AICPA SOC 2 Compliance Guide on AWS

July 2025

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS's current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

Effectively achieving Systems and Organization Controls (SOC 2) compliance in AWS environments requires a principled yet practical approach to implementing controls that align with the AICPA's Trust Services Criteria (TSC). Unlike checkbox-driven audits, SOC 2 emphasizes risk-based, continuous assurance of an organization's ability to protect systems and data across security, availability, processing integrity, confidentiality, and privacy dimensions.

This whitepaper provides guidance for organizations designing and operating workloads in Amazon Web Services (AWS) to meet SOC 2 expectations. It focuses on translating abstract control criteria into actionable technical and procedural controls—using AWS-native services for automation, visibility, and enforcement. From identity and access governance to incident response readiness, each control area is addressed with real-world AWS service mappings and implementation guidance.

While AWS SOC reports cover the security of the cloud, this whitepaper emphasizes SOC 2 compliance in the cloud—focusing on the customer's responsibilities within their own AWS environment.

Intended for cloud security architects, DevOps engineers, compliance leads, and third-party auditors, this paper demystifies SOC 2's flexible framework and demonstrates how AWS customers can confidently manage their control environment, prepare audit-ready evidence, and sustain ongoing compliance at scale.

The content is for illustrative and educational purposes only and does not constitute compliance or audit advice. Customers are responsible for interpreting and applying SOC2 requirements based on their specific environment.

Introduction

As service organizations increasingly migrate their systems, workloads, and data to Amazon Web Services (AWS), the need to demonstrate trust, accountability, and control effectiveness becomes more critical. Customers and business partners demand assurance that cloud-hosted systems are secure, available, confidential, and privacy-conscious.

In this context, providing formal assurance through industry-standard frameworks is a strategic and operational imperative. One of the most recognized and widely adopted assurance frameworks in the United States is SOC 2 (System and Organization Controls 2), developed by the American Institute of Certified Public Accountants (AICPA).

SOC 2 compliance and the examination associated with achieving a favorable SOC 2 report helps organizations demonstrate that they have implemented effective controls aligned to Trust Services Criteria (TSC) referenced in AICPA guides and that those controls operate consistently in AWS environments.

The SOC 2 framework evaluates whether a service organization's systems are designed and operating effectively to meet criteria in one or more of five categories: Security, Availability, Processing Integrity, Confidentiality, and Privacy. These TSC, most recently updated in 2017, are principle-based and map to COSO's internal control framework.

Note: AWS SOC reports—representing *of the cloud* compliance—do not include the Processing Integrity category in their scope. Customers pursuing SOC 2 for their workloads in the cloud should independently assess and implement controls aligned to Processing Integrity, where applicable, based on their own service delivery commitment

This whitepaper provides a structured, practical guide for aligning AWS-based workloads and infrastructure with SOC 2 TSC. It is designed to help organizations understand, implement, and maintain effective controls that meet SOC 2 expectations in the cloud.

Readers will gain clarity on:

- How SOC 2 criteria work
- What controls are expected
- How to implement and validate those controls in AWS
- How to prepare evidence for Type 1 or Type 2 audits

This paper is designed for security architects, compliance professionals, DevOps engineers, auditors, and any stakeholder seeking audit readiness and operational assurance in AWS.

SOC 2

System and Organization Controls 2 (SOC 2) is a compliance framework developed by the American Institute of Certified Public Accountants (AICPA) to help service organizations demonstrate that their systems are designed and operating effectively to meet categories related to:

- Security
- Processing Integrity
- Availability
- Confidentiality
- Privacy

These are collectively known as the *Trust Services Criteria (TSC 2017)*. Each organization undergoing a SOC 2 audit must select which categories are applicable based on the nature of its services and customer commitments. SOC 2 examination comes in two types:

- **Type 1:** Examines the design of controls at a point in time
- **Type 2:** Examines both the design and operating effectiveness of controls over a review period (for example, 6–12 months)

SOC 2 framework is not prescriptive. It provides criteria but not a fixed control list, offering organizations the flexibility to design controls suited to their environment—especially relevant in dynamic cloud contexts such as AWS.

For official references, see AICPA Trust Services Criteria and SOC 2 Resources.

Understanding the SOC 2 framework

The SOC 2 framework is built on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework, which outlines five components of internal controls. The AICPA TSC (TSC 2017) adopts these principles and organizes them into:

- Common criteria for security (CC1 to CC9)
    - These apply to all SOC 2 audits, regardless of which TSC are in scope
    - Address control areas like governance, risk assessment, access control, system operations, and monitoring
- Category-specific criteria (Additional criteria apply only if the organization includes that category in its SOC 2 scope):
    - PI1 (Processing Integrity)
    - A1 (Availability)
    - C1 (Confidentiality)
    - P1–P8 (Privacy)

Each criterion includes:

- **A control objective**: What must be achieved
- **A list of points of focus**: Suggested elements that a well-designed control might include

Auditors assess:

- **Design effectiveness**: Is the control likely to meet the objective?
- **Operational effectiveness (Type 2 only)**: Did it operate consistently during the review period?

The TSC framework can be reviewed in detail using AICPA criteria documentation.

Figure 1 maps SOC 2's Trust Services Criteria—Security, Availability, Processing Integrity, Confidentiality, and Privacy—to the COSO framework, showing how internal controls are layered within the organization's governance and risk environment, in line with AICPA's principle-based approach.

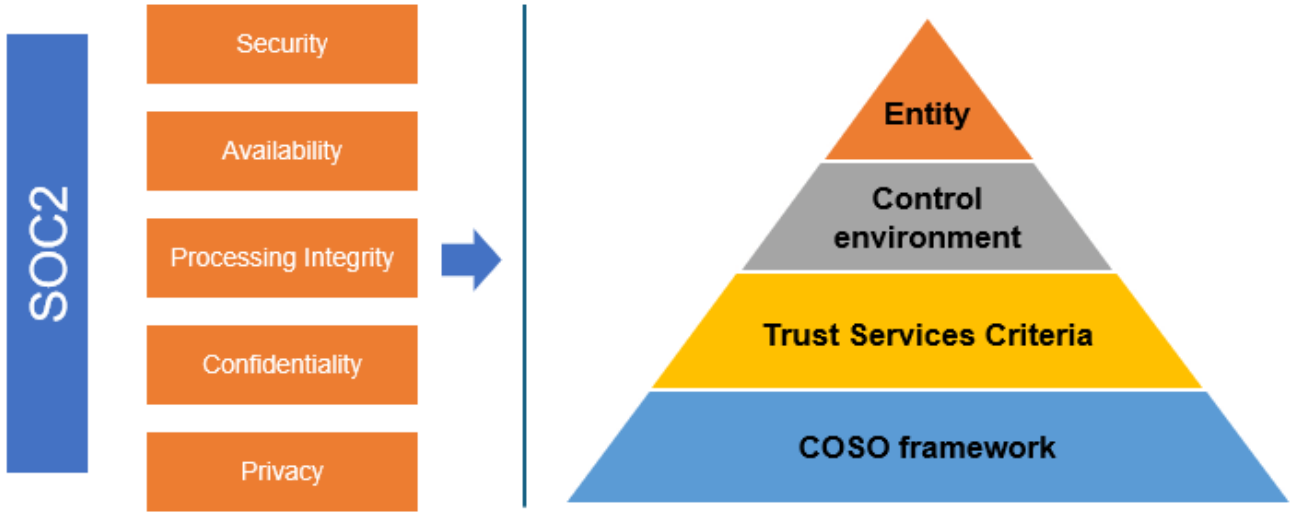

Figure 1: SOC2 TSC and COSO internal control framework

SOC 2 in AWS context

In cloud environments like AWS, implementing SOC 2 controls requires interpreting the TSC within the *shared responsibility model*:

- **AWS** is responsible for the security *of* the cloud (for example, the data center, hardware, and network infrastructure)
- **Customers** are responsible for the security *in* the cloud (for example, identity management, data encryption, logging, and network controls)

This division makes it critical that customers:

- Understand which SOC 2 TSC AWS helps address
- Know what remains their responsibility
- Design controls that use AWS services, such as AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), AWS Config, and AWS CloudTrail
- Document and monitor those controls to demonstrate effectiveness

The flexibility of SOC 2 means each organization must define its own control set. This whitepaper helps translate SOC 2 criteria into actionable customer controls using AWS services and governance structures, aligning technical operations with audit expectations.

While AWS provides a secure and compliance-aligned foundation, organizations remain responsible for implementing all controls within their own AWS environment—this includes how workloads are architected, how identities are managed, how data is protected, and how governance is enforced.

This whitepaper provides practical guidance on how customers can implement controls *in the cloud*, specifically within the scope of their AWS accounts, services, and infrastructure. By interpreting each SOC 2 Trust Services Criterion through the lens of the AWS shared responsibility model, we help customers bridge control expectations with practical implementation steps.

The following sections walk through each SOC2 control criterion, offering practical insight into:

- How customers can interpret and apply each criterion within their AWS environment by identifying controls that align with the TSC and related points of focus
- Which AWS services support compliance
- What configuration decisions must be made
- What remains the customer's responsibility (for example, policies, processes, and reviews).

AWS Shared Responsibility model and its role in SOC 2

The AWS Share Responsibility Model states that "Security and compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Customers are responsible for managing the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall."

In the context of customer SOC 2 assessments, this shared responsibility model clarifies which control objectives can be inherited from AWS and which must be implemented by the customer directly within their cloud workloads. AWS provides secure infrastructure and services, but the customer is accountable for how those services are configured, used, and monitored.

- AWS is responsible for the physical security of its data centers and the isolation of customer environments through hypervisor-level controls. These measures support CC6.4 (logical and physical access controls at the infrastructure level) by helping to prevent unauthorized physical or virtual access to customer workloads.
- Customers are responsible for implementing tenant-level controls, such as IAM role design (CC6.1), KMS policy enforcement (CC5.2), backup strategies, and logging configurations (CC7.x), to satisfy their part of the SOC 2 requirements.

Note: Specific control mappings, responsibilities, and implementation actions are provided in the subsequent sections and detailed tables.

By understanding this delineation, customers can effectively scope, implement, and document their own controls that satisfy SOC 2 requirements while using the built-in assurances provided by the AWS compliance program.

For more details, see the AICPA SOC 2 Resource Library and AWS Compliance Center.

Customers can refer to AWS Prescriptive Guidance to design and implement controls appropriate for their specific environment and compliance needs. These resources provide strategies and patterns that align with AWS best practices and can help organizations operationalize their SOC 2 responsibilities more effectively. When used in conjunction with the

AWS Shared Responsibility Model, this guidance enables customers to architect, configure, and validate controls across security, availability, and privacy domains.

The boundaries of responsibilities between AWS and the customer can vary depending on the AWS services selected. Customers can assess each service operational model and understand how responsibilities shift accordingly.

Complementary User Entity Controls: Customer responsibilities in the cloud

Complementary User Entity Controls (CUECs) are control activities that a service provider expects its customers (user entities) to implement for the provider's controls to function effectively. These controls are disclosed in the service provider's SOC 2 report, not as part of the TSC, but as required contextual disclosures under the AICPA SOC 2 reporting framework.

CUECs are not optional. If the customer fails to implement these controls, the effectiveness of the overall system might be compromised—even if the provider's controls are working as intended.

CUECs and the Shared Responsibility Model

In the context of AWS, the Shared Responsibility Model defines which controls AWS manages (for example, infrastructure security, physical access, and hypervisors) and which controls customers must implement (for example, access management, data protection, and monitoring).

AWS discloses CUECs in its SOC 2 Type II report to communicate the expectations placed on customers. These typically include areas such as:

- Managing IAM roles and permissions
- Encrypting and backing up data
- Reviewing logs and responding to security alerts
- Securing user devices that access AWS services

Thus, CUECs reflect the customer-side of the shared responsibility model, reinforcing the areas that must be addressed by the customer for a secure and compliance-aligned AWS implementation.

Organizations pursuing SOC 2 for workloads running on AWS should:

1. Review the CUECs disclosed in the AWS SOC 2 report
2. Map those CUECs to their own internal control activities
3. Implement supporting policies, procedures, and technical configurations
4. Provide evidence (for example, IAM policies, backup jobs, and incident response logs) that these controls are operating effectively

Figure 2 Shows how SOC 2 TSC, the AWS Shared Responsibility Model, and Complementary User Entity Controls (CUECs) interrelate in the context of a customer's SOC 2 audit. The customer implements the controls needed to support AWS controls (CUECs). The CUECs feed into the Shared Responsibility Model, which defines who is responsible for each of the TSC.

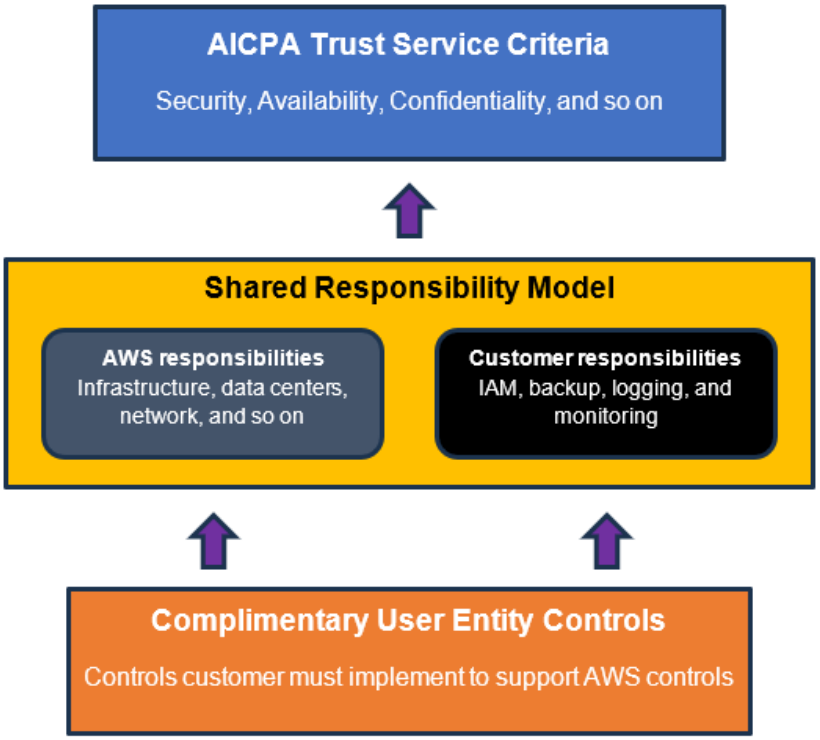

Figure 2: The relationship of the CUEC, AWS Shared Responsibility Model, and TSC

Applying SOC 2 TSC in AWS environments

The SOC 2 framework defines a series of control criteria that service organizations must meet to demonstrate effective system design and operational performance aligned with the TSC. These criteria include both the foundational Common Criteria for Security category (CC1–CC9) and the Category-Specific Criteria for Availability, Processing Integrity, Confidentiality, and Privacy.

Understanding the boundary between AWS and the customer, defined by the AWS Shared Responsibility Model, is only the starting point. This model distinguishes which security and compliance responsibilities are managed by AWS (for example, infrastructure, hardware, and physical access) and which are managed by the customer (for example, data protection, IAM, and workload configurations).

The next step is to translate SOC 2's principle-based and high-level control criteria into specific, actionable responsibilities, technical implementations, and supporting evidence within the customer's AWS environment.

This control mapping section provides practical implementation guidance to help customers:

- Interpret each SOC 2 control criterion within the context of their AWS environment
- Implement technical controls using AWS services and secure configurations
- Define supporting organizational policies, procedures, and governance activities outside of AWS
- Use the publicly available points of focus as interpretive aids to guide control implementation and evidence collection

Each of the following sections outlines:

- A short narrative explaining the purpose of each control area
- Practical AWS service recommendations to support compliance
- Tables that describe SOC 2 control objectives, customer responsibilities in AWS, external controls, and associated points of focus.

This structured approach helps cloud-focused organizations bridge the gap between high-level SOC 2 expectations and practical, verifiable implementation within their AWS environments—supporting both operational maturity and audit readiness.

Note: Many technical and procedural controls can satisfy multiple SOC 2 TSC. For example, a well-configured logging and monitoring solution can address requirements under both Security (CC7.x) and Availability (A1.x). Customers are encouraged to identify opportunities to reuse and align controls across criteria, reducing redundancy and improving audit efficiency. Clear documentation and traceability of such control mappings are essential for demonstrating compliance coverage.

CC1 series: Control Environment

The Control Environment (CC1 series) criteria establish the overall foundation for an effective system of internal control, as defined in the AICPA 2017 TSC.

These criteria help ensure that the entity demonstrates commitment to integrity and ethical values, establishes appropriate governance and oversight structures, defines clear roles and responsibilities, attracts and retains competent individuals, and holds individuals accountable for their internal control responsibilities.

In AWS-hosted environments, such as cloud-focused applications, serverless workloads, or regulated financial services products, the control environment remains the customer's responsibility.

AWS provides tools and services that can support the enforcement, monitoring, and auditing of control activities (for example, IAM, CloudTrail, AWS Config, AWS Organizations service control policies (SCPs), and attribute-based access control (ABAC) policies), but organizational leadership, governance, people management, policies, and accountability structures are entirely owned and operated by the customer.

Customers are responsible for configuring AWS security and access controls (IAM, Organizations SCP, and AWS Config) in line with their organizational policies and for helping to ensure that these configurations are tied into broader internal control structures, accountability models, and governance reporting mechanisms.

When aligning with the SOC 2 TSC, organizations should use the points of focus as interpretive guidance to assess the completeness and effectiveness of their control implementation. While the points of focus are not mandatory or prescriptive checklists, they provide useful context for demonstrating how specific criteria are met.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
CC1.1: The entity demonstrates a commitment to integrity and ethical values.	• Considers contractors and vendor employees in demonstrating its commitment	• To demonstrate AWS commitment, obtain third-party attestation reports from AWS Artifact
CC1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	• Not applicable	• No AWS specific implementation
CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	• Defines, assigns, and limits authorities and responsibilities	• To address strict segregation of duties, implement IAM and AWS IAM Identity Center role-based access control (RBAC) and resource access controls
CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	• Provides training to maintain technical competencies	• To assess individual technical competency, use the AWS Certification and Training program
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	• Enforces accountability through structures, authorities, and responsibilities	• To enforce individual accountability, enable logging with CloudTrail and user activity monitoring with Amazon CloudWatch

Non-AWS implemented controls (organizational, process, and people):

- Make sure that the members of the board have the necessary AWS expertise.

- Formalize an official organization chart that encompasses AWS operations.
- Establish a process for annual performance reviews that incorporate AWS knowledge.

CC2 series: Communication and Information

The Communication and Information (CC2 series) criteria require the entity to obtain, generate, use, and communicate relevant, quality information internally and externally to enable effective control operations.

This includes internal communication of objectives, responsibilities, incident response processes, and system operations, as well as communication with external parties such as customers, vendors, and regulators. In the AWS context, customers are responsible for making sure that their cloud workloads (whether server- based, serverless, or hybrid) generate accurate logs, metrics, and event data, and that relevant system and security information is captured, distributed, and communicated appropriately within their organization and to third parties as needed.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
CC2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	• Captures internal and external sources of data • Processes relevant data into information • Maintains quality throughput processing	• To capture system and user activities, enable CloudTrail and AWS service level logging • To capture and log AWS configuration states, enable the AWS Config Recorder • To obtain actionable information, establish relevant metrics in CloudWatch for alerting and enable AWS Config Conformance Packs

		• To maintain the source data quality, enable CloudTrail log file validation and log file encryption, in addition to Amazon Simple Storage Service (Amazon S3) bucket encryption
CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	• Communicates internal control information • Communicates system changes	• To properly notify personnel of actionable CloudWatch alarms or system changes, create specific Amazon Simple Notification Service (Amazon SNS) topics for information distribution using different communication channels
CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.	• Not applicable	• No AWS specific implementation

Non-AWS implemented controls (organizational, process, and people):

- Monitor system logs and events from AWS services and integrate into centralized monitoring tools (for example, SIEM).
- Establish information requirements for control operations, incident response, and risk management over AWS operations.
- Define and communicate job responsibilities and control objectives in AWS to relevant individuals in a timely manner.

In addition to the controls implemented in or for AWS, it is important for the customer organization to define responsibility for communication strategies, incident escalation paths,

and customer notifications to make sure that system objectives and changes are effectively communicated internally and externally.

CC3 series: Risk Assessment

The Risk Assessment (CC3 series) criteria require the entity to establish and implement processes for identifying, analyzing, and responding to risks that might affect the achievement of system objectives, including security, availability, processing integrity, confidentiality, and privacy.

This includes specifying system objectives, identifying and analyzing internal and external risks (including fraud risks), and assessing changes that could significantly affect internal control.

In AWS-hosted environments, customers are responsible for conducting regular risk assessments covering their cloud architecture, configurations, data flows, and dependencies, while considering threats specific to the cloud shared responsibility model, cloud-focused risks, third-party integrations, and service dependencies.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
CC3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	• Aligns with externally established frameworks	• To use pre-built control evaluations in compliance frameworks, enable AWS Config conformance packs and AWS Security Hub
CC3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	• Identifies and assesses criticality of information assets and identifies threats and vulnerabilities	• To identify system vulnerabilities, enable Amazon Inspector to scan for vulnerabilities in Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Registry (Amazon ECR), and AWS Lambda

		• For threat detection, enable Amazon GuardDuty to monitor AWS accounts and workloads for malicious activities
CC3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	• Considers the risks related to the use of IT and access to information	• To evaluate least-privilege access to information, enable AWS IAM Access Analyzer to track unused access and permissions in AWS accounts
CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.	• Assesses changes in systems and technology	• To accurately track changes, enable AWS CloudFormation drift detection for infrastructure as code (IaS), AWS Config rules for AWS configuration, and CloudTrail for API-initiated changes

Non-AWS Implemented controls (organizational, process, and people):

- Define system objectives for AWS workloads aligned with contracts, regulatory obligations, and organizational strategy
- Subscribe threat intelligent on all services used on AWS
- Evaluate risk impacts and risk opportunities specific to operations in AWS

In addition to the controls implemented in or for AWS, it is important for the customer organization to define ownership of the risk management framework, methodology, prioritization, and risk treatment.

CC4 series: Monitoring Activities

The Monitoring Activities (CC4 series) criteria require the entity to select, develop, and perform ongoing or separate evaluations to determine whether components of internal control are present and functioning and to evaluate and communicate deficiencies to the parties responsible for corrective action. This includes continuous monitoring of systems, configurations, security events, and control effectiveness, as well as the timely identification and remediation of control deficiencies.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
CC4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	• Mix of ongoing and separate evaluations. • Establishes baseline understanding	• To identify system vulnerabilities, enable Amazon Inspector to scan for vulnerabilities in Amazon EC2, Amazon ECR, and Lambda • To continuously evaluate AWS resource configuration against a baseline and enable AWS Config conformance packs
CC4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	• Communicates deficiencies. • Monitors corrective action	• To properly notify personnel of security findings, create specific Amazon SNS topics for information distribution using different communication channels

		• To centralize, monitor, and track security issues and resolutions, enable Security Hub to accept findings from both AWS and non-AWS security tools

Non-AWS implemented controls (organizational, process, and people):

- Establish security baselines for different AWS workloads.
- Define evaluation scope and frequency for AWS workloads and operations based on identified risks.
- Formalize ownership of AWS accounts and workloads for corrective actions.
- Document processes for penetration testing, red teaming, and independent assessments on AWS.

AWS does not perform governance reviews, audits, or human-in-the-loop validations on behalf of customers. Therefore, customers are fully responsible for establishing and operating their monitoring programs, controlling effectiveness reviews, and implementing remediation processes.

CC5 series: Control Activities

The Control Activities (CC5 series) criteria require the entity to select and develop control activities that contribute to the mitigation of risks to the achievement of system objectives, implement general IT controls (ITGC), and deploy controls through policies and procedures. These controls help ensure that risks identified during the risk assessment process are effectively mitigated through operational, technical, and procedural safeguards.

In AWS-hosted environments, customers are responsible for designing, implementing, and enforcing control activities over cloud configurations, deployments, data access, processing, change management, and security monitoring. AWS supports these activities by providing configurable security and operational services.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
CC5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	• Addresses segregation of duties	• To address strict segregation of duties, implement IAM and IAM Identity Center RBAC and resource access controls
CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.	• Establishes relevant technology infrastructure control activities • Establishes relevant security management process controls activities	• To help ensure the completeness, accuracy, and availability of technology processing, enable Security Hub to accept findings from both AWS and non-AWS security tools • To restrict technology access rights, enable IAM Access Analyzer to track unused access and permissions in AWS accounts
CC5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	• Performs in a timely manner • Takes corrective action	• To perform control activities in a timely manner, enable AWS Config Rules to automate evaluation of system controls

		• To help ensure corrective action is automatically completed, configure AWS Config rules to include remediation action

Non-AWS implemented controls (organizational, process, and people):

- Determine controls activities at various levels in AWS regarding the Shared Responsibility Matrix.
- Evaluate the dependency between AWS technical controls and business process controls.
- Establish policies and procedures that govern both automated and manual controls implemented in AWS.

While AWS provides tools, customers retain full responsibility for defining control activities, implementing them in their AWS accounts, and making sure that they are enforced consistently using policies, procedures, and governance processes.

CC6 series: Logical and Physical Access Controls

The Logical and Physical Access Controls (CC6 series) criteria require the entity to implement controls to restrict logical and physical access to systems, data, and facilities, making sure that only authorized individuals are granted appropriate access and that access is revoked when no longer required.

This also includes controls over remote access, transmission, movement, removal of information, and protections against unauthorized or malicious software.

In AWS environments, customers are responsible for managing logical access to their AWS accounts, services, data, and applications.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	• Identifies and manages the inventory of information assets • Restricts logical access • Considers network segmentation • Restricts access to information assets • Manages credentials for infrastructure and software • Uses encryption to protect data • Protects encryption keys	• To track AWS resources and EC2 instances, enable AWS Config configuration recorder and AWS Systems Manager Inventory • To restrict logical access to information assets based on specific requirements, configure RBAC using IAM and IAM Identity Center and access controls with SCPs), resource control policies (RCPs), and resource based policies such as S3 bucket policies • To isolate network environments, use multiple AWS accounts, multiple Amazon Virtual Private Clouds (Amazon VPCs), and restrict traffic using security groups and network access control lists (network ACLs) • To protect authentication data, store credentials in AWS Secrets Manager or Systems Manager Parameter Store

		• To protect data at rest, enable AWS KMS encryption on Amazon storage services, such as Amazon Elastic Block Store (Amazon EBS), Amazon S3, and so on • To protect encryption keys during generation, storage, use, and destruction, use AWS KMS customer managed keys
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	• Reviews appropriateness of access credentials	• To track usage and information on access credentials, enable IAM Access Analyzer and IAM credential reports
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving con-sideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	• Uses role-based access controls	• To segregate incompatible functions, implement IAM and IAM Identity Center RBAC and resource access controls

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	• Not applicable	• AWS is responsible for physical access to the facilities that are hosted on AWS services
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	• Not applicable	• AWS is responsible for the physical assets of the facilities that are hosted on AWS services
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	• Restricts access • Requires additional authentication or credentials • Implements boundary protection systems	• To restrict communication channels, use multiple AWS accounts, multiple Amazon VPCs, and restrict traffic using security groups and network ACLs • To incorporate additional authentication information, enable multifactor authentication (MFA) in IAM and IAM Identity Center

		• To detect external access attempts, enable GuardDuty to alert on activities that show abnormal behavior
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	• Uses encryption technologies or secure communication channels to protect data	• To protect transmission of data, use SSL certificates stored in AWS Certificate Manager (ACM) and AWS PrivateLink, such as VPC endpoints, to securely connect with AWS services
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	• Restricts application and software installation • Detects unauthorized changes to software and configuration parameters • Uses antivirus and anti-malware software	• To restrict the ability to install application and software, enable SCPs and configure AWS Service Catalog • To detect changes to software and configuration, enable CloudFormation drift detection for IaS, AWS Config rules for AWS configuration, and CloudTrail for API-initiated changes • To detect and remediate viruses, enable GuardDuty Malware Protection for EC2 and S3

Non-AWS implemented controls (organizational, process, and people):

- Establish a formal process for logical access provisioning, removal, and review for AWS infrastructure and applications.
- See the AWS third-party attestation for physical access controls around AWS hosted infrastructure.

Physical access controls for AWS infrastructure are managed by AWS and are evaluated as part of the AWS SOC 2 Type II report, which covers physical data center security (for example, badge access, video surveillance, and security guards). Customers can inherit these controls when using AWS infrastructure to demonstrate compliance with relevant criteria, such as CC6.4.

However, under the shared responsibility model, customers remain accountable for managing physical access to any components outside of AWS infrastructure—such as their own corporate offices, on-premises data centers, employee laptops, or other user devices that connect to AWS resources. These areas must be included in the customer's SOC 2 assessment if they impact the confidentiality, integrity, or availability of customer data or systems.

Additional implementation guidance on physical access responsibilities and how they map to SOC 2 criteria (for example, CC6.4 and CC6.5) is provided in the control mapping tables later in this document.

CC7 series: System Operations

The System Operations (CC7 series) criteria require the entity to design and operate activities to manage system operations, detect and monitor deviations from expected performance, and respond to and recover from security incidents and system failures in a controlled manner.

This includes configuration monitoring, anomaly detection, event analysis, incident response, and recovery from disruptions.

In AWS-hosted environments, customers can use a suite of AWS services to enable automated, real-time monitoring, event-driven detection, and response automation.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	• Monitors infrastructure and software • Implements change-detection mechanisms • Detects unknown or unauthorized components • Conducts vulnerability scans	• To alert personnel to unauthorized modifications of critical system files, configuration files, or content files, enable CloudFormation drift detection for IaS, AWS Config rules for AWS configuration, and CloudTrail for API-initiated changes • To identify potential vulnerabilities, enable Amazon Inspector to scan for vulnerabilities in Amazon EC2, Amazon ECR, and Lambda
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	• Implements filters to analyze anomalies	• To filter, summarize, and analyze anomalies using machine learning techniques, enable GuardDuty

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	• Communicates and reviews detected security events	• To properly notify personnel of security events, create specific Amazon SNS topics for information distribution using different communication channels
CC7.4: The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	• Contains security incidents • Mitigates ongoing security incidents • Develops and implements communication protocols for security incidents	• To contain, mitigate, and communicate active security incidents, configure Incident Manager, a capability of AWS Systems Manager Incident Manager, with customized responses plans and runbooks
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.	• Improves response and recovery procedures	• To improve the incident response process, use Incident Manager to collect information to diagnose and learn from incidents

Non-AWS implemented controls (organizational, process, and people):

- Define baseline configurations and golden Amazon Machine Images (AMIs) in AWS.
- Establish formal processes and runbooks for incident response in AWS.
- Conduct periodic automated and manual incident response testing for AWS services.

While AWS provides the infrastructure and tools for operational excellence and incident handling, the customer is fully responsible for defining, implementing, and operating the incident response plan, system monitoring strategy, and recovery procedures tailored to their business and compliance requirements.

CC8 series: Change Management

The Change Management (CC8 series) criteria require the entity to implement a formal change management process to make sure that changes to infrastructure, data, software, and procedures are authorized, tested, documented, and properly implemented.

This helps reduce the risk of unauthorized, ineffective, or uncontrolled changes impacting system security, availability, processing integrity, confidentiality, and privacy.

In AWS-hosted environments, customers are responsible for managing changes to their cloud resources, configurations, and services. AWS provides services to help automate, manage, and control changes securely and at scale.

SOC 2 TSC identifier	Points of focus Covered	Customer Responsibilities (AWS specific implementation)
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	• Manages changes throughout the system lifecycle • Tracks system changes • Tests system changes • Approves system changes • Deploys system changes • Creates baseline configuration of IT technology	• To automate change process, use Change Manager, a capability of AWS Systems Manager • To use software development lifecycle controls for infrastructure changes, implement CloudFormation for IaC • To standardize code change requirements for testing, approval, and deployment, implement AWS CodePipeline and AWS Developer Tools • To maintain baseline configuration, use Amazon EC2 Image Builder to update golden AMIs

Non-AWS implemented controls (organizational, process, and people):

- Define baseline configurations and golden AMIs in AWS.
- Establish processes for emergency changes in AWS.

While AWS supports secure change management through these services, the entity is responsible for defining change management policies, workflows, risk assessments, approvals, testing, rollback procedures, and verifying change governance adherence across their environment.

CC9 series: Risk Mitigation

The Risk Mitigation (CC9 series) criteria require the entity to identify, select, and develop risk mitigation activities for risks arising from business disruptions and use of vendors and business partners.

This helps ensure that the entity is prepared to handle incidents that could affect system objectives and that third-party risks are appropriately managed.

In AWS-hosted environments, the entity remains responsible for managing their risk posture, including business continuity planning (BCP), disaster recovery (DR), third-party risk management, and vendor oversight. AWS provides tools and services that can support technical resilience, business continuity, and visibility into cloud vendor dependencies.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	• Considers mitigation of risks of business disruption	• To limit the impact of security event disruptions, implement multi-Availability Zone (AZ) and multi-AWS Region architectures and use AWS Backup and AWS Elastic Disaster Recovery backups to recover from potential disruptions

CC9.2: The entity assesses and manages risks associated with vendors and business partners.	• Assesses vendor and partner business risks	• To demonstrate AWS commitment, obtain third-party attestation reports from AWS Artifact

Non-AWS implemented controls (organizational, process, and people):

- Conduct business impact analysis (BIA) on AWS workloads to verify that the AWS architecture supports the workloads.
- Update the alternate security contact across AWS accounts for timely security notifications.

Other processes, including vendor risk management programs, BCP and DR governance, tabletop exercises, and formal risk acceptance remain fully the customer's responsibility.

While the Common Criteria (CC1–CC9) of SOC 2 apply universally to all trust categories, Category-Specific Criteria expand the control scope when a service organization includes additional commitments related to system Availability, Processing Integrity, Confidentiality, or Privacy.

Each of these categories introduces its own control objectives and points of focus that require focused implementation and validation. In AWS environments, meeting these extended requirements involves both technical configurations and supporting organizational governance. This includes:

- Architecting workloads for resilience, continuity, and integrity
- Applying controls for data protection, consent management, and privacy transparency
- Using AWS services for enforcement, monitoring, and evidence generation

These mappings provide prescriptive guidance for how customers can:

- Interpret each SOC 2 category-specific criterion in the context of AWS
- Identify and configure AWS services that directly support compliance objectives
- Design non-technical controls such as policies, training, and documented procedures
- Align their environment to AICPA-defined points of focus used in SOC 2 audits

This structured approach enables organizations to translate SOC 2 principles into clear, operational actions in the cloud—supporting both audit readiness and real-world risk mitigation.

Category specific criteria and AWS guidance

In SOC 2 (TSC 2017), the Category-Specific Criteria (Availability, Processing Integrity, Confidentiality, and Privacy) extend the Common Criteria (CC1–CC9) by focusing on controls that address the specific objectives committed by the service organization to its customers or regulators.

These categories are scoped into a SOC 2 examination when the organization asserts commitments around system uptime, data processing accuracy, information confidentiality, or personal data privacy.

While AWS provides a highly resilient, secure, and globally available cloud environment, customers are responsible for configuring AWS services appropriately, implementing controls within their AWS environment, and managing supporting organizational policies, processes, and governance frameworks to meet these criteria.

This whitepaper provides prescriptive guidance for customers to:

- Use AWS services (for example, CloudWatch, AWS Config, Amazon Inspector, AWS KMS, Amazon Macie, AWS Backup, and Elastic Disaster Recovery) to implement technical controls supporting SOC 2 category-specific objectives
- Understand the AWS shared responsibility model boundaries for each category
- Design and operate necessary organizational controls and governance to supplement AWS technical capabilities

This guidance enables customers to align their AWS-based workloads and services with the SOC 2 TSC 2017 category-specific requirements effectively.

PI series: Processing Integrity

The Processing Integrity (PI series) criteria in SOC 2 TSC 2017 focus on making sure that system processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and objectives.

These criteria require controls over data inputs, processing, outputs, and storage to help ensure that data is handled appropriately throughout its lifecycle and that errors or deviations are identified and corrected promptly.

In AWS-hosted environments, while AWS provides services that support data processing (for example, compute, storage, database services), the customer retains full responsibility for making sure of the correctness, integrity, and accuracy of data and processes within their applications and workflows.

Customers should implement data validation checks, processing logs, monitoring mechanisms, and reconciliation controls, using AWS services combined with strong governance, documented processing procedures, and error-handling protocols.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	• Not applicable	• No AWS specific implementation
PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	• Evaluates processing inputs • Creates and maintains records of system inputs	• To evaluate REST API input, enable Amazon API Gateway request validation • To retain system and application logs, enable CloudTrail and export native system and application logs to CloudWatch log groups

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	• Records systems processing activities	• To retain system and application logs, enable CloudTrail and export native system and application logs to CloudWatch log groups
PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	• Protects output • Distributes output only to intended parties • Creates and maintains records of system output	• To protect process output, enable AWS KMS encryption on Amazon storage services, such Amazon EBS, Amazon S3, and so on • To limit output distribution, implement IAM and IAM Identity Center RBAC and resource access controls • To retain system and application logs, enable CloudTrail and export native system and application logs to CloudWatch log groups
PI1.5: The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	• Protects stored items • Archives and protects system records • Creates and maintains records of system storage activities	• To protect stored items, enable AWS KMS encryption on Amazon storage services, such Amazon EBS, Amazon S3, and so on

		• To protect system records, enable AWS KMS encryption on CloudTrail trails and CloudWatch log groups • To retain system and application logs, enable CloudTrail and export native system and application logs to CloudWatch log groups

Non-AWS implemented controls (organizational, process, and people):

- Define key characteristics of processing inputs for AWS workloads
- Establish a set of processing specifications for AWS workloads

A series: Availability

The *Availability* criteria in SOC 2 TSC 2017 address the requirement that systems and data be available for operation and use as committed or agreed. These criteria help ensure that the entity maintains sufficient capacity, resilience, and disaster recovery to meet service level agreements (SLAs), customer expectations, and operational requirements.

In AWS-hosted environments, customers can use a range of resilient infrastructure and automation services to support availability goals. However, AWS is only responsible for the availability of its global infrastructure and managed services. Customers are responsible for:

- Architecting fault-tolerant workloads
- Implementing disaster recovery plans
- Monitoring system health
- Performing backup and restoration testing

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	• Measures current usages • Makes changes based on forecasts	• To manage capacity constraints, enable CloudWatch metrics to monitor resource utilization • To address capacity constraints, configure Auto Scaling for Amazon EC2, Amazon Elastic Container Service (Amazon ECS), and Amazon Relational Database Service (Amazon RDS)
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	• Performs data backup • Implements alternate processing infrastructure	• To protect data from unexpected loss, configure centralized backup policies in AWS Backups for a variety of AWS services, such as Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3, and so on • To limit the impact of location disruptions, implement multi-AZ and multi-Region architectures in addition to cross-Region replication

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.	• Implements business continuity plan testing	• To minimize downtime and data loss, set up Elastic Disaster Recovery for replication and non-disruptive testing

Non-AWS implemented controls (organizational, process, and people):

- Define relevant recovery time objectives (RTOs) and recovery point objectives (RPOs) for data and systems based on the BIA of the AWS workloads.
- Develop system and data backup plans and resilient architecture on AWS using the defined RTOs and RPOs.

C series: Confidentiality

The *Confidentiality* criteria in SOC 2 TSC 2017 focus on protecting information designated as confidential from unauthorized access, use, or disclosure—from creation or receipt through storage and final disposal. This includes internal business data, intellectual property, contractual data, and customer-sensitive information.

In AWS environments, while AWS provides secure infrastructure, customers are responsible for managing access to confidential data stored or processed in AWS services. This includes identifying what data is confidential, implementing encryption, enforcing access controls, and defining secure data handling and disposal procedures.

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	• Identifies confidential information • Protects confidential information from destruction	• To identify confidential information, enable Macie for sensitive data discovery and protection • To designate confidential information, enforce resource labeling with an Organizations tag policy

		• To avoid accidental resource and data deletion, enable termination protection on EC2 instances and MFA delete on S3 buckets
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	• Identifies confidential information for destruction • Destroys confidential information	• To designate confidential information, enforce resource labeling with an Organizations tag policy • To remove expired data automatically, apply Amazon S3 Lifecycle configuration and object expiration rules to delete old data beyond data retention needs

Non-AWS implemented controls (organizational, process, and people):

- Develop a standardized tagging policy for data and resources in AWS
- Define retention requirements for data stored on AWS

P series: Privacy

The *Privacy* criteria in SOC 2 TSC 2017 focus specifically on personal data—how it is collected, used, retained, disclosed, and disposed of in accordance with the entity's privacy commitments and legal requirements. This includes providing proper notice, consent, data minimization, user access, breach notification, and enforcement of privacy policies.

In AWS environments, while AWS secures the cloud infrastructure, customers are responsible for configuring how personal data is handled within their applications and services, and for enforcing privacy governance aligned with laws like GDPR, HIPAA, or CCPA.

Relevant AWS services for privacy

- **IAM, AWS KMS, and Macie** – for identity-based access, encryption, and data classification
- **CloudTrail and AWS Config** – for audit logging and policy tracking
- **Macie** – for detecting personally identifiable information (PII) in Amazon S3
- **AWS Shield, AWS WAF, and GuardDuty** – for protecting personal data from external threats
- **Lambda and** AWS Step Functions – for automated processing and access workflows
- AWS Control Tower **and SCPs** – for consistent data handling control

P1 series: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	• Communicates to data subjects • Provides notice to data subjects • Covers entities and activities in notice	• Host and serve the privacy notice using Amazon S3 and CloudFront with version control for accessibility and low latency • Use Amazon Cognito to link the notice acceptance to authenticated user accounts (for example, on sign-in or registration)

		• Implement just-in-time disclosures using API Gateway and Lambda when specific personal data processing is initiated (for example, when a file is uploaded or a support ticket is created) • Send notification emails using Amazon Simple Email Service (Amazon SES) or push notifications using Amazon SNS to communicate updates to privacy practices • Use CloudTrail and AWS Config to track backend changes related to systems processing personal data (for example, enabling new logging mechanisms, or adding destinations for personal data) • Use Amazon S3 object versioning, and Amazon Athena and AWS Glue to audit and demonstrate historical privacy notice changes

Non-AWS implemented controls (organizational, process, and people)

- Draft a clear, comprehensive privacy notice that outlines what personal data is collected, how it's used, and with whom it's shared.
- Implement a notice update procedure that includes legal and compliance review before any privacy-related change is deployed.
- Define roles responsible for reviewing, updating, and approving privacy notices (for example, data privacy officer (DPO), legal counsel, or marketing).
- Make sure that privacy notice updates are translated, localized, and accessible to affected users (for example, based on region or language).
- Maintain a log of notice updates, along with date and time stamps and internal references to affected systems or processes.
- Train product teams to notify privacy or compliance teams when introducing new data uses that might affect the privacy notice.

P2 series: Privacy Criteria Related to Choice and Consent

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the	• Communicates to data subjects • Communicates consequences of denying or withdrawing consent • Obtains implicit or explicit consent • Documents and obtains consent for new purposes and uses • Obtains explicit consent for sensitive information	• Use CloudFront and Amazon S3 to serve privacy preference UIs and policy documents across Regions with low latency • Use AWS WAF to enforce Regional access controls or restrict UI to appropriate users

intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	• Obtains consent for data transfers	• Use Amazon Cognito to authenticate users and collect consent as part of sign-up and sign-in flows • Store consent flags and history in Amazon DynamoDB, Amazon Aurora, or Amazon RDS, with timestamps, purpose, and method of consent • Use CloudTrail to audit consent-related API actions • Implement explicit opt-in (for example, for marketing) and log opt-outs (for example, cookie rejection) using Lambda and API Gateway • Tag datasets with metadata representing the consent basis using AWS resource tags • Apply IAM or application-level policies that check user consent before data access is granted • Notify individuals of consequences of consent or denial

		• Use Amazon SES or in-app messaging through Amazon SNS to communicate the implications of consent or refusal (for example, account limitations) • Use Macie to classify PII and map to declared purposes • Use CloudWatch Events to trigger remediation workflows

Non-AWS implemented controls (organizational, process, and people)

- Maintain a formal consent management policy, defining how, when, and for what purposes consent must be obtained.
- Make sure that privacy notices and interfaces explain individual choices and consequences clearly and understandably.
- Define and document legal bases for both explicit and implicit consent, aligned with applicable laws (for example, GDPR, and CCPA).
- Maintain an audit trail for all consent-related interactions, including logs of updates, revocations, and user decisions.
- Train personnel involved in data collection (for example, developers, marketers, and support staff) on proper consent capture and use.
- Implement internal reviews to help ensure that new features or integrations respect previously collected consent terms.
- Establish processes and procedures to revalidate consent periodically, especially for sensitive or long-term data retention.

P3 series: Privacy Criteria Related to Collection

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P3.1: Personal information is collected consistent with the entity's objectives related to privacy.	• Limits the collection of personal information • Collects information by fair and lawful means • Collects information from reliable sources • Informs data subjects when additional information is required	• Store and serve declared purposes in your privacy notice using Amazon S3 and CloudFront • Include purpose metadata (for example, "analytics" or "account management") in data collection logic • Tag resources and datasets using AWS resource tags with purpose indicators • Use IAM condition keys to restrict access or write actions based on these tags • Use CloudTrail and AWS Config to track Lambda, API Gateway, or Amazon S3 write operations and verify alignment with declared collection intents • Use Macie to detect PII in unexpected locations (for example, logs or raw ingestion files)

		• Use Security Hub, AWS Config Rules, and CloudWatch alarms to alert if resources are collecting or storing personal data outside approved trust zones or patterns
P3.2: For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy	• Obtains explicit consent for sensitive information • Documents explicit consent to retain information	• Use Amazon Cognito with pre-signup Lambda triggers to enforce consent capture before user registration • Integrate consent modals in frontend apps backed by API Gateway and Lambda for processing consent acknowledgments • Host privacy notices and just-in-time disclosures using Amazon S3 and CloudFront, possibly integrated into application UIs • Use Amazon SNS or Amazon SES to send consent explanation emails before personal data is collected

		• Use DynamoDB, Aurora, or Amazon RDS to persist consent metadata (user ID, timestamp, IP, and purpose, consequence notice version) • Use CloudTrail to log system-level events indicating when and by whom consent was recorded • Use IAM policies or custom logic in Lambda to block workflows that require consent unless the user's consent status is valid and current • Optionally, enforce consent preconditions using Step Functions in onboarding workflows

Non-AWS implemented controls (organizational, process, and people)

- Define and document a data collection policy outlining allowed purposes, data types, and scope of collection.
- Make sure that all applications and forms limit data fields to only what is necessary for stated objectives
- Conduct privacy impact assessments (PIAs) for new collection mechanisms to validate alignment with privacy goals.
- Review collected data periodically to confirm continued relevance to business and privacy objectives.

- Train developers and product teams on data minimization principles and purpose alignment.
- Engage legal and privacy officers to review whether system behavior aligns with declared objectives before launch or integration.
- Define a consent management policy with clear procedures for when and how explicit consent is required.
- Maintain a catalog of processing activities that require explicit consent (for example, marketing, biometric data, or sensitive profiling).
- Make sure that just-in-time consent interfaces are part of all user data collection touchpoints (web, mobile, or API).
- Clearly disclose the consequences of not giving consent, such as reduced service availability or limited access.
- Establish periodic reviews to help ensure legal validity of consent mechanisms, especially for sensitive or regulated data types.
- Train developers and legal teams to collaborate on consent language, timing, and user interface placement.
- Retain consent evidence and link to specific privacy policy version in force at the time of acceptance.

P4 series: Privacy Criteria Related to Use, Retention, and Disposal

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	• Uses personal information for intended uses	• Define approved purposes and tag data accordingly using AWS resource tags (for example, Purpose=Marketing)

		• Restrict access by purpose using IAM policies, S3 bucket policies, and AWS Lake Formation permissions • Use Macie to scan for PII and confirm that personal data is not being used in non-authorized services or locations • Monitor logs with CloudTrail and CloudWatch to detect unauthorized usage or API calls against PII-linked resources
P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.	• Retains personal information • Protects personal information	• Set Amazon S3 Lifecycle configuration to delete or transition objects based on retention timelines • Use DynamoDB Time to Live (TTL) or database triggers in Aurora or Amazon RDS to purge expired records • Maintain tagging for retention duration (for example, Retention = 90 days) and use AWS Config to validate conformance

		• Automate retention workflows using Step Functions, Amazon EventBridge, and Lambda
P4.3: The entity securely disposes of personal information to meet the entity's objectives related to privacy.	• Captures, identifies and flags requests for deletion • Disposes of, destroys and redacts personal information • Destroys personal information	• Enable Amazon S3 Object Lock with retention expiration followed by deletion • Use AWS KMS key deletion schedules to help ensure cryptographic erasure if encryption is used • Configure Amazon RDS, Amazon EBS, and Amazon Elastic File System (Amazon EFS)volumes with secure deletion protocols before deprovisioning • Track disposal actions using CloudTrail, and alert on failure events using CloudWatch alarms • For manual deletion workflows, build auditable pipelines using Step Functions and Lambda to confirm successful erasure of personal data

Non-AWS implemented controls (organizational, process, and people)

To help ensure personal information is used, retained, and disposed of in line with privacy objectives, the organization should consider implementing the following governance and process-level controls:

- **Data governance policies:** Establish formal policies for data usage, retention, and disposal that clearly define approved purposes, timeframes, and disposal methods aligned with regulatory and contractual obligations.
- **Data classification and mapping:** Maintain a current data inventory and classification scheme that identifies personal data across systems, associates it with intended purposes, and aligns it with defined retention schedules.
- **Retention schedules and procedures:** Define retention periods by data category and business function. Make sure that these are documented, accessible to stakeholders, and regularly reviewed for compliance with evolving legal or business requirements.
- **Disposal processes and standard operating procedures (SOPs):** Implement secure disposal procedures for personal data, whether manual or automated, including deletion, anonymization, or destruction. Make sure that procedures follow standards like NIST SP 800-88 or local equivalents.
- **Training and awareness:** Train staff (engineering, support, legal, and so on) on appropriate data handling practices—including restrictions on data reuse, retention obligations, and secure deletion practices.
- **Periodic reviews and audits:** Conduct regular reviews to detect data that is outdated, excessive, or improperly retained. Validate that data deletion workflows operate as intended and audit logs are intact.
- **Incident response alignment:** Make sure that data handling processes are integrated with breach response and legal hold procedures to help prevent unintended deletion or misuse during sensitive periods.

P5 series: Privacy Criteria Related to Access

Control objective (SOC 2 TSC 2017)	Points of focus covered	Customer responsibilities (AWS specific implementation)

P5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	• Authenticates data subjects' identity • Permits data subjects access to their personal information • Provides understandable personal information within reasonable information • Informs data subjects if access is denied	• Maintain indexed personal information in queryable stores such as Amazon RDS, Aurora, or DynamoDB with identity-linked keys • Create DSAR request forms or portals hosted on Amazon S3 with backend APIs in API Gateway and Lambda • Implement secure identity verification workflows using Amazon Cognito. • Generate reports using Athena, AWS Glue, or Lambda that compile data into downloadable formats (CSV, PDF) and deliver using Amazon SES or presigned Amazon S3 URLs • Track access events and responses using CloudTrail and log audit entries in CloudWatch Logs
P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such	• Communicates denial of access requests	• Build secure request workflows using API Gateway and Lambda to allow users to submit correction requests

information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	• Permits data subjects to update or correct personal information • Communicates denial of correction requests	• Store updated data in DynamoDB, Aurora, or Amazon RDS, with CloudTrail tracking who made changes and when • Propagate changes using Amazon SNS or EventBridge to downstream systems and third-party APIs • Maintain logs of denied requests and justifications using DynamoDB or Amazon S3, and provide user notifications through Amazon SES or in-app messages • Use IAM policies to restrict edit access to authorized roles and systems only

Non-AWS implemented controls (organizational, process, and people)

To help ensure that data subjects can access and correct their personal information in accordance with privacy objectives, the organization should implement the following operational, legal, and governance controls:

- **Data subject rights and Data subject access requests (DSR and DSAR) procedures:** Establish and document SOPs to handle data subject access and correction requests, including identification verification, request validation, fulfillment timelines, and escalation paths.

- **Identity verification controls:** Implement robust verification methods to confirm the identity of requesters before providing or modifying personal data, in alignment with regional privacy laws (for example, GDPR, CCPA).
- **Data inventory and mapping:** Maintain a detailed and regularly updated inventory of systems and data flows to enable quick and accurate data retrieval or updates when responding to access or correction requests.
- **Response templates and legal review:** Prepare standardized communication templates for granting, denying, or requesting clarification on access or correction requests. Make sure that legal or privacy teams review complex or denied requests for compliance.
- **Training and awareness:** Train customer support, legal, engineering, and compliance teams on how to identify, triage, and fulfill data subject rights requests securely and in a timely manner.
- **Denial justification and appeals:** Create a policy for handling denied requests, including proper documentation of the reason for denial and the process for appeals or complaints.
- **Change propagation:** If personal information is corrected, make sure that downstream systems and third-party processors are notified as committed or required by contract or regulation.
- **Logging and monitoring:** Maintain secure logs of all access and correction requests and outcomes to support audit readiness and demonstrate accountability.

P6 series: Privacy Criteria Related to Disclosure and Notification

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	• Communicates privacy policies to third parties • Discloses personal information only when appropriate	• Capture disclosure consent through Amazon Cognito or frontend apps powered by API Gateway and Lambda

	• Discloses personal information only to appropriate third parties • Discloses information to third parties for new purposes	• Record consent status in DynamoDB or Aurora, linked to the third-party service ID • Enforce data sharing logic in backend code to check for valid consent before transferring to external APIs, Amazon S3 cross-account, or PrivateLink endpoints • Use CloudTrail and CloudWatch Logs to monitor disclosure workflows
P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	• Creates and retains records of authorized disclosures	• Log disclosure events in Amazon DynamoDB or Amazon S3 with event metadata (timestamp, subject ID, recipient, and data shared) • Use EventBridge and Step Functions to trigger audit record creation upon each authorized sharing • Send audit logs to CloudWatch Logs, Amazon Data Firehose, or Amazon OpenSearch for visualization and tracking

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	• Creates and retains records of detected or reported unauthorized disclosures	• Detect breaches using GuardDuty, Security Hub, and Macie (for example, PII exposure in Amazon S3) • Route alerts to Amazon SNS or Amazon Security Lake and trigger incident logging with Lambda or Step Functions • Store incident evidence and breach metadata securely in Amazon S3 with AWS KMS encryption, using Object Lock to help ensure immutability • Use AWS Audit Manager or third-party investor relations (IR) services to centralize breach investigation records
P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	• Discloses personal information only to appropriate third parties • Remediates misuse of personal information by a third party	• Store signed contracts and vendor agreements in Amazon S3 with restricted access using bucket policies • Track vendor onboarding and offboarding and assessment status in DynamoDB or Systems Manager Inventory

		• Use AWS Artifact to request and track third-party privacy certifications (for example, ISO 27701, SOC 2 reports) • Maintain an internal vendor privacy risk register in Amazon RDS or integrate with governance, risk, and compliance (GRC) services (for example, ServiceNow)
P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.	• Remediates misuse of personal information by a third party • Reports actual or suspected unauthorized disclosures	• Include breach notification clauses in third-party contracts and track compliance in your contract database • Set up Amazon SNS or custom Lambda endpoints to receive breach alerts from vendors or integrated systems • Integrate with third-party services using EventBridge or API Gateway for automated intake of vendor incident notifications

		• Route alerts to Security Hub or ChatOps channels (for example, Amazon Chime or Slack) for immediate response
P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	• Remediates misuse of personal information by a third party • Provides notice of breaches and incidents	• Use Security Hub and GuardDuty to detect suspicious activity that might indicate data misuse or a breach • Aggregate findings into centralized response workflows using Amazon Detective, EventBridge, and Lambda to triage and route incidents • Store detailed forensic logs and analysis in Amazon S3 (with versioning and AWS KMS encryption) and CloudTrail Lake for long-term querying • Maintain automated alerts and escalations using Amazon SNS and integrate with incident ticketing systems through Lambda or Step Functions

		• Use Macie to detect if exposed or exfiltrated data contains PII or personal health information (PHI) and tag those objects for breach scope estimation • Create notification templates and dispatch alerts to affected users using Amazon SES or Amazon SMS through Amazon Pinpoint
P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	• Identifies types of personal information and handling process • Captures, identifies, and communicates requests for information	• • Identifies types of personal and sensitive information and how they're handled • Captures and responds to data subject requests for accounting of personal data and disclosures • Identify personal or sensitive data types using Macie to scan Amazon S3 buckets for PII, financial, and health data; classify and label assets based on sensitivity

		• Use AWS Glue Data Catalog to maintain metadata on datasets containing personal information, including their source, transformation logic, and destinations • Use CloudTrail Lake to query detailed logs about data access and disclosures by IAM users, roles, or services • Capture data subject requests through API Gateway and Lambda, storing request logs and timestamps in DynamoDB or Amazon RDS • Securely generate and share accounting reports using Amazon S3 (with S3 Object Lock and AWS KMS encryption) and notify users using Amazon SES • Use Amazon Cognito for secure authentication and identity linkage of data requests to specific data subjects

		• Implement centralized evidence gathering using Audit Manager and Athena for structured querying across logs, systems, and data repositories • Integrate ticketing or workflow systems using Step Functions and EventBridge for request status tracking and escalation

Non-AWS implemented controls (organizational, process, and people)

- Define and enforce a third-party data sharing policy, including requirements for explicit consent prior to disclosure.
- Maintain data processing agreements (DPAs) with all vendors accessing personal data, with clauses on use, breach notification, and termination handling.
- Establish a consent management process to capture, store, and retrieve data subject authorizations for disclosures.
- Maintain a disclosure log documenting all authorized and unauthorized data sharing events, including purpose, recipient, and lawful basis.
- Implement a privacy incident response plan, covering breach detection, classification, communication timelines, and regulator notification procedures.
- Define and document vendor breach reporting obligations and integrate vendor disclosures into internal response workflows.
- Conduct periodic vendor privacy risk assessments and follow up on non-compliance with corrective action.
- Respond to data subject access and accounting requests with verified identity procedures and structured reports of held and disclosed information.

- Provide training and awareness for legal, compliance, IT, and procurement teams on privacy obligations tied to disclosure, breach response, and vendor oversight.
- Maintain documentation and audit readiness for all privacy-related decisions, processes, and exceptions related to third-party data disclosures.

P7 series: Privacy Criteria Related to Quality

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	• Helps ensure accuracy and completeness of personal information • Helps ensure relevance of personal information	• Implement data validation and cleansing routines at data ingestion points using Lambda, AWS Glue, or AWS Glue DataBrew to enforce accuracy and format rules • Use Data Catalog to maintain metadata describing the source, context, and use case of personal data, supporting data relevance assessments

		• Apply Macie to classify and review data stored in Amazon S3, flagging sensitive data stored in non-relevant locations. Integrate Amazon RDS, DynamoDB, or Amazon with business logic that enforces required fields and input constraints for personal information • Use Amazon AppFlow or AWS Database Migration Service (AWS DMS)to synchronize personal data across systems to reduce inconsistencies and duplication. • Use CloudWatch and AWS Config to monitor configuration drift in systems managing personal data.

Non-AWS implemented controls (organizational, process, and people)

- Define policies and procedures to help ensure that personal data is collected only if relevant and with a clearly documented lawful purpose.
- Train staff on how to validate and update data during collection and throughout the data lifecycle.
- Implement periodic reviews and quality audits of personal data to detect and correct inaccuracies or outdated entries.

- Establish data stewardship roles responsible for maintaining the accuracy, completeness, and relevance of personal information.
- Enable data subject access and correction workflows to help ensure that individuals can update their own information when necessary.
- Limit collection forms and field to what is essential for the declared purpose, avoiding overcollection of personal data.

P8 series: Privacy Criteria Related to Monitoring and Enforcement

SOC 2 TSC identifier	Points of focus covered	Customer responsibilities (AWS specific implementation)
P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	• Communicates to data subjects • Addresses inquiries, complaints, and disputes • Documents and communicates dispute resolution and recourse • Documents and reports compliance review results • Documents and reports instances of noncompliance • Performs ongoing monitoring	• Use API Gateway and Lambda to build secure inquiry intake endpoints and integrate with case management tools • Store and track inquiry metadata using DynamoDB or Amazon RDS, including timestamps, resolution steps, and outcomes • Use Amazon SES or Pinpoint for secure notification to data subjects confirming receipt and resolution of complaints

		• Implement compliance dashboards using Amazon QuickSight, Athena, and Amazon S3 to visualize dispute resolution SLAs, patterns, and noncompliance trends • Use AWS Config and Security Hub to monitor compliance across AWS resources; generate alerts on configuration violations tied to privacy controls • Maintain immutable logs using CloudTrail and Amazon S3 Object Lock for audit support

Non-AWS implemented controls (organizational, process, and people)

- Establish a formal complaint-handling policy with defined intake channels (for example, web, phone, or email) and timelines for response and resolution.
- Train customer service, privacy, and legal teams to handle privacy inquiries and resolve complaints in accordance with applicable laws (for example, CCPA, or GDPR).
- Document every inquiry or complaint, track resolution steps, and provide written confirmation to the individual regarding the outcome.
- Perform periodic privacy compliance reviews and generate internal reports for leadership, outlining any issues, trends, and improvement actions.
- Track and report instances of noncompliance, applying corrective or disciplinary actions as appropriate.

- Maintain an ongoing monitoring plan that assesses the effectiveness of controls, remediates deficiencies, and helps ensure continuous improvement.
- Review and update processes regularly to incorporate regulatory changes and lessons learned from past complaints or incidents.

Note: For detailed implementation guidance and service selection, see the AWS Privacy Reference Architecture. It provides detailed patterns and AWS service recommendations to help build privacy-aware systems aligned with SOC 2 and other privacy frameworks.

Control design and documentation best practices

Meeting SOC 2 requirements in AWS is not just about implementing technical features—it's about designing and documenting well-governed controls that align with both AICPA's expectations and your operating model.

Efficient SOC 2 control

Each control should include the following key attributes to help ensure alignment with SOC 2 compliance expectations:

- **Purpose:** Aligned to a specific Trust Services Criterion
- **Owned:** Assigned to a responsible individual or team
- **Recurring:** Executed at a defined cadence
- **Evidence:** Producing auditable proof of operation
- **Mapped (where applicable):** Linked to AWS configurations, service settings, or organization policies that support the control's intent; not all controls will map directly to AWS features.

Documenting controls in AWS environments

AWS controls must be supplemented with organizational governance. Each documented control should include:

Attribute	Description
Control ID	A unique label tied to a Trust Service Criterion (for example, CC6.1-MFA)

Attribute	Description
Control description	What the control does and why it exists
Owner	Responsible person or team
Execution frequency	Daily, weekly, monthly, or quarterly
AWS services involved	For example, IAM, AWS KMS, AWS Config, CloudTrail
Expected evidence	For example, policy documents, logs, screenshots, and Config reports
Points of focus addressed	Which points of focus are satisfied by this control

Evidence collection and audit readiness

A successful SOC 2 audit relies on timely, accurate, and consistent evidence that demonstrates how controls are operating over time. For customer-managed controls that use AWS services in their design and operation, AWS provides several tools—such as CloudTrail, AWS Config, Security Hub, and Audit Manager—to help simplify evidence collection. However, customers must still design and maintain a structured process to manage this evidence in a traceable and auditable manner.

Note: Audit evidence sources are not limited to AWS services; they can also include internal policy documents, IT ticketing systems, access reviews, screenshots, third-party logs, and other manual procedures, depending on the nature of the control

AWS sources of evidence

The following table outlines common AWS services used as sources of evidence during audits, along with the type of information each provides.

AWS tool	Type of evidence
CloudTrail	API calls, authentication, config changes
AWS Config	Compliance evaluations, resource history
CloudWatch Logs	Application logs, alarms, usage data
IAM Reports	User and group access rights and changes

AWS tool	Type of evidence
Audit Manager	Control framework mapping, evidence folders
Security Hub	Findings, status of integrated services

Evidence collection strategies

To support audit readiness and demonstrate control effectiveness, the following evidence collection strategies can be implemented as part of your compliance program.

- Tag artifacts with control IDs (for example, CC5.3, or A1.2)
- Use Amazon S3 with versioning and access logs for long-term evidence retention
- Automate evidence exports with EventBridge and Lambda (for example, send logs to Amazon S3)
- Prepare walk-Polthroughs describing how each control works and where evidence is stored
- Run mock audits using Audit Manager or internal security teams to simulate questions and evidence requirements

Risk and governance: SOC 2 for the executive team

It is important for responsible executives to understand that the AICPA TSC that are assessed during the SOC 2 audit are equally focused on governance and specific technical or security measures such as firewalls, encryption, or log management and analysis. Your customers request SOC 2 reports from service providers such as your company to understand the risks presented to their own organization as they use the services provided by you, the service provider organization. The SOC 2 auditor's opinion will rest on how well your organization identifies and responds to the risks inherent in your operational environment to effectively and securely serve your customers.

This is a critical part of the SOC 2 assessment that many executive teams don't anticipate, and it can be critical to the outcome of your audit. The SOC 2 auditor will be trying to understand the relationship between management and any information security-related business processes or functions; therefore, the executive team should be able to demonstrate the free flow and

frequent consideration of information and metrics regarding existing risks and the measures adopted by the organization to mitigate or manage those risks.

Basic principles associated with the management of IT risk:

- Business leaders are expected to invest money for one of two reasons: either to exploit opportunities or to mitigate risks. In every business, financial resources (always limited) must be directed as efficiently as possible. This includes resources dedicated to the mitigation of IT risk.
- The existence of specific IT-related risks is why businesses create information security programs.
- Like all risks to the enterprise, IT-related risk must be managed and monitored. This is normally accomplished using a *risk register* that should roll up into the overall corporate risk management program, which is frequently managed by the CFO or Legal teams.
- The financial decisions associated with IT risk management should be balanced along with the remainder of the risks managed by the organization's executive team. For this to happen, executives should maintain awareness of current risks and potential impacts, so that appropriate resources can be assigned.

During the SOC 2 audit, the auditor will seek to answer the following questions:

- Does the Board of Directors (or Executive team) understand the level of risk for the organization based upon accurate information received from the individual business units or departments?
- Does the Board of Directors or executive team act to address the risk at the appropriate level and in a sufficient manner?

The SOC 2 audit is an assessment of the level of positive control the board of directors or the executive team exerts over the assessment and understanding of risks to the services being provided to their customers, the organizational systems and controls they put in place to make sure that those risks are addressed and managed appropriately, and the continued monitoring and timely management of evolving risks to the organization.

To explain all the specific functions of an effective IT risk management program is beyond the scope of this whitepaper. See the earlier section, *CC9 series: Risk Mitigation*, for more specific information regarding the Risk Management TSC. While the specific technical measures and solutions outlined in this document are essential for exerting control over your AWS-located

workloads, they aren't sufficient by themselves; service providers must demonstrate an appropriate level of attention to all identified sources of risk to the delivery of services to their customers.

Conclusion and recommendations

The SOC2 framework is not meant to be a point-in-time checkbox exercise, it is an ongoing trust framework. Organizations operating in AWS must go beyond security features and demonstrate governance, consistency, and maturity in how they implement and maintain controls.

This whitepaper serves as a guide for security architects, compliance leaders, DevOps teams, and assessors to:

- Understand SOC 2 requirements in AWS-specific terms
- Implement controls that address both technical and procedural gaps
- Automate evidence collection using AWS-native tooling
- Sustain compliance with minimal operational burden

Key takeaways

- Use the AWS Shared Responsibility Model to scope your control obligations clearly.
- Use AWS services (such as IAM, AWS Config, CloudTrail, AWS KMS, and AWS Backup) for control enforcement and evidence generation.
- Build and maintain a control register with traceable mappings to TSC and points of focus.
- Prepare for audits continuously by treating SOC 2 as a living part of your cloud operating model.

Contributors

Contributors to this document include:

- Abdul Javid, Sr. Assurance Consultant, AWS Security Assurance Services LLC
- Viktor Mu, Sr. Assurance Consultant, AWS Security Assurance Service LLC
- Wil Woodrum, Sr. Assurance Consultant, AWS Security Assurance Services LLC

Further reading

For additional information, see:

- System and Organization Controls: SOC Suite of Services
- Trust Services Criteria 2017
- AWS prescriptive guidance
- AWS SOC Reports FAQ
- AWS Whitepapers & guides
- NIST Risk Management Framework

Document revisions

Date	Description
July 21, 2025	Initial version