combining services from multiple cloud service providers (CSPs). In this NIST Interagency Report (IR), the NIST Multi-Cloud Security Public Working Group (MSCPWG) aggregate, categorize, and discuss the security challenges posed by running workloads in multi-cloud environments that are distributed between private, community, and public clouds. This includes maintaining confidentiality, integrity, and availability for workloads that span multi-cloud environments while adhering to recognized security principles, such as zero trust, least privilege, defense in depth, authorization, and certification.

This document also distinguishes between a *multiple-cloud strategy* and a *multi-cloud service* (i.e., provider-packaged and managed). In a multiple-cloud strategy, a CSC (e.g., enterprise, developer) intentionally orchestrates a cloud ecosystem using services from different CSPs (e.g., AWS for compute, Google Cloud for AI/ML, Azure for identity services). The CSC is responsible for interconnectivity, security policies, governance, and data movement across the various cloud environments. In contrast, a multi-cloud service refers to a provider-packaged and managed solution in which integration and cross-cloud coordination are handled by the provider rather than the consumer. Architectures that combine multiple CSOs from the same CSP or that stack software-as-a-service (SaaS) or platform-as-a-service (PaaS) offerings on infrastructure managed by a single hyperscaler are not considered multi-cloud architectures under this definition.

## 1.1. Document Goals

The primary objectives of this document are to:

1. Identify core security challenges that may arise within multi-cloud offerings in which increased complexities create challenges that are not found in single cloud architectures or CSC-orchestrated cloud ecosystems
2. Promote collaboration across industries to explore and prioritize identified challenges
3. Support future work to develop best practices, reference architectures, and solutions that address these challenges at scale

This IR is descriptive and vendor-agnostic. It does not prescribe a reference architecture, endorse specific tools, or provide implementation guidance. Instead, it describes recurring challenge areas that are specific to multi-cloud service offerings from distinct cloud service providers as well as the implications for cloud service consumers. A multi-cloud considers any combination of deployment (e.g., private, community, public, hybrid) and service models (e.g., infrastructure as a service [IaaS], PaaS, SaaS, as defined in NIST SP 800-145 [1]). This analysis emphasizes the seams between providers where misalignments most often arise, such as identity and access, telemetry and logging, configuration and change management, data protection, and compliance/authorization. The intent is to surface a taxonomy of challenges, relate them to existing NIST guidance (e.g., SP 800-145, SP 800-207, SP 800-53/-37), and

highlight areas where additional community collaboration, reference architectures, and NCCoE practice guides could reduce risk.

While the current dataset represents a wide spectrum of challenges identified by MCSPWG, it is not intended to be exhaustive. The group anticipates that the dataset will evolve as multi-cloud adoption grows and new security architectures emerge. By establishing a shared baseline, MCSPWG aims to foster continued collaboration and iteration across both public and private sectors.

## 1.2. Audience

The primary audience for this document includes developers, architects, cyber security professionals, and risk management professionals. Other interested parties may include executives, technical leaders, and general customers of cloud services.

## 1.3. Scope

This document focuses on identifying, categorizing, and analyzing recurring security and compliance challenges that arise when organizations adopt multi-cloud solutions (see Sec. 1.1), encompassing any combination of deployment models (i.e., private, community, public, hybrid) and service models (e.g., IaaS, PaaS, SaaS), as defined in NIST Special Publication (SP) 800-145 [1].

The scope explicitly excludes:

- Single-cloud architectures or deployments limited to a single CSP
- Detailed technical configurations, operational playbooks, or specific product evaluations
- Prescriptive security control baselines or one-size-fits-all recommendations

By bounding the analysis, this IR aims to provide a structured problem statement and shared vocabulary that can inform future research, procurement, standards development, and solution design across government, industry, and academia.

## 2. Research Methodology

The MCSPWG is composed of representatives from private industry, the public sector, academia, and civil society. It is an open group, and all interested parties may participate.

Since the definition for *multi-cloud* varies across the information technology community, the MCSPWG defined the scope of this activity by reviewing the NIST and ISO definitions for cloud computing, cloud deployment models, and cloud service models and contextualizing "multi-cloud architectures" in these terms. Participants submitted challenges, which the working group vetted for inclusion. The data was aggregated and reviewed by active members of MCSPWG using the following methodology:

- Multi-cloud-specific challenges were provided by stakeholders and industry professionals.
- MCSPWG tracked and iterated the identified challenges using online collaborative documentation.
- MCSPWG held monthly meetings to discuss and categorize challenges.

After aggregation, MCSPWG evaluated and categorized each challenge as either *security*-related or *authorization*-related.[1] They were further subcategorized based on *functional* or *technical* underlying factors, and each challenge was assigned a set of attributes:

- Unique challenge ID
- Title
- Primary category (*security* or *authorization*)
- Subcategory
- Challenge description
- Outcome or benefit of overcoming the challenge

This effort identified complex, multidimensional challenges that are underrepresented in security assessments and often extend beyond the boundaries of individual organizations and technological domains. The dataset serves as both a knowledge base and a collaborative framework to help guide future research, policy, and technical development.

[1] The terms "authorization" and "authorization to operate (ATO)" are sometimes used interchangeably.

# 3. Overview

## 3.1. Multi-Cloud Architectures

SP 800-145, *The NIST Definition of Cloud Computing* [1], defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources…that can be rapidly provisioned and released with minimal management effort or service provider interaction." This foundational document outlines the following:

- Cloud deployment models:
  - Private cloud
  - Community cloud
  - Public cloud
  - Hybrid cloud
- Cloud service models, which are defined in part as "capabilities provided to the consumer" and delineate different degrees of ownership, data management, and the distribution of responsibilities between CSPs and CSCs:
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)

While SP 800-145 defines a hybrid cloud as "a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities" [1], it does not define *multi-cloud* or any variation of the term.

ISO/IEC 22123-1:2023 [8] offers formal definitions for several cloud computing deployment model terms:

- Hybrid cloud — Cloud deployment model that uses a private cloud and a public cloud
- Multi-cloud — Cloud deployment model in which a cloud service customer uses public cloud services provided by two or more cloud service providers
- Hybrid multi-cloud — Cloud deployment model in which a cloud service customer uses cloud services from a hybrid cloud and a multi-cloud
- Inter-cloud — Cloud deployment model in which a cloud service provider offers a cloud service by using one or more cloud services provided by other cloud service providers

These and other cloud taxonomy standards largely classify environments based on provider relationships and deployment boundaries, omitting service models entirely. While they are useful for describing cloud ownership and operational responsibility, these definitions do not adequately capture the architectural, security, compliance, governance, or interoperability challenges that emerge when organizations integrate multiple cloud service offerings. The

terms may conflict with each other or present different scoping, thus complicating conversations about security and authorization challenges and proposed solutions to them.

In practice, these challenges arise from differences in deployment models, service models, trust boundaries, management planes, identity systems, compliance inheritance structures, and operational dependencies, regardless of whether the offerings originate from a single CSP or multiple CSPs. CSCs strategically implement multi-cloud architectures to reduce vendor lock-in, improve flexibility, and optimize performance by taking advantage of the unique capabilities and benefits of each CSO and CSP. Through the interoperability of these cloud services, such architectures often constitute a CSO themselves in which CSCs become CSPs in their own right. These new CSOs may follow one or many of the service and deployment models described above, contributing to a cascading ecosystem of interoperability and dependency.

Given this dynamic and layered environment, the need for robust analysis of security, compliance, and governance practices in multi-cloud architectures is both urgent and ongoing. The MCSPWG's research has adopted an architecture-centric perspective rather than a provider-centric perspective to provide a working definition for *multi-cloud architecture* that better reflects the colloquial use of the term while maintaining the specificity needed to conduct research:

> A system architecture that integrates multiple cloud service offerings spanning one or more cloud service models, deployment models, trust domains, and/or cloud service providers to deliver a unified business or mission capability.

### 3.2. Defining Challenges for Multi-Cloud Architectures

Multi-cloud security and compliance challenges are not simply the sum of individual cloud provider issues. Rather, they are complex, interdependent, and often emergent due to the simultaneous use of heterogeneous CSOs. For the purposes of this report, a multi-cloud security or compliance challenge is defined as:

> Any technical, operational, policy, or governance issue that impairs or complicates the assurance of security controls, compliance obligations, or system resilience across multiple, provider-packaged while independently managed cloud services offerings.

These challenges may arise from one or more of the following gaps:

- **Lack of standardization:** Differences in how CSPs define, implement, and document access control, logging, identity federation, encryption, and compliance frameworks
- **Fragmented visibility:** Inability to gain comprehensive situational awareness across cloud boundaries due to siloed telemetry, disparate logging formats, and incompatible monitoring tools

- **Decentralized control:** Lack of centralized enforcement mechanisms for policy, configuration, or compliance, resulting in the inconsistent application of security practices
- **Interoperability barriers:** Integration of multiple CSP services that introduce architectural incompatibilities, third-party dependencies, and hidden or novel attack surfaces
- **Compliance and audit gaps:** Regulatory and authorization or certification processes hindered by the inability to obtain or generate consistent and verifiable security documentation across all participating CSPs and/or for a CSC's multi-cloud information system

These challenges require collective research, tooling, and governance strategies that recognize the inherently decentralized nature of multi-cloud ecosystems.

# 4. Multi-Cloud Architecture Challenges

The most significant challenges in securing a *multi-cloud* architecture involving multiple distinct CSPs include:

- Security-significant differences in cloud-native services across providers, including variations in cryptographic implementations, access control granularity, control inheritance models, and integration patterns
- Organizational logistics and staffing complexity across heterogeneous environments that lead organizations to maintain separate teams per provider with coordination overhead
- Increased difficulty in implementing centralized security capabilities across provider boundaries, including log aggregation, identity federation, secrets management, and policy enforcement

Consequently, satisfying the same security requirement across two provider environments may require different architectural components, configuration baselines, and compensating controls. The challenge is amplified when one CSP lacks a functionally equivalent service or when the available service does not meet the required assurance level. In assessed and authorized environments, an additional complication arises when a service falls within the authorization boundary of one provider but not the other. This discrepancy can render a service unavailable or require additional scrutiny, tailoring, or compensating controls.

Organizational complexity also increases significantly. Because each CSP's cloud-native ecosystem has distinct operational paradigms, tooling, and security constructs, it is uncommon to find personnel with deep expertise across multiple environments. As a result, organizations frequently maintain separate teams aligned to each provider. This separation introduces coordination overhead and increases the difficulty of ensuring that security controls are implemented consistently and equivalently across providers.

Centralized security capabilities present additional architectural challenges in multi-provider environments. Log aggregation and monitoring become more complex when security-relevant telemetry originates from multiple CSOs from the same or multiple CSPs, each with distinct log schemas, metadata structures, retention models, and export constraints. Hypervisor-level and provider-managed service logs may be particularly difficult to extract outside a CSP boundary. Ensuring comprehensive visibility for monitoring, correlation, and incident response across providers requires deliberate architectural design and secure cross-cloud communication pathways.

Similarly, implementing centralized identity, credential, and access management (ICAM) across multiple CSPs introduces complexity in federation, role mapping, attribute synchronization, and RBAC alignment. Differences in identity primitives, token models, and access control enforcement mechanisms complicate efforts to maintain uniform least-privilege enforcement across providers.

Secrets management is also more difficult in a provider-packaged multi-cloud architecture. Cloud-native services are typically optimized for secrets management within their own provider

boundary and are not inherently designed for cross-provider sharing. As a result, organizations may experience the duplication of secrets, increased storage locations, and greater complexity in life cycle management, rotation, and access governance.

These structural, operational, and security divergences should be considered when reviewing analysis and categorization (see Sec. 5), as they directly influence both risk posture and implementation strategy in multi-provider cloud architectures.

### 4.1. Security Challenges

Addressing data security in a multi-cloud ecosystem is paramount since the cloud service consumer's information is being distributed across a heterogeneous ecosystem. The underlying CSPs and third-party service providers involved in the multi-cloud architecture exhibit different degrees of opacity regarding their security measures and controls, which expands the potential attack surface and increases the number of administrative boundaries that data must traverse. For a CSC, this can significantly increase uncertainty in the security state of their environment and the complexity of securing their data.

While data encryption at rest and in transit is effective for securing data, managing encryption keys across multiple CSPs and third-party cloud service providers is technically challenging. Encryption key management must remain robust and synchronized across disparate CSP storage infrastructures to maintain confidentiality at rest and in transit. The CSC also faces substantial challenges in establishing persistent monitoring and security protocols for data transfers between internal CSP nodes and external replicated storage providers.

Risk management and compliance with geographically specific policies and regulations may be further complicated by geographic residency risks. Data distributed across foreign jurisdictions may become subject to local legal and judicial processes that could lead to a permanent loss of access or sovereignty.

To detect and remediate configuration drift, each underlying CSP often employs unique system configurations that are tailored to specific governance frameworks (e.g., NIST RMF and SP 800-53 security and privacy controls versus ISO/IEC 27001 and 27017). This operational fragmentation prevents a unified response to both authorized and unauthorized configuration changes, particularly when multiple systems are managed by third-party entities that may not share real-time incident telemetry due to proprietary or security-related restrictions.

Ultimately, CSCs encounter asymmetric incident response and disaster recovery environments in which provider-orchestrated policies may fundamentally diverge from the CSC's internal requirements. This lack of transparency is often total, as CSPs frequently deny the CSC the necessary administrative privileges to conduct disaster recovery activities on the specific non-CSC-related cloud systems on which their services reside.

The following subsections discuss the categories, their associated descriptions, and security-related challenges in multi-cloud environments.

### 4.1.1. Access Control

For a CSC, managing access control in a provider-orchestrated and managed multi-cloud ecosystem is complex. The following points elaborate on security-related access control challenges:

- **Policy implementation across heterogeneous systems:** It is challenging for CSCs to ensure that access control policies are implemented consistently across various CSP information systems, which may each have unique native architectures.
- **Identification of privileged (backend) accounts:** It is difficult for CSCs to identify which CSP personnel hold privileged access accounts that directly impact the consumer's specific cloud services.
- **Verification of cross-cloud user authorization:** It is difficult for CSCs to identify and verify the authorization of all user accounts across multiple CSOs from one or more CSPs involved in the multi-cloud architecture.
- **Biometric and multi-factor authentication (MFA) validation:** It is difficult for CSCs to verify whether biometric or multi-factor authentication (MFA) have been consistently employed by all participating CSPs for the specific information systems that support their cloud services.
- **Inconsistent role and duty separation:** It is difficult for CSCs to verify the CSP's roles, separation of duties, and consistent implementation across multiple CSOs when those functions are managed by different providers with different internal standards.
- **Authenticator policy compliance:** It is difficult for CSCs to verify whether the authenticator policies of every underlying CSP meet the consumer's specific security and regulatory requirements.
- **Third-party vendor access risks:** Managing security is further complicated by the need to verify the access control policies and implementations of other vendors or third-party cloud service providers that are utilized by the CSPs.
- **Increased attack surface via distribution:** Distributing data across multiple CSPs and third-party systems naturally increases the risk of unauthorized access, leaks, or data breaches.
- **Variable third-party access procedures:** Inconsistent access policies implemented by a CSP's third-party providers can lead to security gaps that result in unauthorized access to CSC information.

### 4.1.2. Vulnerability Management

A CSC may encounter significant abstraction layers that complicate vulnerability management in a multi-cloud ecosystem. The following points detail specific vulnerability management challenges for consumers:

- **Analysis of different reporting formats:** Even when CSCs receive complete vulnerability reports, it is challenging to analyze and normalize proprietary formats of vulnerability scan reports that have been generated by disparate tools.
- **Procedure standardization:** Implementing standardized vulnerability scanning procedures is difficult across multiple CSP infrastructures that may each have unique operational requirements.
- **Scanning schedule constraints:** A CSC's vulnerability scanning schedule is often constrained by the specific information system restrictions, maintenance windows, and patching cycles of individual CSPs.
- **Restricted system access:** CSCs may be unable to conduct independent vulnerability scans due to a lack of direct access to the CSP's information systems.
- **Configuration opacity:** CSPs may not allow CSCs to access the specific information system configurations of underlying CSOs, which can hinder the independent identification and/or validation of configuration-based vulnerabilities.
- **Opaque scan results:** CSPs may withhold detailed vulnerability scan results from CSCs to voluntarily or involuntarily obfuscate vulnerability data by citing concerns regarding proprietary information or backend system security.
- **Policy transparency gaps:** CSCs often lack access to the specific patch management policies and procedures implemented by each CSP.
- **Remediation coordination complexity:** It can be extremely complex for CSCs to coordinate the patching and remediation of vulnerabilities across multiple CSOs from one or more CSPs.
- **Inaccessible patching results:** Consumers may be unable to obtain vulnerability patching and remediation results for multiple CSOs from one or more CSPs.
- **Incomplete asset inventory:** CSPs may fail to provide a unified, comprehensive asset inventory that accounts for all resources across multiple CSOs.

### 4.1.3. Incident Response

The lack of control and visibility can affect incident response capabilities across a distributed environment. The following points summarize the incident response challenges that are specific to consumers in a multi-cloud ecosystem:

- **Reporting latency and information gaps:** CSPs may not send timely and comprehensive incident data to CSCs.

- **Opaque operational procedures:** CSPs frequently withhold detailed incident response policies and procedures for their CSOs by citing proprietary or security concerns.
- **Monitoring tool blind spots:** Consumers may be uninformed of the specific monitoring tools, procedures, and results used by individual CSPs to detect threats within a multi-cloud environment.
- **Unverifiable personnel readiness:** CSCs often lack access to incident response training records for the personnel who manage various CSOs.
- **Inaccessible testing results:** It is difficult for CSCs to obtain detailed information on the incident response testing procedures or the actual results of those tests from all integrated CSOs.
- **Restricted direct monitoring privileges:** Managed providers may not grant CSCs the required administrative access privileges to independently monitor their cloud services across different CSP environments.
- **Disparate event reporting:** CSCs may not receive standardized incident event information or reporting documentation because of the varied logging formats and reporting schemas used by multiple underlying providers.
- **Audit log fragmentation:** CSCs may be unable to access comprehensive audit logs, including those from external third-party services that support CSOs.
- **Alerting limitations:** CSPs may not provide CSCs with the native capability to receive direct incident alerts from all CSO components, leading to delayed situational awareness.

### 4.1.4. Architecture

CSCs are often distanced from the underlying technical details in the CSOs that comprise a multi-cloud environment, which creates significant gaps in visibility and documentation. These architectural security challenges arise can be categorized in two groups:

1. System boundary and responsibility ambiguity
    - **Restricted boundary documentation:** Providers often withhold documentation that defines the system boundary for their integrated services in sufficient detail for the CSC to effectively apply security controls.
    - **Control information gaps:** CSCs may struggle to obtain precise information from their CSPs regarding the specific security responsibilities and levels of control that they maintain within the boundary of each CSP's CSO.
    - **Increased boundary complexity:** Relying on multiple underlying CSPs and abstracted services makes it difficult for the CSC to define a clear and accurate information system boundary for their cloud assets.

2. Strategic planning and capability visibility
    - **Contingency planning obstacles:** Consumers often face a lack of access to the underlying architectural documents required to create effective, integrated contingency plans for their cross-cloud services. This includes accounting for differing recovery time and recovery point objectives (RTOs/RPOs) for each CSO, varying communication expectations across CSPs, and resource planning for availability requirements for their multi-cloud environment.
    - **Cryptographic implementation blind spots:** Managed providers may not give CSCs detailed information regarding cryptographic system capabilities or the specific implementation architecture used across multiple integrated CSOs.

### 4.1.5. Data Protection

Consumers must rely on their CSPs to ensure that security, encryption, and regulatory standards are met across all CSOs, which can lead to significant data protection challenges due to varying layers of abstraction, levels of responsibility, and capabilities. The following points summarize data protection challenges that are specific to consumers in a multi-cloud ecosystem:

- **Architectural opacity:** The CSC may struggle to obtain detailed information system architecture for integrated cloud services, which hinders the implementation of appropriate controls.
- **Mechanism identification gaps:** Due to a lack of direct access to underlying systems or detailed architecture documentation, the CSC may be unable to independently identify the specific data protection mechanisms employed by each integrated CSP.
- **Regulatory alignment conflict:** Underlying CSPs may have security control implementation requirements that fundamentally differ from the CSC's internal mandates (e.g., specific regulatory or compliance standards).
- **High dependency on CSPs:** CSCs can become heavily dependent on CSPs and third-party providers to implement and maintain security for data stored within each CSO.
- **Geographic data blind spots:** CSPs may not provide precise information regarding the physical or logical location of CSC data as it moves through the multi-cloud environment.
- **Compliance documentation barriers:** The CSC often faces challenges in obtaining information system security documentation from all providers involved in the protection of data within the multi-cloud environment.
- **Information exchange complexity:** CSPs may fail to provide formal information exchange documentation (e.g., memorandums of understanding, service-level agreements [SLAs]) for the critical connections that facilitate the transfer of CSC information.

- **Encryption standard disparity:** The encryption standards or specific implementations used by underlying CSOs may not meet the CSC's internal data protection requirements.
- **Risk of regulatory non-compliance:** Inconsistent encryption implementations across CSOs in a multi-cloud environment may fail to meet the specific regulatory requirements that govern the CSC's industry or jurisdiction.
- **Different cloud service models:** A multi-cloud environment may use multiple CSOs delivered as IaaS, PaaS, or SaaS, which each offer different levels of responsibility for the CSC to secure the CSO. This can result in unclear or inconsistent security control application throughout the multi-cloud environment.

#### 4.1.6. Contingency Planning and Disaster Recovery

CSCs must account for varying conditions across the CSPs and CSOs that comprise their environment when planning for contingency or disaster events. The following points summarize the security challenges related to contingency planning and disaster recovery in a multi-cloud ecosystem:

- **Lack of documentation:** CSPs often withhold contingency planning policies and procedures from CSCs, citing concerns regarding privileged backend information and overall system security.
- **Lack of testing evidence:** CSPs do not typically offer the results of contingency or disaster recovery plan tests to CSCs, limiting the CSC's ability to apply security controls effectively.
- **Difficulty in verifying preparedness:** CSC data may be stored across multiple CSOs from CSPs with different contingency plans (e.g., SLAs, RTOs, RPOs), which makes it challenging to verify that their multi-cloud environment's availability requirements are being met effectively.

#### 4.1.7. Configuration Management

Multi-cloud ecosystems present a range of configuration management challenges driven by limited visibility into CSPs environments, inconsistent levels of control, and variability in CSP practices. These challenges can impede the CSC's ability to verify, enforce, and maintain secure configurations across heterogeneous cloud platforms. At a high level, the primary configuration management challenges can be summarized as follows:

- **Direct verification barriers:** CSCs are often denied administrative access to CSP information systems, which prevents them from manually verifying that their cloud services are utilizing secure configurations.
- **Access to systems:** Providers frequently restrict the CSC from having sufficient access privileges to conduct independent configuration scans across the underlying systems that support the multi-cloud environment.

- **Scan result opacity:** CSCs may not receive the raw results of configuration scans conducted by the CSPs, which limits their ability to independently assess the security posture of their multi-cloud environment.
- **Change control process opacity:** It is challenging for CSCs to obtain detailed configuration change control documentation related to the specific cloud services integrated into the multi-cloud environment, such as a comprehensive configuration management plan or the specific policies and procedures that the CSPs use to manage their cloud services.
- **Unclear administrative governance:** CSPs do not often provide CSCs with clear documentation regarding system administrator roles, responsibilities, or the access restrictions applied to those making configuration changes to their CSOs.
- **Inconsistent baselines:** CSPs and CSCs may be misaligned on configuration standards and requirements, leading to inconsistent security baseline implementations throughout the multi-cloud environment.
- **Operational redundancy:** Due to the technical differences across CSOs, the CSC often requires specialized personnel and/or entire teams to implement and manage equivalent configuration changes for each CSO and/or CSP.
- **Technical heterogeneity:** The configuration of "equivalent" cloud-native services (e.g., storage, compute) is often significantly different between CSOs, which complicates the approval of changes and the timing of deployments.

### 4.1.8. Documentation

CSCs often encounter significant documentation hurdles due to the lack of direct visibility into the security compliance and inheritance details of each individual CSP. The following points summarize security-related documentation challenges within a multi-cloud environment:

- **Incomplete documentation flow:** CSCs may not receive or have the opportunity to review the complete set of information system documentation from individual CSPs regarding the specific CSOs they are using, leading to a weak or incomplete security posture.
- **Delays in critical updates:** Consumers often face challenges in receiving updated information system documentation from all involved CSPs in a timely manner, which can delay the adoption of new security features and/or prevent the CSC from addressing newly introduced security complexities.
- **Difficulty identifying inherited controls:** Within a complex managed service, it can be difficult for the CSC to clearly identify which specific security controls are inherited from which underlying CSP and consistently implement their responsibilities properly across all CSOs.
- **Inconsistent responsibility details:** The documentation regarding inheritance and customer responsibility typically differs and may conflict across each CSO, even for

controls that are commonly inherited. This can lead to operational friction, unnoticed exceptions to required security implementations, and inconsistently applied security policies.

### 4.2. Assessment and Authorization Challenges

[OMB A-130] defines an authorization (i.e., authorization to operate, authorization to use) as the official management decision given by a senior federal official to authorize the operation of an information system and explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls [6]. Authorization also applies to common controls inherited by agency information systems. The authorization is valid for a specific time period and needs to meet specific terms and conditions. The authorizing official reviews the information system security plan (SSP), security assessment plan (SAP), security assessment report (SAR), and plan of action and milestones (POA&M) and then makes a risk-based decision to either deny or grant an authorization for the information system. Following an initial authorization, there are monthly and annual obligations for maintaining such authorization, including annual reassessments.

One of the challenges with authorizations is defining the boundaries of an information system, especially in a multi-cloud environment where multiple CSOs from one or more CSPs introduce complexities in multiple different types of boundaries. Each CSO and/or CSP that comprises a multi-cloud environment may themselves be a multi-cloud environment. A CSP supporting a multi-cloud environment and the CSC to whom that environment belongs may both be consumers of the same CSO. For example, an IaaS provider supporting a multi-cloud SaaS environment may use the same security incident and event management (SIEM) service as the SaaS they support. Each CSO will have their own information system boundary, which includes:

- **Architectural boundary**, which may include infrastructure, platforms, and services [2]
- **Security boundary**, which may include information system security controls, access controls, and regulatory compliance mechanisms [3]
- **Network architecture**, which includes subnets and infrastructure devices [2][4]
- **Operational boundary**, which may include information system monitoring, auditing, and audit log capture, collection, and storage; data and information backups; disaster recovery; and incident response [3]
- **Data boundary**, which may include data and information protection and data storage, processing, and transmission between CSOs [5]

The identified challenges span 10 functional categories. Table 1 summarizes the six most security-critical categories, their relative impact score, and cross-category connection count, which measure how broadly a challenge propagates risk when left unmitigated.

643 **Table 1. [add caption]**

| Challenge Area | Impact Score | Connections |
|---|---|---|
| Access / Identity | 97 | 11 |
| Vulnerability Management | 85 | 9 |
| Incident Response | 90 | 10 |
| Architecture | 88 | 10 |
| Data / Config / DR | 82 | 9 |
| Operations / Docs | 91 | 9 |

644 The impact score reflects combined "blast radius," cross-domain influence, and ATO criticality.
645 Connections represent the number of correlated challenge nodes in the graph (see Fig. 1 ).

646

647 The following subsections describe these categories and their associated challenges in a multi-
648 cloud environment.

649 **4.2.1. Access Control**

650 In multi-cloud environments, CSCs face specific authorization and visibility challenges that stem
651 from the involved CSP's role in managing, authorizing, and maintaining the components that
652 comprise each CSO. Because the CSC interacts with the sum of parts rather than the individual
653 components that make up the CSO, the following challenges arise in maintaining oversight
654 across the underlying environments:

655 • **Policy transparency across CSPs:** CSCs may struggle to obtain specific account
656 management policies and procedures for each underlying CSO.

657 • **Restricted management access:** CSCs often lack direct access to the individual account
658 management systems of various integrated CSOs.

659 • **Policy inconsistency:** It is difficult for a consumer to verify that access control policies
660 are being enforced uniformly across all CSPs involved in the multi-cloud service.

661 • **Visibility of privileged accounts:** CSCs may not be able to identify which CSP personnel
662 hold privileged access to the systems that support each CSO.

663 • **Biometric and MFA verification:** Consumers face hurdles in verifying whether biometric
664 or MFA verification is strictly enforced across every layer within each CSO.

665 • **Access control and role review:** CSCs may have a limited ability to review the access
666 control lists (ACLs) and user roles used by each CSP to support the cloud service.

667 • **Authorization accountability:** Verifying that all user accounts and privileges across
668 multiple CSP infrastructures have been properly authorized becomes a complex audit
669 task for CSCs.

- **Role-assignment procedures:** It is difficult to identify the disparate policies that each CSP uses to assign roles and privileges to their own internal users who maintain the CSOs that comprise the multi-cloud environment.
- **Emergency access governance:** CSCs lack direct insight into how various CSPs handle temporary or emergency access requests, making it difficult to confirm whether these procedures are consistently followed.
- **Limited mechanism visibility:** If a CSO supporting a CSC's multi-cloud environment is itself a multi-cloud environment, the CSC may not be able to identify or audit the specific access control mechanisms implemented by that CSO's CSP to connect across the varying clouds that support the CSO.
- **Data protection blind spots:** Due to a lack of direct access to the underlying information systems, the CSC cannot independently verify the data protection mechanisms employed by each CSP.
- **Indirect risk assessment:** Assessing the total risk of the multi-cloud ecosystem is not additive and is hindered by the CSC's lack of direct access privileges to the backend systems of each contributing CSP.
- **Heterogeneous granularity:** CSCs must navigate significant differences in how access controls are configured and the level of granularity available across the different physical and logical components of each integrated CSO.

### 4.2.2. Vulnerability Management

In a multi-cloud environment, the responsibility for security and authorization decisions is abstracted away from CSCs at different levels, depending on the service delivery model. This creates significant "blind spots" in vulnerability management, as the CSC must rely on the provider to harmonize security across disparate infrastructures while they retain the responsibility of properly securing their data. The following points highlight the specific challenges of managing vulnerabilities for a multi-cloud architecture:

- **Tooling incompatibility across integrated CSPs:** The multi-cloud provider may struggle to unify the unique security tools and configurations used by each underlying CSP, leading to inconsistent vulnerability detection across the multi-cloud environment.
- **Restricted authentication scanning:** Because each CSO is not managed by the CSC, the CSC is often denied the high-level access privileges required to conduct deep authentication scans on the individual CSP infrastructures supporting the CSOs.
- **Fragmented continuous monitoring:** The CSC lacks the cross-platform visibility necessary to perform unified continuous monitoring across the multiple CSOs and their varying layers.
- **Security-based monitoring restrictions:** Providers often cite the protection of privileged system information as a reason to block CSCs from performing independent continuous monitoring on the backend components of CSOs.

- **Opaque monitoring plans:** CSPs may fail to deliver a comprehensive, integrated continuous monitoring plan that covers all CSOs involved in the multi-cloud architecture, particularly if a supporting CSO is itself a multi-cloud architecture.
- **Restricted scan result transparency:** Providers may deny the CSC access to the raw vulnerability scan results from individual CSPs, making it difficult for the CSC to verify the security posture of each CSO.
- **Patching information gaps:** CSCs often lack visibility into specific patch management cycles and the actual patching status of the various CSP information systems that support each CSO.
- **Lack of remediation prioritization:** CSCs may not receive clear information from CSPs regarding how they prioritize patches or what remediation actions are being taken across the various CSOs.
- **Incomplete cross-cloud asset inventory:** CSPs may not provide a unified, real-time asset inventory that identifies all resources across the various CSOs.
- **Complex vulnerability scanning:** Orchestrating vulnerability scans across multiple CSOs introduces architectural hurdles, including:
    - **Tool placement logic:** Determining whether to centralize scanning tools in one CSO, deploy them across all CSOs, or execute them from outside the multi-cloud architecture's boundary
    - **Cross-environment secure paths:** Establishing and maintaining secure communication pathways between scanning tools and assets that reside in different CSOs
    - **Unified remediation tracking:** Tracking and fixing identical vulnerabilities across different CSOs within the CSC's organization

### 4.2.3. Incident Response

A CSC's authorization process can be negatively impacted by their inability to conduct security operations across the underlying components of each CSO. This abstraction creates significant barriers for incident response, as the CSC is often distanced from the raw telemetry and operational procedures of each contributing CSP. The following points highlight the specific challenges of managing incident response for a multi-cloud architecture:

- **Delayed cross-provider incident reporting:** CSCs may not receive timely incident data from the CSPs involved in a compromise of the multi-cloud architecture because information must filter through each CSP's reporting chain before reaching the consumer.
- **Opaque incident response policies:** It is difficult for CSCs to obtain the specific incident response policies and procedures used by each underlying CSP.

- **Opacity of monitoring tools:** CSCs often lack information regarding the specific monitoring tools and system monitoring practices employed by various CSPs.
- **Restricted training verification:** CSPs may not provide records proving that personnel at each underlying CSP have received proper incident response training.
- **Lack of integrated testing results:** Consumers face challenges in obtaining incident response testing procedures and the actual results of those tests from every CSP integrated into the multi-cloud service.
- **Denial of independent monitoring access:** CSCs are frequently denied the access privileges necessary to conduct their own independent monitoring of the CSOs and their underlying components.
- **Fragmentation of cloud-native incident response capabilities:** Differences in the native incident response capabilities of each CSP can lead to inconsistent execution and highly complex incident response plans.

### 4.2.4. Architecture

Cloud service consumers rely on CSPs to architect and design systems that implement various CSOs, which introduces architecture-related authorization challenges as the boundary between the consumer's control and the provider's managed infrastructure becomes increasingly opaque. The following points summarize architecture-related authorization challenges[2] within the context of such offerings:

- **Boundary documentation constraints:** CSPs may withhold documentation that explicitly defines the system boundary for their CSOs, often citing concerns over privileged information and backend system security.
- **Ambiguity of responsibilities:** CSCs may lack clear information regarding their specific security responsibilities and the extent of their control within the CSOs that comprise the multi-cloud architecture.
- **Increased boundary complexity:** It may be difficult for CSCs to define clear information system boundaries for their own cloud assets because the multi-cloud architecture relies on multiple underlying CSPs and CSOs.
- **Identification of disparate functions:** It may be difficult for CSCs to identify and document the various functions provided by the multiple CSP information systems that make up each CSO.

[2] These authorization challenges are also identified as security challenges in Sec. 4.1.4.

### 4.2.5. Data Protection

CSCs are largely responsible for data protection in multi-cloud ecosystems, though they must rely on the CSP's controls. The following points summarize the data protection challenges within a multi-cloud architecture:

- **Opaque system architecture:** CSCs may struggle to obtain detailed information system architecture for the integrated cloud services, as providers often cite proprietary system concerns or security risks.
- **Hidden data protection mechanisms:** Due to a lack of direct access to underlying systems or architecture documentation, CSCs may be unable to identify the specific data protection mechanisms employed by each integrated CSP.
- **Conflicting control requirements:** Underlying CSPs may have security control implementation requirements (e.g., regulatory, compliance) that differ from the CSC's internal standards.
- **Security dependency:** CSCs must rely heavily on CSPs and underlying providers to maintain the authorization status of each integrated CSO.
- **Ambiguity in data residency:** CSPs may not always provide precise information regarding the physical or logical location of CSC data within each CSO comprising the multi-cloud environment.
- **Inaccessible compliance documentation:** It may be difficult for CSCs to obtain system security plans, assessment results, or mitigation strategies for various CSOs.
- **Information exchange gaps:** Providers may not provide formal information exchange documentation (e.g., memorandums of understanding, SLAs) for connections between the CSPs that handle the transfer of CSC data.
- **Disparity in compliant protection:** Differences in the cloud-native storage and transmission capabilities across integrated CSOs can create significant disparities in the availability of compliant protection.
- **Synchronization complexity:** Synchronizing data between multiple CSOs within a multi-cloud architecture requires secure communication channels and is often complicated by conflicting storage formats across different provider infrastructures.

### 4.2.6. Contingency Planning and Disaster Recovery

CSCs are often separated from the specific recovery protocols and data access required to ensure business continuity. The following points summarize relevant contingency planning and disaster recovery challenges for multi-cloud architectures:

- **Restricted access to recovery policies:** CSCs may struggle to obtain specific contingency plans and disaster recovery policies from the underlying CSPs, as providers often cite proprietary information as a barrier to transparency.

- **Opaque testing documentation:** Obtaining clear documentation regarding contingency plan testing for the cloud services being utilized can be difficult for CSCs.
- **Opacity of disaster recovery results:** CSCs may be unable to access the actual results and information from disaster recovery testing performed on the CSOs that support their multi-cloud architecture.
- **Barriers to independent testing:** CSPs may restrict CSCs from accessing backed-up data, which prevents the consumer from conducting their own independent system recovery and reconstitution testing.
- **Lack of failover planning visibility:** CSCs may not receive detailed failover planning or corresponding testing results for the cloud services integrated into the multi-cloud environment.
- **Operational complexity of heterogeneous support:** Differences in cloud-native services and the various support teams involved across multiple CSPs complicate the overall planning, training, and execution of business continuity (BC) and disaster recovery (DR) capabilities.

### 4.2.7. Configuration Management

CSCs are often distanced from the direct administrative access required to verify security settings across the integrated environment. The following points highlight the specific configuration and authorization challenges for CSCs in multi-cloud environments:

- **Restricted configuration access:** CSCs may be denied direct access to the underlying CSO information systems, which prevents them from manually verifying the secure configurations of their cloud services.
- **Barriers to independent scanning:** CSCs often lack the access privileges necessary to conduct independent configuration scans on the backend systems supporting the CSOs that comprise the multi-cloud architecture.
- **Lack of scan result transparency:** CSPs may not provide the raw results of configuration scans related to the CSO components that directly support the CSC, hindering the consumer's ability to assess compliance.
- **Opaque management plans:** It may be difficult for CSCs to obtain comprehensive configuration management plans or the specific policies and procedures that govern the integrated CSOs.
- **Change control gaps:** CSCs often lack detailed configuration change control documentation, which makes it difficult to track modifications across the multi-cloud architecture.
- **Undefined administrative roles:** CSPs may not clearly define or share the specific system administrator roles, responsibilities, and access restrictions related to configuration changes within the CSOs that support the multi-cloud architecture.

- **Heterogeneous configuration requirements:** The configuration of CSOs with similar capabilities and functionalities frequently varies significantly, which complicates the approval of changes and the timing of deployments.
- **Resource inefficiency:** CSCs often require separate, specialized teams and/or personnel to implement equivalent configuration changes across the unique CSOs that comprise the multi-cloud architecture.

### 4.2.8. Documentation

CSCs often have limited visibility into the compliance and inheritance details of each individual cloud service offering because CSPs act as intermediaries for the underlying components of each CSO. The following points summarize the authorization-related documentation challenges within a multi-cloud environment:

- **Incomplete documentation flow:** CSCs may not receive or have the opportunity to review the complete set of information system documentation from individual CSPs regarding the specific cloud services they are using.
- **Delays in critical updates:** CSCs may not receive updated information system documentation from all involved CSPs in a timely manner, which can stall authorization processes.
- **Difficulty identifying inherited controls:** It may be difficult for CSCs to clearly identify which specific security controls are inherited from which underlying CSO.
- **Inconsistent responsibility details:** The documentation regarding inheritance and customer responsibility typically differs across each CSP, even for controls that are commonly inherited, which creates a fragmented compliance picture.

# 5. Analysis of Challenges

This section provides additional insight into the nature of the identified challenges in securing and authorizing multi-cloud ecosystems.

## 5.1. Correlation Graph Analysis

Figure 1 shows a correlation graph of challenges that was built using four criteria (see Sec. 5.1.1) to determine whether two challenges should be linked.

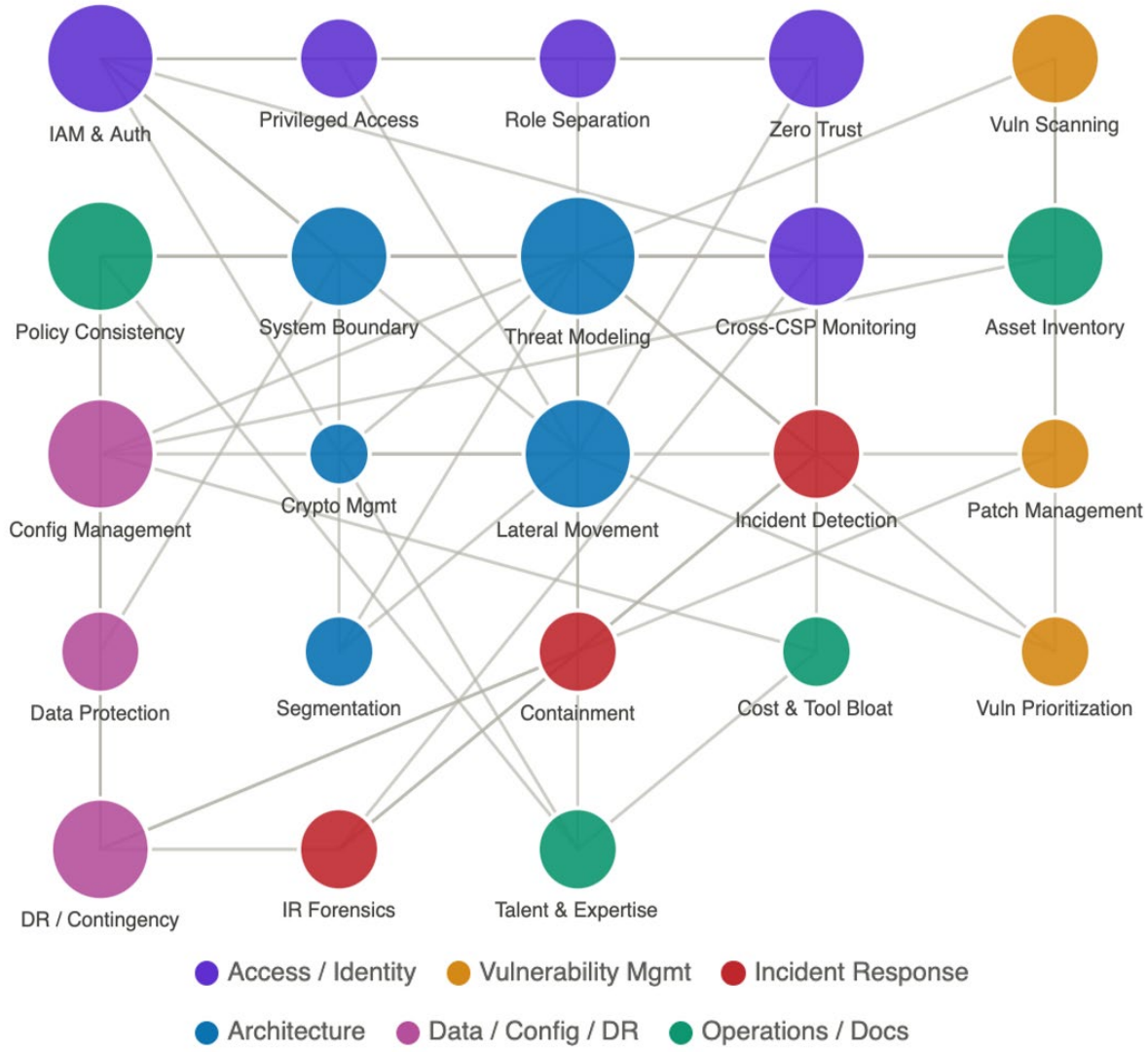


**Figure 1. Challenges correlation graph[3]**

Challenges were *not* linked simply because they appear in the same category or have similar levels of difficulty. Rather, challenges are linked if resolving one meaningfully changes the

[3] The document is accompanied by an interactive graph page available at multicloud_challenge_correlation_graph.html.

difficulty or feasibility the other. Thematic proximity without a functional dependency was treated as coincidence, not correlation. For example, Cryptographic Management and Data Protection are both "data security" concerns but are not directly linked in the graph because resolving one does not structurally simplify the other.

### 5.1.1. Correlation Graph Criteria

Below are the four criteria used to generate the graph shown in Fig. 1:

1. **Criterion #1: Shared dependency on a common resource or capability**

   Two challenges are considered to be correlated when solving one requires the same underlying capability as the other. For example, IAM and cross-CSP monitoring both depend on a unified identity data model in that authentication alerts cannot be correlated across CSPs without consistent identity representations. Similarly, asset inventory and vulnerability scanning both depend on the same asset enumeration capability.

2. **Criterion #2: Causal (amplification) relationships**

   A link was drawn when one challenge directly worsened or triggered another. The following are the clearest examples:

   - The lack of a system boundary definition causes ambiguity in control inheritance, which directly breaks policy consistency and configuration management.
   - Weak privileged access controls expand the blast radius of lateral movement (i.e., an attacker who compromises one privileged account crosses CSP boundaries more easily).
   - Poor incident detection directly degrades containment speed and forensic quality since containment requires detection, and reconstructing an attack path requires complete logs.

3. **Criterion #3: Cross-domain operational overlap**

   Some challenges span multiple security domains and, therefore, correlate with challenges in each of those domains. For instance, patch management sits at the intersection of vulnerability management and configuration management since applying a patch is both a vulnerability remediation act and a configuration change event. In a multi-cloud environment, it also touches disaster recovery planning if patching requires downtime windows.

4. **Criterion #4: ATO boundary effects**

   Several challenges are correlated specifically because they share an ATO friction point (i.e., the legal and administrative boundary around each CSP), which creates the same kind of verification gap for multiple different controls. Role reparation, emergency access, and system boundary definition all have ATO-tagged challenges because the authorizing entity faces the same structural problem in each case: they cannot directly

inspect or verify CSP internals. This creates a cluster of challenges that are independently categorized but share a root cause, and mitigating that root cause (i.e., establishing contractual visibility mechanisms with each CSP) helps all of them simultaneously.

### 5.1.2. Graph Analysis Findings

The correlation graph (see Fig. 1) reveals three structural clusters:

1. **Identity cluster** (IAM, Privileged Access, Role Separation, Zero Trust, Monitoring), which is tightly interconnected, meaning that identity weaknesses propagate rapidly across detection and containment
2. **Architecture cluster** (Boundary, Threat Modeling, Lateral Movement, Segmentation, Crypto), which is a "middle layer" cluster that bridges identity failures to operational impact
3. **Operations cluster** (Inventory, Policy, Configuration, Disaster Recovery, Data, Talent), which groups "slow burn" challenges that do not cause immediate incidents but determine whether all other mitigations are sustainable

The highest-degree nodes (i.e., most connections) are IAM, inventory, and policy. This confirms that those nodes are the correct starting targets for mitigation efforts. Talent and cost, while lower-scoring, act as systemic enablers, meaning that insufficient expertise limits the organization's ability to address the higher-impact challenges at all.

### 5.1.3. Highest Impact Challenges Based on the Graph Analysis

After ranking challenges based on how many downstream challenges become easier if the analyzed one is mitigated, the following seven challenges were identified as having the highest impact:

1. **Asset inventory:** Information on what exists across all CSPs and/or CSOs is necessary for scanning, patching, policy, threat modeling, and boundary definition. Asset inventory is the single biggest force multiplier and the prerequisite for almost everything else.
2. **IAM and authentication:** Fixing fragmented IAM propagates improvements across at least eight other challenges, including lateral movement, zero trust, detection, containment, privilege management, and system boundary definition.
3. **Incident detection/SIEM:** A multi-cloud environment generates massive, heterogeneous log streams. Normalizing and correlating them directly improves containment speed, forensic quality, and the accuracy of lessons learned.
4. **Policy consistency:** A coherent policy bridges the meta-challenge layer to execution and enables configuration management, data governance, and disaster recovery planning.

5. **System boundary definition:** This unlocks correct control inheritance mapping, ATO documentation, and shared responsibility clarity. Most ATO-specific challenges cascade from this one being poorly defined.
6. **Threat modeling:** A holistic threat model is the architectural skeleton that gives all other controls purpose. It correlates with lateral movement, segmentation, cryptographic management, and vulnerability prioritization.
7. **Cross-CSP monitoring:** Anomaly correlation across IAM systems links access control and identity management with incident response.

## 5.2. Analysis of High-Level System Drivers

Challenges in securing and authorizing multi-cloud ecosystems generally stem from six high-level systemic drivers:

1. Inherent complexity and Lack of standardization (see Sec. 5.2.1)
2. Increased attack surface (see Sec. 5.2.2)
3. Visibility and control gaps (see Sec. 5.2.3)
4. Talent and resource strain (see 5.2.4)
5. Compliance and governance hurdles (see Sec. 5.2.5)

### 5.2.1. Inherent Complexity and Lack of Standardization

It is difficult to establish an end-to-end unified cybersecurity strategy for multi-cloud architectures due to the inherent complexity of such environments and a lack of standardization among cloud service offerings. Each CSP has their own approach to solving their customers' challenges and use cases. Among CSPs in the same market, approaches may differ widely, even when industry-standard data formats and communication protocols are in place. CSPs who use security products that are themselves CSOs fall victim to both ends of this challenge: they try to solve challenges resulting from consuming multiple CSOs by using CSOs that present the challenge, increasing the footprint and complexity of the multi-cloud environment [9][10]. However, using traditional self-managed security tooling increases operational complexity and misalignment.

One critical example of this is inconsistent identity and access management [CS-01, CS-02, CS-03, CS-07]. Although single single-on and federation solutions help mitigate management overhead, these solutions still derive their overall permission sets for each role from the applications and CSOs to which they provide access. CSOs often group permissions together to ease adoption and simplify management, and overlapping desired permissions from different CSOs may require additional undesired permissions. However, highly granular permissions do not necessarily solve this challenge because they increase management overhead and the expertise required for effective security [CS-08].

As CSOs are added to a multi-cloud environment, increasingly broad and deep expertise is needed to weave disparate architectures from each CSO into a coherent, cohesive, and secure implementation [CS-60, CS-61]. The security best practices offered by each CSP may not apply or may even conflict with other CSPs and their offerings. Recovery processes and SLAs may also vary significantly across CSOs without an option for alignment [CS-24].

### 5.2.2. Increased Attack Surface

As more CSOs are added to a multi-cloud environment, the attack surface of that environment naturally increases. Modeling the interactions between CSOs is challenging due to the unique characteristics of each offering and the opaque interplays between vulnerabilities and misconfigurations in them [CS-26, CS-28]. For example, a public API endpoint in one offering, an improperly configured access policy in another, and a known but seemingly unrelated vulnerability in a third may result in a potential attack chain that is difficult to identify prior to exploitation [CS-31].

### 5.2.3. Visibility and Control Gaps

Achieving comprehensive visibility and control across a multi-cloud infrastructure is difficult because each cloud provider has unique security protocols, compliance requirements, and scanning tools [CS-16F, CS-17B, CS-56, CS-57]. This fragmentation can lead to significant gaps in risk assessments, vulnerability scanning, and overall situational awareness. Without a consolidated view of a multi-cloud environment's posture across all cloud environments, organizations may struggle to accurately identify, quantify, and prioritize risks. Security teams must monitor a greater number of services and contend with the complexity of aligning security log and alert information from disparate cloud sources. Inconsistent message formats across CSOs can lead to longer remediation times and the potential for missing critical information during an investigation [CS-19, CS-20].

Fragmented data across the environment and varying restrictions on interconnectivity and authorization can also delay incident response [CS-21, CS-23, CS-24]. The capabilities and interoperability of responder tooling with the various CSOs in the environment may be limited. Generating holistic reports on incidents and risks from CSOs with different output formats for their raw data can also be burdensome as analysts work to aggregate incident information into a consumable, actionable report [CS-17I, CS-25, CS-26].

### 5.2.4. Talent and Resource Strain

Operating across multiple CSOs magnifies human-capital demands in ways that are not linear with the number of services in use. Teams must simultaneously consider provider-specific architectures, policy languages, telemetry formats, and deployment pipelines while sustaining consistent operations. This breadth of expertise is difficult to hire for and harder to retain, leading to longer onboarding and cross-training cycles, increased context-switching for engineers, and slower mean time to detect and respond (MTTD/MTTR) during incidents. In

practice, limited expert time becomes the scarcest resource; the same few specialists are repeatedly pulled into identity design, logging normalization, control mappings, incident handling, and compliance reporting, which can lead to fatigue and burnout risks that further erode resiliency.

Financial resources are strained as well. Multi-cloud environments often duplicate capabilities, monitoring, secrets management, and policy enforcement because native controls rarely align across providers. Organizations pay in both license/subscription costs and the engineering time required to integrate, normalize, and govern these overlapping stacks. If shared services cannot be extended uniformly across CSP boundaries, program offices must fund parallel solutions and accept higher operating complexity as the price of coverage. The result is a persistent "platform tax" that diverts resources from mission features to glue code, data shaping, and control rationalization.

Talent shortages intersect with authorization and governance workloads. Different boundary definitions, recovery postures, and provider documentation practices mean that compliance evidence production (e.g., for ATOs) scales with the number of CSOs rather than with the scope of the system alone. Security and risk teams spend disproportionate time tracing inherited controls, reconciling divergent artifacts, and translating provider attestations into an enterprise-standard control lexicon. Without dedicated platform engineering and documentation functions, these repetitive translation tasks crowd out proactive hardening and tabletop exercises.

Mitigations typically combine people, process, and platform moves. Establish a small platform/core team to publish paved-road patterns (e.g., identity baselines, logging schemas, deployment guardrails) and reusable IaC modules; adopt a common evidence model and metadata standards to reduce translation overhead; invest in role-based, skills-mapped training tied to the specific CSOs in use; and use automation to enforce controls and generate compliance artifacts "as code." Organizations that explicitly budget for these enablement layers rather than treating them as ad hoc tasks consistently report lower operational drag and more predictable risk reduction over time.

### 5.2.5. Compliance and Governance Hurdles

Shared responsibility models delineate the responsibilities of CSPs and CSCs in securing a CSO. When multiple CSOs are brought together into a multi-cloud architecture, it is difficult to align the shared responsibility models for each offering with an organization's business processes and structure [CS-32A] and to develop a comprehensive body of evidence to validate the proper implementation of responsibilities [CS-32B]. As more offerings are integrated, the scope of responsibility increases, and the differences in terminology and capabilities across CSOs add further complexity, which often leads to the inconsistent application of security controls throughout the environment [CS-110].

Due to inherent differences in cloud-native services, components that appear to be equivalent across providers may actually have critical differences in security practices. Similarly, the same type of component may be owned or administered by different teams, depending on the

expertise required [CS-100, CS-101, CS-102]. Adding to this, multi-cloud systems can be subject to diverse, often conflicting regulatory requirements across different jurisdictions and CSPs [CS-33]. Determining the exact location of customer data can be challenging in a multi-cloud system due to differing visibility and implementation approaches across providers, which complicates data residency and locality requirement implementation and validation.

Altogether, these compliance and governance challenges make it very difficult to maintain clear and representative documentation of the system [CS-100, CS-101, CS-102]. This leads to misunderstandings about the security and compliance state of the system and may require extended compliance and technical resources to properly evaluate and correct the shortcomings.

# 6. Summary of Findings

## 6.1. Security Challenges

Multi-cloud environments present unique security challenges that differ significantly from those of single-cloud or on-premises architectures. These challenges arise from using multiple CSPs and/or CSOs, each with their own security models, tools, configurations, and shared responsibility frameworks. This diversity makes it difficult for organizations to maintain consistent security policies and enforce uniform controls across multi-cloud environments.

One major challenge is the lack of standardized security controls, where each CSP implements IAM, logging, monitoring, and encryption differently. A CSP may even implement these things differently across its own suite of CSOs. As a result, security teams must understand and manage multiple tool sets and configurations, which can increase the likelihood of misconfigurations.

Visibility and monitoring are also significantly more difficult in a multi-cloud environment. Security teams often struggle to obtain a comprehensive view of assets, workloads, and network traffic across different cloud environments. This fragmented visibility can delay threat detection and incident response, as auditing and monitoring data are spread across multiple systems with varying formats and access methods. Without centralized monitoring, identifying abnormal behavior or correlating events across clouds becomes a complex and error-prone process.

Identity and access management presents another critical challenge. Managing identities across multiple clouds requires federated identity solutions and careful coordination to avoid privilege sprawl. Inconsistent access control policies can result in users having excessive permissions, an increased attack surface, and the risk of credential misuse or insider threats.

Data security and compliance are also more complicated in multi-cloud deployments. Organizations must ensure that sensitive data is protected consistently across all environments, regardless of where it is stored or processed. Differences in data protection mechanisms, regional regulations, and compliance requirements can lead to gaps in coverage. Ensuring data sovereignty and meeting regulatory obligations becomes especially challenging when data moves between clouds or is replicated across regions.

Another key issue is the complexity of secure configuration and workload portability. Applications that are designed for one cloud provider may not easily translate to another without changes in architecture or security controls. This can lead to inconsistent security postures between environments, especially when workloads are migrated or replicated. Additionally, the use of cloud-native services that are unique to each provider can create dependencies that complicate security standardization.

Supply chain and third-party risks may also increase in multi-cloud settings. Organizations may rely on one or more CSPs, but each of these CSPs may rely on their own third-party vendors for services, tools, and integrations. Each additional dependency introduces potential vulnerabilities and requires careful vetting, monitoring, and risk management.

Finally, governance and policy enforcement become more difficult as organizations implement multi-cloud environments. Maintaining consistent security policies, auditing, and configurations and ensuring compliance across multi-cloud environments requires automation and standardization. Without these capabilities, organizations may face gaps in enforcement and increased exposure to security incidents.

While multi-cloud strategies offer flexibility and resilience, they significantly increase the complexity of security management. Addressing these challenges requires robust governance frameworks, centralized visibility, consistent policy enforcement, and a strong emphasis on automation and standardization.

## 6.2. Authorization Challenges

Authorization in a multi-cloud environment introduces complex challenges that go well beyond traditional single-system ATO processes. Authorization depends on clearly defined system boundaries, comprehensive security documentation, and the consistent enforcement of controls. In a multi-cloud setting, these elements are divided across multiple CSPs and/or CSOs that have their own architectures, policies, and operational requirements.

One of the main challenges is defining the boundaries of the information system. In a multi-cloud architecture, a single application or system may stretch across multiple infrastructures, platforms, and services provided by different CSPs. Each provider maintains their own architectural, security, network, operational, and data boundaries. This division makes it difficult for authorizing officials to determine where one system ends and another begins. Without clearly defined boundaries, it becomes challenging to accurately assess risk or assign responsibility for specific controls, which are requirements for granting or maintaining an ATO.

Another challenge lies in access control. Authorization requires visibility into user accounts, roles, privileges, and authentication mechanisms. In a multi-cloud environment, CSPs may not provide full transparency into their account management systems or access control policies due to security requirements. This limits the CSC's ability to verify whether access controls are consistently implemented across providers. Additional challenges include identifying privileged accounts, confirming the use of multi-factor authentication, and ensuring that all user privileges are properly authorized. Organizations may also struggle to validate how temporary or emergency access is granted and revoked, increasing the risk of unauthorized access or privilege escalation.

The lack of standardized policies and procedures across CSPs further complicates the ATO process. Each provider may implement different approaches to role assignment, identity management, and access enforcement. This inconsistency forces organizations to reconcile multiple frameworks and often results in gaps or overlaps in control coverage. In some cases, CSPs may restrict access to their internal systems, preventing CSCs from independently verifying controls or conducting vulnerability scans or audits. This lack of visibility undermines trust and complicates the risk-based decision-making process of ATOs.

Vulnerability management also presents significant authorization challenges. Authorization decisions rely on an accurate and continuous assessment of system vulnerabilities. However,

CSPs may use proprietary tools and configurations, and they may not allow customers to perform authenticated scans or continuous monitoring. Limited access to vulnerability scan results, patch management data, and asset inventories makes it difficult to assess the true security posture of the system. Without this information, authorizing officials may lack the evidence needed to determine whether risks are acceptable.

The distributed nature of multi-cloud environments complicates ongoing monitoring and compliance. Continuous monitoring is a key requirement for maintaining an ATO, but CSPs may restrict access to logs, monitoring tools, vulnerability scan results, configuration settings, or incident response data. This limits an organization's ability to detect, respond to, and report security incidents in a timely manner. As a result, maintaining an ATO becomes an ongoing challenge rather than a one-time decision.

Authorization challenges in multi-cloud environments originate from divided system boundaries, limited visibility into CSP operations, inconsistent access control practices, and restricted vulnerability management capabilities. Addressing these challenges requires stronger standardization, improved transparency from providers, and enhanced coordination between all stakeholders involved in the ATO process.

## References

[1] Mell P, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-145. http://dx.doi.org/10.6028/NIST.SP.800-145

[2] Liu F, Tong J, Mao J, Bohn RB, Messina JV, Badger ML, Leaf DM (2011) NIST Cloud Computing Reference Architecture (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 500-292. https://doi.org/10.6028/NIST.SP.500-292

[3] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[4] Rose S, Borchert O, Mitchell S, Connelly S (2023) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-207. https://doi.org/10.6028/NIST.SP.800-207

[5] Ross R, Pillitteri V (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3

[6] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[7] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[8] International Organization for Standardization. (2023). ISO/IEC 22123-1:2023 Information technology—Cloud computing—Part 1: Vocabulary (2nd ed.). ISO.

[9] Kropov, V (2025, October 17). Practical multi-cloud security for enterprises: Best practices and expert tips. https://www.n-ix.com/multi-cloud-security/

[10] Shua, A. (2025, January 27). Multi-Cloud Environment: How Secure Are They? https://www.forbes.com/councils/forbestechcouncil/2025/01/27/multi-cloud-environments-how-secure-are-they/

## Appendix A. Identified Challenges

The following tables enumerate each multi-cloud architecture security challenge identified by the Multi-Cloud Security Public Working Group. These challenges have been lightly edited but largely represent the raw inputs used to generate this report.

- Access Control
- Vulnerability Management
- Incident Response
- Architecture
- Data Protection
- Contingency Planning and Disaster Recovery
- Business Operations
- Configuration Management
- Documentation
- Certification and Authorization
- Meta Challenges/Challenges with the Challenges

## A.1. Access Control

Table 2 enumerates the unique access control challenges in a multi-cloud architecture.

**Table 2. Access control challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-01** | Identity and Access Management | Multiple user authentication and authorization systems (named access systems) | Managing multiple CSP-employed access control systems and/or multiple third-party access control systems, as used by each CSP | The authorizing entity will need access to all CSP account management systems. Each CSP may have built-in systems for managing authentication, roles, user authorizations, and access privileges. These authentication and authorization aspects may not be aligned in all CSPs in terms of user ID or the propagation of roles and authorizations. | The authorizing entity will have access to the CSP's account management systems to review system user roles and privileges. | ATO |
| **CS-02A** | Identity and Access Management | Identity and access management (IAM) | Verifying the consistent application of access control policies across multiple CSPs | Each CSP may have its own IAM system with its own specific implementation, making it difficult for a CSC to implement an effective access control policy across a multi-cloud environment. | The authorizing entity will be able to verify the consistent implementation of least privilege and separation of duties across multiple CSPs' IAM systems. | Security and ATO |
| **CS-02B** | Identity and Access Management | Identity and access management (IAM) | Verifying whether a CSP's access control policies are consistently applied | The authorizing entity must be able to validate that access control policies are consistently applied across multiple CSPs. | The authorizing entity will be able to validate that there is a consistent implementation of least privilege and separation of duties across multiple CSPs' IAM systems. | ATO |
| **CS-03** | Identity and Access Management | Managing privileged access | Understanding the scale of CSP user privileged access | It may be difficult for the authorizing entity to identify all privileged user access accounts. Each CSP may require multiple | The authorizing entity will be able to verify the CSP's user accounts with privileged access. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| | | | | privileged user roles or accounts. | | |
| **CS-04** | Identity and Access Management | Authorization of service accounts | Granting full and proper access to the service accounts used for security functionality | The authorizing entity will need to review the CSP's access control policies and procedures and have access to all CSP service accounts. | The authorizing entity will be able to verify that the active CSP service accounts are required and that previous service accounts have been terminated. | Security |
| **CS-05** | Identity and Access Management | Biometric authentication | Verifying that biometric authentication has been employed by the CSP | The authorizing entity will need access to the CSP's authentication systems to verify whether biometric authentication has been employed. | The authorizing entity will be able to verify whether CSPs have employed biometric authentication, including the authentication process and the secure storage of biometric data. | Security |
| **CS-06** | Identity and Access Management | Multi-factor authentication (MFA) | Verifying that MFA has been employed by the CSP | The authorizing entity will need to verify whether the CSP has employed MFA, including the authentication policy, procedures, and implementation verification. | The authorizing entity will be able to verify whether the CSP has employed MFA. | Security |
| **CS-07A** | Role Separation | Identifying roles and separation of duties | Identifying CSP users' roles and privileges | The authorizing entity will need to review the CSP's system ACLs and user roles and privileges. | The authorizing entity will be able to review the CSP's system ACLs, and user roles and privileges. | Security |
| **CS-07B** | Role Separation | Verifying roles and separation of duties | Verifying CSP users' roles and privileges | The authorizing entity will need to review the CSP's system ACLs and user roles and privileges. | The authorizing entity will be able to verify the CSP's system ACLs and user roles and privileges. | ATO |
| **CS-08A** | Role Separation | Identifying account and role authorizations | Identifying the CSP's user accounts and role authorizations | The authorizing entity will need to identify user accounts and their corresponding role authorizations. | The authorizing entity will be able to verify that the CSP's user account and | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| | | | | | their corresponding roles have been authorized. | |
| **CS-08B** | Role Separation | Verifying account and role authorizations | Verifying that the CSP's user accounts and roles have been authorized | The authorizing entity will need to verify that the CSP's user accounts and their corresponding roles have been authorized. | The authorizing entity will be able to verify that the CSP's user accounts and their corresponding roles have been authorized. | ATO |
| **CS-09** | Role Separation | Ensuring revocation of access | Verifying that the CSP's user access is revoked when needed | Multiple authorization management systems used by CSPs may make it difficult for the authorizing entity to identify the time frame for revoking a user's system access. | The authorizing entity will be able to verify the time frames for revoking the CSP user's system access. | ATO |
| **CS-10** | Role Separation | Criteria for assigning roles | Verifying the CSP's policies and procedures for assigning user roles | Multiple CSP account management policies and procedures may make it difficult for the authorizing entity to identify how roles are assigned to CSP users. | The authorizing entity will be able to identify the CSP's policies and procedures for assigning roles to user accounts. | ATO |
| **CS-11A** | Emergency Access | Consistent temporary and/or emergency access | Verifying the CSP's user account creation procedures to identify temporary and emergency system user access processes | The authorizing entity will need to review the CSP's time frames, conditions, levels of access, procedures, and policies for temporary and emergency user access. | The authorizing entity will be able to identify the CSP's policies, procedures, and implementation of temporary and emergency user system access. | Security |
| **CS-11B** | Emergency Access | Verifying emergency access | Verifying that the CSP's temporary and emergency access privileges have been terminated | It may be difficult to verifying whether a CSP's emergency user access has been terminated. | The authorizing entity will be able to verify that the temporary and emergency user access granted by the CSP has been terminated. | ATO |
| **CS-12A** | Least Privilege | Identifying effective user privileges | Identifying and deriving effective access control privileges for users and software in compliance with zero trust principles | Implementing methods to identify and derive effective privileges of users and software across multiple IAM systems in | Systems will be able to identify and derive the privileges of users and software across different | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| | | | | hybrid CSP environments may be challenging. | IAM systems in hybrid CSP environments. | |
| **CS-12B** | Least Privilege | Verifying effective user privileges | Verifying the effective access control privileges of users and software in compliance with zero trust principles | Implementing methods to verify derived effective privileges of users and software across multiple IAM systems in hybrid CSP environments may be challenging. | Systems will be able to verify the derived effective privileges of users and software across multiple IAM systems in hybrid CSP environments. | ATO |
| **CS-13A** | Least Privilege | Identifying effective administrator privileges | Identifying effective access control privileges of administrative users and software in compliance with zero trust principles | Implementing methods to identify derived effective privileges of administrative users and software across multiple IAM systems in hybrid CSP environments may be challenging. | Systems will be able to identify the derived effective privileges of administrative users and software across multiple IAM systems in hybrid CSP environments. | Security |
| **CS-13B** | Least Privilege | Verifying effective administrator privileges | Verifying the derived effective access control privileges of administrative users and software in compliance with zero trust principles | Implementing methods to verify the derived effective privileges of administrative users and software across multiple IAM systems in hybrid CSP environments may be challenging. | Systems will be able to verify the derived effective privileges of administrative users and software across different multiple IAM systems in hybrid CSP environments. | ATO |
| **CS-14** | Least Privilege | Identifying anomalous behavior | Identifying the anomalous behavior of users and software. | Implementing methods to identify the anomalous behavior of users and software across multiple IAM systems in hybrid CSP environments using a common definition of anomalies may be challenging. | Systems will be able to uniformly identify the anomalous behavior of users and software across multiple IAM systems in hybrid CSP environments using a unified approach. | Security |
| **CS-15** | Least Privilege | Correlated monitoring of user and software authentication | Deriving and implementing methods to cross-correlate monitoring alerts for users and software across multiple CSP environments | Identifying a common method to cross-correlate monitoring alerts for users and software (e.g., definitions of alerts, including contents and formats) | There will be a mutually harmonized system for monitoring users and software across hybrid CSP environments. | ATO |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| | | | | across multiple CSP environments may be challenging. | | |

## A.2. Vulnerability Management

Table 3 enumerates the unique vulnerability management challenges in a multi-cloud architecture.

**Table 3. Vulnerability management challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-16 A** | Vulnerabilities | Complex and diverse infrastructure | Increased complexity of managing vulnerability scans in multi-cloud environments due to the diverse security tools, configurations, and APIs of different CSPs | Each cloud provider's unique security tools and configurations cause inconsistencies in scans. The lack of standardization makes it difficult to create a unified, end-to-end scanning approach that covers all cloud environments. The nuances of different APIs from each cloud provider require organizations to adjust their processes for each provider. | A harmonized vulnerability management program addresses multiple cloud providers and offers standardized scanning procedures that are adaptable to each provider's APIs and configurations while establishing and regularly updating best practices for consistent and comprehensive scanning. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-16 B** | Vulnerabilities | Inconsistency in vulnerability scan depth and breadth | Ensuring comprehensive and effective vulnerability scans in multi-cloud environments with varying cloud abstractions and provider capabilities | Differences in cloud abstractions, customer responsibilities, and provider tools and capabilities complicate the task of ensuring that scans cover the entire system and provide valuable insights. This includes reaching all components for scanning purposes (i.e., identification of assets to be scanned) and performing proper authenticated scans. | A standardized scanning framework accounts for different cloud abstractions and provider capabilities to ensure the consistent validation of scan depth and coverage across all environments. | Security |
| **CS-16 C** | Vulnerabilities | Obstacles in assessing the chain of vulnerabilities and their impacts | Addressing the full scope of vulnerabilities and control weaknesses in multi-cloud environments with interconnected impacts on security | The involvement of multiple cloud providers that have unique infrastructures and security controls complicates assessments of how vulnerabilities are linked and their collective effects on system security. | A comprehensive risk assessment framework maps and analyzes the interconnectedness of vulnerabilities across different cloud providers to understand their collective impact on security. | Security |
| **CS-16 D** | Vulnerabilities | Lack of standardization in scanning tools and cloud environment assets to be scanned | Implementing a cohesive security scanning strategy when there is a lack of uniformity among cloud providers | Organizations must navigate different security standards, certifications, compliance frameworks, scanning tools, and methodologies, which complicates comprehensive security scanning across multiple cloud environments. | A flexible security scanning framework is in place and can adapt to the diverse standards and tools of different cloud providers to ensure consistent and comprehensive scans. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-16E** | Vulnerabilities | Interdependencies and second-order security impacts | Evaluating cloud service security while considering the second-order effects of risk exceptions on overall system security | It is essential to assess how an API interacts with other services and the impact of vendor dependencies and operational requirements since vulnerabilities in one service can affect the entire system, especially in multi-cloud environments. | Develop a comprehensive risk assessment approach that maps interdependencies and evaluates the potential cascading effects of risk exceptions across all services and vendors involved. | Security |
| **CS-16F** | Vulnerabilities | Visibility and control | Achieving comprehensive visibility and control over a multi-cloud infrastructure while avoiding potential blind spots in risk assessments of vulnerability scans | The unique security protocols, compliance requirements, and scanning tools of various CSPs complicate the implementation of a unified security scanning strategy and hinder a holistic view of the infrastructure. | Establish an integrated security management system that consolidates data from all cloud providers to ensure consistent visibility and control when identifying and addressing vulnerabilities across the entire environment. | Security |
| **CS-16G** | Vulnerabilities | Integration and interoperability of scanning tools | Integrating security scanning tools across different cloud platforms despite compatibility and interoperability issues | Each CSP's unique scanning capabilities, APIs, and methodologies and the lack of standardization complicate the creation of a unified scanning strategy. | Invest in adaptable integration solutions that bridge the differences between cloud platforms to ensure seamless compatibility and a cohesive security scanning approach. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-16H** | Vulnerabilities | Coordinating scanning schedules | Scheduling security scans in a multi-cloud environment with varying maintenance windows, downtime restrictions, and scanning limitations across providers | The variability in provider constraints complicates scanning schedules and requires careful planning to avoid service disruptions and ensure effective scanning without impacting critical operations. | Develop a coordinated scanning schedule that aligns with each provider's constraints and optimizes resource utilization to ensure minimal disruption and maintain performance across the multi-cloud environment. | Security |
| **CS-16I** | Vulnerabilities | Data protection and privacy | Ensuring data protection and privacy during security scans in multi-cloud environments while considering the distribution of sensitive information across multiple providers | Conducting scans involves accessing sensitive data, which raises concerns about exposure or unauthorized access and requires a balance between thorough scanning and safeguarding data confidentiality and integrity. | Implement robust security measures (e.g., encryption, access controls, compliance with data protection regulations), and carefully plan data transfers between providers to minimize risks during scanning. | Security |
| **CS-16J** | Vulnerabilities | Scalability and Performance | Running security scans at scale in multi-cloud environments | Comprehensive scans across multiple providers consume substantial computing resources and can lead to increased latency, reduced system responsiveness, and potential disruptions to critical operations. | Optimize scan scheduling and resource allocation to minimize performance impacts and ensure that scans are conducted efficiently without disrupting critical operations. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-16K** | Vulnerabilities | Compliance and regulatory challenges | Ensuring security scans meet varying compliance requirements across different cloud providers | Each CSP has unique compliance frameworks and security protocols that require organizations to navigate and align their scanning practices with each provider's specific requirements. | Develop a centralized compliance management strategy that standardizes security scanning practices across providers, leverages expertise and resources, and adheres to all relevant standards. | Security |
| **CS-17A** | Vulnerability Management | Complexity and diversity in addressing vulnerabilities | Managing vulnerabilities in multi-cloud environments with different CSP infrastructures and security tools | The varied nature of these environments results in differing vulnerabilities across providers and complicates efforts to identify and address them consistently and effectively. | Implement a unified vulnerability management framework that standardizes processes across all cloud providers to reduce the risk of misconfigurations and ensure comprehensive security coverage. | Security |
| **CS-17B** | Vulnerability Management | Lack of visibility | Achieving complete visibility into multi-cloud environments | The unique systems and configurations of each cloud provider hinder a comprehensive view of assets and vulnerabilities, which makes it difficult to effectively identify, prioritize, and manage vulnerabilities. | Deploy centralized monitoring and management tools that provide unified visibility across all cloud environments and enable effective vulnerability assessment and consistent security practices. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-17 C** | Vulnerability Management | Inconsistent security configurations | Ensuring consistent security configurations across multiple cloud providers with varying security settings and features | Each CSP's unique security tools and configurations require organizations to invest time in understanding and managing them to maintain a consistent security posture, including configurations made to address hardening requirements or standards. | Establish standardized security policies and practices that can be consistently applied across all cloud providers to ensure a cohesive and robust security framework. | Security |
| **CS-17 D** | Vulnerability Management | Patch management | Coordinating and managing security patch applications across multiple cloud environments with different processes and requirements from various providers | Ensuring that workloads are running the most up-to-date versions of their dependencies is essential, but the task is complicated by the need to manage patch schedules and update procedures across different cloud platforms. | Implementing a centralized patch management system that automates and streamlines updates across all cloud environments can help overcome logistical hurdles and ensure consistent security practices. | Security |
| **CS-17 E** | Vulnerability Management | Integration and compatibility | Ensuring compatibility between vulnerability management tools and the diverse APIs and interfaces of multiple cloud providers | Different levels of support for vulnerability scanning and reporting from each cloud provider necessitate careful integration of tools to effectively monitor vulnerabilities across all environments. | Organizations should adopt flexible vulnerability management solutions that can be customized to work seamlessly with the APIs and interfaces of each cloud provider. | Security |
| **CS-17 F** | Vulnerability Management | Compliance and regulatory requirements | Navigating unique compliance standards from multiple cloud providers | Each CSP's distinct regulations require organizations to align with their own compliance obligations. | Invest in compliance management tools that streamline and automate adherence to diverse regulatory standards across providers. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-17 G** | Vulnerability Management | Prioritization and remediation | Prioritizing and remediating risks in a multi-cloud system with intricate architecture and dependencies | Given the interdependencies between cross-cloud components, prioritization based on defense-in-depth assurance may not be possible due to the lack of data or the complex analysis needed to obtain risk levels. | Develop a comprehensive risk management strategy that includes thorough analysis of system architecture and dependencies to prioritize and address the most critical vulnerabilities first. | Security |
| **CS-17 H** | Vulnerability Management | Resource allocation | Allocating skilled security personnel and tools effectively across multiple cloud providers is difficult, particularly for organizations with limited resources. | Effective vulnerability management in multi-cloud environments necessitates a well-defined strategy for resource allocation to ensure comprehensive coverage. | Develop a strategic plan that prioritizes resource allocation based on risk assessment and criticality across the cloud environment. | Security |
| **CS-17 I** | Vulnerability Management | Reporting consistency | Reporting vulnerabilities and their associated risks when different scanning tools and the aggregation of vulnerabilities from multiple sources are needed | Multi-cloud environments use various vulnerability scanning tools with different naming conventions and depths of scanning and assessing. Centralizing this information in a single report for the entire multi-cloud environment may present challenges given discrepancies in the raw data in different formats. | A centralized and holistic report for vulnerabilities and their associated risks on all cloud platforms can ensure consistency in vulnerability reporting. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-17 J** | Vulnerability Management | Automation of patching | Having automated patching despite incompatibilities in certain cloud environments, dedicated requirements for testing in each cloud environment before patching, and the lack of patching orchestration in a multi-cloud environment | The orchestration of a multi-cloud environment patching process may present compatibility and interconnectivity issues. Certain limitations for patching based on the other technological components may occur in one or more cloud environments, which can limit the automation process. | Creating an automated patching process across a multi-cloud environment | Security |

## A.3. Incident Response

Table 4 enumerates the unique incident response challenges in a multi-cloud architecture.

1227 **Table 4. Incident response challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-18** | Incident Response | Scale of incident response activities | Introduction multiple CSPs, which significantly increases the workload for a traditional incident response team | Each cloud has its own configuration particularities, messaging formats, and procedural requirements. | More consistent and streamlined incident response procedures improve response capabilities and lower the training required for incident response professionals. | Security |
| **CS-19** | Incident Detection | Complexity of attack scenarios and SIEM rules | Detecting incidents as the attack surface area and complexity of aligning sources from multiple clouds increases | Teams need to monitor considerably more platforms and services, regularly evaluate the effectiveness and value of their security monitoring, identify relevant logs, send those logs to the relevant SIEM tool, and create appropriate detection rules with a high level of complexity. | Overcoming this challenge provides a level of assurance for cloud monitoring and software understanding at a similar level to monitoring a single cloud, which increases agility and overall competency in incident response. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-20** | Visibility | Normalization of logging and reporting during the investigation phase | Learning the format and meaning of each platform's audit logging service while adopting multiple clouds | Inconsistent message formats can lead to longer time to remediation and potentially missing important information in an investigation. This creates a greater mental workload for both those crafting security policies and those responding to incidents. | Overcoming this challenge greatly enriches the data that is provided by the multitude of cloud systems that each output their own service-specific logs. Enriching the data will result in faster response times and better investigation outcomes. | Security |
| **CS-21** | Security Operations | Complexity of incident response activities | Varying capabilities across clouds that increase the complexity of thorough and effective incident response processes | Teams may encounter limitations in real-time forensic capabilities in a multi-cloud environment, which can affect proper containment or eradication and the legible correlation of alerts from multiple sources of varying fidelity. | Overcoming this challenge will allow teams to understand incidents more quickly, improve response times, and aid in investigations. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-22** | Interoperability | Lack of standardization across providers | Rejecting security interoperability across cloud providers, which greatly increases the strain on security teams | A lack of standardization across providers has resulted in increased knowledge requirements, procedural complexity, and difficulty in gaining situational awareness. Custom or third-party solutions are often needed, which leads to further complexity. | Overcoming this challenge would lead to higher levels of interoperability, improve security postures, and enhance threat modeling, the creation of playbooks, and incident response simulations. | Security |
| **CS-23** | Containment | Limitations in containment across multiple cloud environments | Limitations in the automated and manual containment of security incidents that involve multiple cloud environments | The automated containment or swift manual containment of affected assets may be affected by limited connectivity, authentication, authorization, and/or the interoperability of containment tools. | Overcoming this challenge would improve the containment of affected assets across multiple cloud environments | Security |
| **CS-24** | Recover | Limitations in fulfilling RTO and RPO | Limitations in ensuring the fulfilment of RTO and RPO given complex scenarios that should be considered and regularly tested | Applications on multiple cloud environments may have different versions of operating systems or databases, which could challenge the feasibility of fulfilling envisaged RTO and RPO. | Overcoming this challenge would ensure the fulfilment of RTO and RPO. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-25** | Reporting | Limitations in holistic and aggregated reporting | Limitations in aggregating the data needed for reporting | Significant manual effort may be needed to ensure that all relevant data from all cloud environments are analyzed from a reporting perspective and included in the reports to management and/or relevant authorities. | Overcoming this challenge would create aggregated and holistic reports on the incident | Security |
| **CS-26** | Lessons learned | Difficulty in identifying root causes | Limitations in swiftly identifying the root cause and attack pathway of an incident | Significant time and effort may be required to identify the root cause and attack pathway of an incident to clearly formulate lessons learned from both an incident management process and security posture perspective. In some cases, the accuracy of such conclusions may not be high. | Swiftly identifying accurate lessons learned can improve the incident management process and security posture. | Security |

## A.4. Architecture

Table 5 enumerates the unique architecture challenge in a multi-cloud architecture.

**Table 5. Architecture challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-23** | Architecture | Cross-cloud alignment of best practices | Implementing security practices for CSP customers, which may leave gaps or potentially conflict with one another | Each CSP, regardless of service type, typically provides best security practices and architectures to their customers. In a multi-cloud environment, security expertise is required to analyze these practices and architectures and synthesize them into a cohesive implementation. | Utilizing appropriate security expertise can eliminate security gaps between services and components, reduce overhead, and simplify auditing. | Security ATO |
| **CS-24** | Architecture | Contingency planning | Increased difficulty in mapping a business process to a set of IT assets to support a proper business impact analysis and contingency plan | CSP services must be chosen to support the recovery metrics of the business process. Because each service is from a different provider, it may be difficult to align capabilities and recovery SLAs to support the information system. Multiple cloud services may support different business processes, making this alignment even more difficult. | Overcoming this challenge would create business process/IT alignment and robust resiliency planning.<br><br>It would also increase confidence in ability to continuously operate in a disaster scenario<br>More purposeful resource allocation | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-25** | Architecture | Security application mismanagement | Choosing applications that offer simplified visibility into multi-cloud environments | Vendors do not typically promote interoperability between services or tooling. Those that do function as aggregators that may not meet the functional requirements of the information system or the feature requirements of its users. | Promoting interoperability and visibility into multi-cloud environments reduces incident response time, increases the robustness of responses, and informs future investigations. | Security |
| **CS-26** | Architecture | Larger attack surface | Effectively managing security for complex multi-cloud environments with an increased potential for security vulnerabilities | The varied and complex nature of multi-cloud environments increases the potential for security vulnerabilities. For example, an API endpoint that is publicly accessible in Google Cloud might make that particular environment vulnerable to attacks, whereas an improperly set IAM policy in AWS could permit unauthorized access to its resources. These two vulnerabilities could result in a unique and opaque threat scenario that requires specialized capabilities or expertise to identify. | Effectively managing security and reducing the attack surface can improve monitoring. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-27** | Architecture | Segmentation | Skipping certain services in one or more CSPs in a multi-cloud environment, which may cause segmentation to lose its value | Failing to consistently apply controls across CSPs and services may create gaps that undermine the overall effectiveness of segmentation. | Properly considering the services in all clouds upon successful data flow and asset mapping as well as the purpose of each segment can improve architectural consistency and enable the uniform application of security controls. | Security |
| **CS-28** | Architecture | Threat modeling | Clearly identifying and reducing the attack surface of the system | Threat modeling in a multi-cloud environment requires a holistic view of complex threats, asset identification, and modeling complex interactions between services from multiple CSPs. The unique characteristics of services (particularly those involving key management, identity, and network configuration) across different providers add additional considerations and risks. | Proper threat modeling can reduce the attack surface and lead to the uniform application of security controls, targeted risk mitigation, and architectural revision. | Security |
| **CS-29A** | Boundary | System boundary definition | Defining system boundaries while considering additional complexities regarding responsibility and control | Each shared responsibility model may have different customer responsibilities for similar controls and may apply them to different types of assets within the cloud service, even when the assets are similar. | Properly defining system boundaries allows for full control implementation, establishes a body of evidence for the system's shared responsibility model, and clearly delineates responsibilities across the system. | ATO |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-29B** | Boundary | Evaluation of the system boundary | Communicating the type of inheritance or origination for a control across multiple clouds in a way that clearly communicates what must be assessed and how | Control origination may vary depending on the shared responsibility model and organizational complexities. Controls for one cloud offering may originate from one division or team, while those for another offering originate from another, making it difficult to determine responsibility and apply controls effectively. | Proper boundary evaluation and communication can improve the consistent application of security controls, identify responsibilities, and improve auditability. | ATO |
| **CS-30** | Cryptography Management | Differences in cryptographic capabilities and implementations | Managing cryptographic mechanisms in a multi-cloud environment and resolving issues that result from their mismanagement | The security of cryptographic mechanisms can vary based on different algorithms, technologies, PKI infrastructures, and the management capabilities of each CSP. | Correct, secure, and effective cryptographic mechanism implementation and management can resolve issues more effectively. | Security |
| **CS-31** | Lateral Movement | Data movement between CSPs. | Identifying and securing chains of weaknesses and opportunities for movement between providers | The complexity of cloud environments makes it difficult to identify and secure opportunities for lateral movement between providers. This ties directly to identity and the difficulty of limiting privileges in a complex cloud environment. | Properly identifying and securing opportunities for lateral movement can reduce the attack surface and improve the security posture. | |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-32A** | Shared Responsibility | Identifying practical differences between models | Identifying the practical differences between shared responsibility models and aligning them to an organization's business processes and structure | As more cloud services are brought into a system, the scope of the customer's responsibility increases. Differences in terminology, capabilities, and CSPs' interest in presenting themselves as uniquely suited to addressing various customer scenarios present additional complexity. | Cross-functional collaboration and upper management involvement in seemingly low-level decision-making can align the various shared responsibility models, eliminate gaps in implementation requirements, streamline and simplify business processes and architectures, and identify effective and secure solutions. | Security |
| **CS-32B** | Shared Responsibility | Verifying the proper implementation of shared responsibilities | It is difficult to identify the practical differences between shared responsibility models and, by extension, to develop a comprehensive, testable body of evidence. | The chosen solutions may not perfectly align with the requirements defined in a particular service's shared responsibility model. Care must be taken not only to ensure the solution meets the security needs of the multi-cloud environment, but that evidence can be aligned with those seemingly mismatched requirements. | | ATO |

## A.5. Data Protection

Table 6 enumerates the unique data protection challenges in a multi-cloud architecture.

**Table 6. Data protection challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-33** | Data Protection | Governance | Adapting governance frameworks to account for various regulatory requirements across different jurisdictions | Establish and enforce a formal data-protection governance framework, including policies, roles, and responsibilities for handling sensitive customer data. | Form a cross-functional Data Governance Board with codified ownership and stewardship policies and quarterly policy reviews. Post-implementation audits should show 100 % policy adherence and zero incidents of unmanaged data access. Requirements must also be adaptable across different CSPs to ensure comprehensive alignment for the organization. | Security |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-44** | Data Protection | Customer information location | Locating customer data within a multi-cloud system despite differences in visibility and implementations across CSPs | Maintaining control over data location is critical for meeting regulatory obligations and ensuring that data protection measures, access controls, and compliance requirements are applied consistently across cloud platforms. | Complete a comprehensive data-location mapping across all environments, and implement geo-fencing to restrict data replication to approved regions. Maintain an accurate inventory of where customer data is stored, processed, and backed up, and update system documentation. Validation during the ATO assessment will confirm full compliance with locality constraints. | ATO |
| **CS-45** | Data Protection | Jurisdictional complexity | Accounting for conflicting or overlapping regulatory requirements as data traverses multiple jurisdictions | Address legal and regulatory complexities that may arise from cross-border data flows by implementing controls for multi-jurisdiction compliance. | Develop a cross-border data transfer framework, classify data based on jurisdictional risk, and enforce conditional access policies. External legal reviews and subsequent ATO approval will validate that all international data handling meets applicable laws. | ATO |

## A.6. Contingency Planning and Disaster Recovery

Table 7 enumerates the unique contingency planning and disaster recovery challenge in a multi-cloud architecture.

**Table 7. Contingency planning and disaster recovery challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-46** | Failover/Redundancy | Failover planning | Inadequate failover planning that fails to properly take all cloud services into account | Failover planning is an essential part of ensuring continued operations in a disaster situation. In a multi-cloud environment, it can be difficult to ensure that failover planning covers every system, which can impact disaster recovery and business continuity planning. | Proper failover planning can improve recovery times, minimize downtime, protect data, and enhance operational stability. | |
| **CS-47** | Failover/Redundancy | Integration complexity | Implementing cohesive disaster recovery and business continuity planning for diverse architectures across multi-cloud environments | Identifying dependencies across multiple cloud providers can be challenging, including identifying roles in business processes and compensating measures in a disaster scenario. | A streamlined and efficient recovery process can lead to quicker response times during disasters and a unified approach to maintaining continuity across diverse infrastructures. | ATO |
| **CS-48** | Failover/Redundancy | Comprehensive component coverage | Failing to consider all components (e.g., DNS, external servers) in a multi-cloud environment and creating gaps in recovery plans | Components in one provider may depend on other providers or components in another provider for full functionality. | Considering all components can lead to a more robust and complete disaster recovery strategy that reduces the risk of gaps and ensures faster, more reliable system restoration. | ATO |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-49** | Failover/Redundancy | Data security | Jeopardizing data integrity and compliance through insecure or poorly managed failover processes | Without a full understanding of the security control dependencies in a multi-cloud system, data may be exposed during a disaster scenario. | Strengthened security during failover processes can improve data integrity, ensure compliance with regulations, and reduce the risk of security breaches or data loss during recovery efforts. | ATO |
| **CS-50** | Failover/Redundancy | Alert fatigue | Overwhelming monitoring systems with the volume of alerts generated by CSPs, leading to critical incidents affecting failover and recovery processes | Without a clear understanding and presentation of the connections between these alerts, it is difficult for incident response personnel to determine how they are connected, what the implications may be, and the appropriate course of action to address the incident. | Improving the efficiency of monitoring systems enables better prioritization and management of alerts and faster reactions to critical alerts. | Security |
| **CS-51** | Failover/Redundancy | Unified contingency or disaster response | Coordinating response efforts across multiple services in the event of a failure | Every CSP has their own SLAs and standards for interacting with their customers. If consumers of multiple cloud services do not have rehearsed, defined protocols and methods of coordination, incident response activities can be uncoordinated and delayed. | Clear communication and coordination can improve response times. | |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-52** | Contingency | Alignment of SLAs | Aligning SLAs among CSPs, including timing and availability | Failure to consider the RTOs and RPOs of multiple cloud services may result in unforeseen interservice dependencies and delayed recovery. | Organizations must consider the timing and availability differences resulting from provider SLAs to improve recovery time. | |
| **CS-53** | Contingency | Diverse recovery processes | Create a cohesive and efficient incident response strategy in a multi-cloud system | Failure to consider different recovery processes and protocols across multiple CSPs can result in incoherent recovery processes and wasted effort and time in a disaster scenario. | A cohesive and efficient incident response strategy will improve recovery and save time after an incident. | |
| **CS-54** | | Resource allocation for testing | Straining resources while testing and validation contingency plans across a multi-cloud environment | Resource constraints can lead to oversights in contingency planning and testing that potentially create gaps in preparedness and compromise the organization's ability to recover. | Properly analyzing the costs and benefits of contingency plan testing can improve overall disaster preparedness and recovery times. | |
| **CS-55** | | Data consistency | Ensuring data consistency and integrity despite varying replication and synchronization methods across cloud environments | Inconsistent data handling can cause discrepancies, stale data, or even data loss, which impacts the application's reliability and performance and ultimately erodes trust in the data. | Data consistency and integrity across cloud environments can ensure accurate data recovery and minimize the risk of data discrepancies. | |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-56** | | Data silos | Fragmented data across different cloud providers leading to visibility gaps | If data is fragmented across different cloud platforms, it becomes difficult to gain a holistic view of the system and analyze the data in a meaningful way. This fragmentation prevents users from having a real-time view of the infrastructure, which can result in missed issues, incomplete contingency planning, and disjointed recovery processes. | A unified view of data across multiple cloud providers improves visibility, enables more effective contingency planning and decision-making, and leads to smoother recovery processes. | |
| **CS-57** | | Integration complexity | Integrating monitoring tools and processes across multiple cloud environments, which can create compatibility issues and hinder effective contingency planning and execution | When monitoring tools do not work seamlessly together, various issues can occur (e.g., blind spots, fragmented visibility). This can make it harder to detect issues and respond effectively during incidents. | Improved visibility and alignment across systems leads to more efficient contingency planning and execution, faster detection of issues, and a more coordinated, effective response during disasters. | |

## A.7. Business Operations

Table 8 enumerates the unique business operation challenges in a multi-cloud architecture.

**Table 8. Business operation challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-58** | Business Operations | Costs resulting from complexity | Increasing costs through tool and process bloat | Each tool added to an environment adds to monitoring and operational overhead, such as new business processes for managing these tools, their output, and their operations. These bespoke processes may confuse personnel and cause significant inefficiencies. | Deliberately and purposefully selecting and implementing system capabilities reduces tool footprint and ensures efficient alignment with the organization's overall strategies. | |
| **CS-59** | Business Operations | Cost resulting from misalignment in provider capabilities | Controlling the costs associated with different CSPs | Opaque pricing models and scaling usage can result in security tool failure, including the loss of access to audit logs, monitoring information, and data ingest. | Keeping within expected cost deviations and properly planning for cost overrun scenarios can ensure continued operations and reduce business risks. | |
| **CS-60** | Business Operations | Talent — Capabilities | Hiring talent with the requisite knowledge to secure services and the aggregate environment that they support | Security personnel must understand specialized technical concepts as well as the nuances of each service at the architectural level, which could increase the number of personnel needed and reduce the potential talent pool. | Improve talent acquisition by selecting the right personnel for roles. | |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-61** | Business Operations | Talent — Breadth of responsibility | Personnel may be responsible for multiple things at once (e.g., network security, IAM, patching, configuration management) | Rather than traditional vertical stove piping of responsibilities, cloud environments tend to cut across them horizontally and put responsibility for multiple domains on a single team (DevSecOps is a perfect example). This increases the scope of responsibility for each team, potentially past their existing expertise. | Selecting personnel who have the experience and can be responsible for multiple domains. | |

## A.8. Configuration Management

Table 9 enumerates the unique configuration management challenges in a multi-cloud architecture.

**Table 9. Configuration management challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-62** | System Configuration | Niche configuration requirements | Catching misconfigurations and different implementations for the same security requirement among different CSPs | CSCs need to confirm that the CSPs implement their secure configurations, which may be unique to their business and mission requirements. This process may include reviewing configuration scans conducted by the CSPs or the CSCs. | The authorizing entity will be able to verify the consistent implementation of the CSC's baseline configuration. The CSC will also be able to verify that the CSPs have implemented their configurations and that the CSC's configurations have not been modified. | Security/ ATO |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-63** | System Configuration | Translating configuration requirements across providers | Replicating one set of configurations to another CSP, given the different mechanisms for enforcing such configurations | CSCs need the capability to replicate their secure configurations across all CSPs, regardless of the CSP's cloud architecture. CSCs will need to confirm that their secure configurations are implemented by the CSPs. | The authorizing entity will be able to verify the consistent implementation of the CSC's baseline configuration. The CSC will also be able to verify that the CSPs implement their configurations and that the CSC's configurations have not been modified. | Security/ ATO |
| **CS-64** | System Configuration | Consistency of configurations | Maintaining synchronized configurations on multiple CSPs | CSCs need to confirm that the CSPs implement their secure configurations by reviewing configuration scans conducted by the CSPs or CSCs. | The authorizing entity will be able to verify the consistent implementation of the CSC's baseline configuration. The CSC will also be able to verify that their configurations have not been modified. | Security/ ATO |

## A.9. Documentation

Table 10 enumerates the unique documentation challenge in a multi-cloud architecture.

**Table 10. Documentation challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-100** | Scope | Accurate documentation of system scope | Opportunities for ambiguity or misattribution when representing the system scope across different cloud services | Due to differences in cloud-native services, documentation for a system that is deployed across two or more CSOs and leverages services from those CSOs risks documenting the leveraged service if they are equivalent but have key differences. | At a minimum, system documentation clearly identify the services that are being leveraged from each CSO and ensure correct attribution of the service to the appropriate CSO. A documentation standard should emerge, and cloud-agnostic solutions should be favored where practical. | ATO |
| **CS-101** | Components | Accurate documentation of component deployment | Opportunities for ambiguity or different details when deploying the same component into two different CSOs with two different hypervisors | Each CSO has different hypervisors and approaches to virtual machines, containers, networking, and other components. While the goal may be an identical deployment of components in two or more CSOs, technical constraints may require some differences in deployment mechanisms or configuration details. | Differences should be properly captured and attributed to the correct CSO deployment. Ideally, a documentation standard should emerge, and cloud-agnostic solutions should be favored where practical. | ATO |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-102** | Responsibilities and Ownership | Accurate documentation of administrative responsibilities and component ownership | Documenting the ownership of and responsibilities for a component that may be administered by different teams based on the CSO in which it is deployed | Due to differences in cloud-native administration and the complexities involved, many organizations need different teams for each major CSO. As a result, the same component may be managed by one team for the first CSO and a different team for the second CSO. | Differences should be properly captured and attributed to the correct CSO deployment, and the number of administrative teams involved should be minimized. Ideally, a documentation standard should emerge, and cloud-agnostic solutions should be favored where practical. | ATO |

## A.10. Certification and Authorization

Table 11 enumerates the unique certification and authorization challenges in a multi-cloud architecture.

**Table 11. Certification and authorization challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-110** | Authorization Boundary | Appropriate authorization boundary is defined | Defining an appropriate authorization boundary | Clearly defining a system authorization boundary is complicated by differences in virtual private clouds/networks between in-scope CSOs, design decisions to only host certain services in only one of the CSOs (e.g., centralized logging), and differences in the possible communication pathways between deployments in different CSOs (e.g., dedicated circuits, internet-traversing VPN tunnels). | Differences should be properly captured and attributed to the correct CSO deployment. Ideally, a documentation standard should emerge, and cloud-agnostic solutions should be favored where practical. | ATO |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| | Control Satisfaction | Accurate documentation of differences in control inheritance and satisfaction | Satisfying controls differently between CSOs | Differences in the way each CSO's cloud-native services are implemented can result in inconsistent control satisfaction among leveraged CSOs, such as differences in how each handles logging. | Differences should be properly captured and attributed to the correct CSO deployment. Ideally, a documentation standard should emerge, and cloud-agnostic solutions should be favored where practical. | ATO |

## A.11. Meta Challenges

The following table enumerates each meta-challenge unique to the other challenges of a multi-cloud architecture.

**Table 12. Meta challenges in a multi-cloud architecture**

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-65** | Policy | Creating and applying security policies. | Writing and applying policies that provide a coherent statement on security objectives and implementation | Adopting multiple clouds complicates security policy generation and application because it means considering multiple types of security architectures and the divergent properties of underlying services and applications. | *This field left intentionally blank; this will differ depending on many contextual factors.* | *This field left intentionally blank; this will differ depending on many contextual factors.* |

| ID | Subcategory | Short Title | Challenge | Description | Result of Overcoming Challenge | Security or ATO |
|---|---|---|---|---|---|---|
| **CS-66** | Inventory | | Creating an inventory of a cloud environment as the resources on it expands | Creating a complete inventory of a cloud environment requires considering the architectural requirements and dependencies across services in the platform. Maintaining a centralized or correlated decentralized inventory can be difficult to achieve given the differences in data structures per CSP and the manner in which such data can be transferred into inventory solutions. | *This field left intentionally blank; this will differ depending on many contextual factors.* | *This field left intentionally blank; this will differ depending on many contextual factors.* |
| **CS-67** | Environment of Operation | Consistency of operations | Creating consistency across operating environments as more clouds are adopted | Maintaining consistent operations for application developers is difficult as more tools are adopted to address caveats in specific environments. | *This field left intentionally blank; this will differ depending on many contextual factors.* | *This field left intentionally blank; this will differ depending on many contextual factors.* |

1253

## Appendix B. List of Symbols, Abbreviations, and Acronyms

**CSC**
Cloud Service Consumer

**CSO**
Cloud Service Offering

**CSP**
Cloud Service Provider

**ICAM**
Identity, Credential, and Access Management

**IR**
Interagency Report

**MCSPWG**
Multi-Cloud Security Public Working Group

**MTTD**
Mean Time to Detect

**MTTR**
Mean Time to Respond

**NIST**
National Institute of Standards and Technology

**SSP**
System Security Plan

**VPC**
Virtual Private Cloud

# Appendix C. Glossary

**authorizing official (AO)**
An executive within an organization who is empowered to issue an *authorization to operate (ATO)* for a system. For example, the United States Federal Information Security Modernization Act (FISMA) empowers US Agency CIO as the authorizing official for all systems operating on behalf of that agency.

**authorization to operate (ATO)**
Formal permission for a system to be used by an organization. This is usually granted by an empowered executive within the organization.

**control**
This is typically a shorthand reference to a *control definition*, *control implementation*, or *control response*, depending on context.

**control definition**
A security or regulatory requirement statement that is imposed on a system.

**control implementation**
An implemented capability within a system (technical) or in support of a system (organizational) intended to satisfy a control definition that has been imposed on the system.

**control response**
A written explanation that identifies a specific control definition and describes the control implementation.

**cloud service consumer (CSC)**
The customer or end user of a *cloud service offering (CSO)*.

**cloud service provider (CSP)**
An organization that provides cloud services.

**cloud service offering (CSO)**
A system based on cloud technologies that is owned by a CSP and is available to *customers*.

**customer**
A person or organization paying for the *CSO* or an end user who relies on the *CSO*. See *CSC*.

**system security plan (SSP)**
A document that describes the security mechanisms in a system. Typically expressed in response to the control definitions within a governing cybersecurity framework.

**system**
Unless otherwise specified, a reference to the cloud workload on which this document focuses. Also referred to as "the system."

**virtual network**
Customer-managed virtual networks within a *CSO*, which are often private and critical to the workload's function. Similar to a *VPC*.

**virtual private cloud (VPC)**
An industry-generic term for a private network section within a public cloud environment.