# ISO 27001:2022 on AWS

## Compliance Guide

*March 2026*

# 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 current Amazon Web Services (AWS) 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.

The information within this guide is presented as informational and is for reference only. Customers must manage their own International Organization for Standardization's Information Security Management System (ISO/IEC 27001:2022) compliance certification. While customers may use AWS services to store, process, or transmit their own sensitive information, AWS does not directly manage customer information security management systems (ISMS). This compliance guide is provided as a courtesy to facilitate customers' consideration and review of their ISMS scope and implementation of controls when using AWS services as they prepare for their ISO 27001:2022 certification. This document does not replace or change the contents of the AWS ISO 27001:2022 certification available in the AWS Artifact service.

This guide is provided by AWS Security Assurance Services, LLC (AWS SAS), a wholly owned subsidiary of AWS. AWS SAS, a Payment Card Industry-Qualified Security Assessor company (PCI-QSAC) and HITRUST External Assessor Firm, is a team of industry certified assessors, helping customers to achieve, maintain, and automate compliance in the cloud by connecting audit standards to AWS service-specific features and functionality.

# Contents

# Abstract

This guide helps organizations understand and implement ISO 27001:2022 requirements using AWS services. It provides practical guidance for establishing, implementing, maintaining, and continually improving an ISMS in AWS environments. While using AWS services assessed under our compliance programs does not automatically guarantee compliance, appropriate use of AWS services reduces the technical complexity of achieving certification.

# Introduction

This guide provides customers with information to help them plan for and document the compliance of your Amazon Web Services (AWS) workloads. This guide shows you how to implement an information security management system (ISMS) using AWS services. You will learn how to implement security controls aligned to ISO 27001:2022 Annex A, prepare audit-ready evidence using AWS native tooling, and explain your control implementation clearly to auditors. This guide helps you use AWS security features to meet ISO 27001:2022 requirements, whether you're pursuing initial certification or maintaining an existing ISMS. Organizations seeking assistance with implementing or maintaining their ISMS can contact the AWS Security Assurance Services team or their AWS account representative for support.

# Understand ISO 27001 and ISO 27002

The ISO 27000 family of standards provides internationally recognized frameworks for implementing and maintaining effective information security management systems. This section explores the two primary standards in this family: ISO 27001:2022, which establishes requirements for an information security management system (ISMS), and ISO 27002:2022, which provides implementation guidance for security controls.

## ISO 27001 framework

ISO 27001:2022 is the leading international standard for an ISMS. It provides a systematic approach to managing sensitive company information through a comprehensive framework of policies and procedures. The standard encompasses an organization's people, processes, and IT systems, and directs the implementation of a strong risk management process. ISO 27001:2022, the latest version, introduces significant changes that include the restructuring of control categories and the addition of new controls focusing on threat intelligence and cloud security.

The standard requires organizations to:
Systematically examine information security risks, accounting for threats, vulnerabilities, and impacts

Design and implement a coherent and comprehensive suite of security controls

Adopt an overarching management process to maintain controls so they continuously meet information security needs

## ISO 27002 implementation guidance

ISO/IEC 27002:2022 serves as a detailed guidance document that provides specific implementation advice for the controls listed in ISO 27001:2022 Annex A. The 2022 revision reorganized the controls into four main themes:

Organizational controls (37 controls)

People controls (8 controls)

Physical controls (14 controls)

Technological controls (34 controls)

This restructuring better reflects modern security practices and technological advancements, particularly in cloud computing and digital transformation.

# AWS Shared Responsibility Model

The first step in developing a strong ISMS and effectively managing organizational risks is to understand how AWS supports customer security posture by performing certain security controls on their behalf.

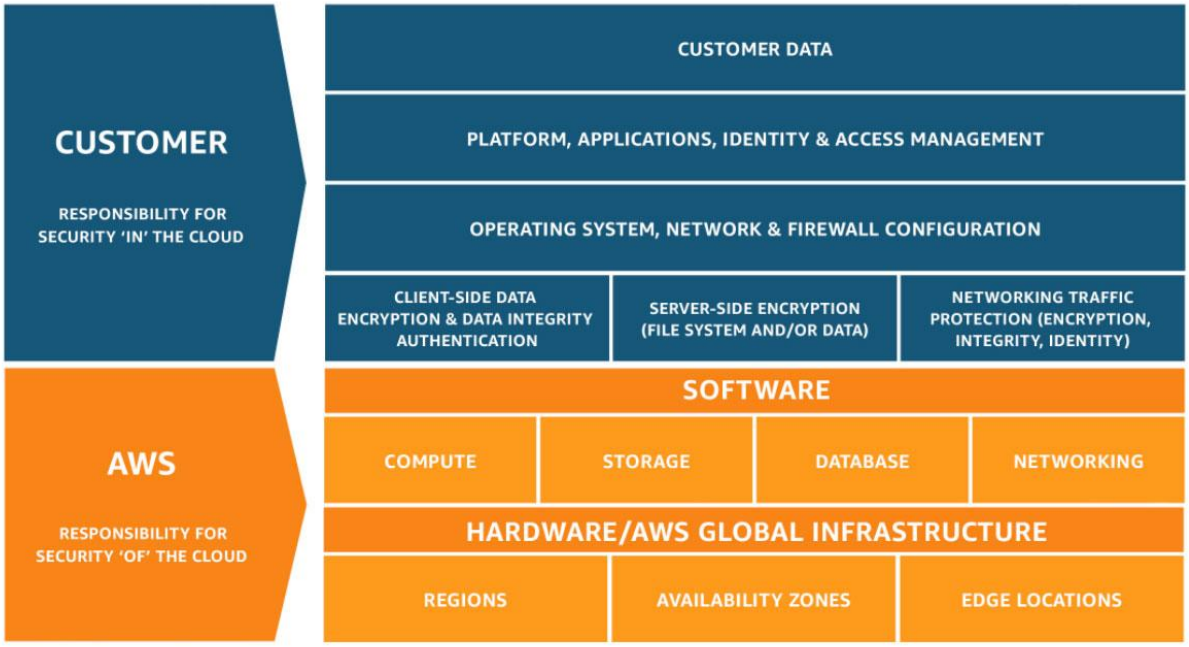


*Figure 1: Understanding security **of** the cloud compared to security **in** the cloud*

AWS and customers share security responsibilities under the shared responsibility model. Understanding this model is the first step to implementing ISO 27001/27002 controls in an AWS environment. AWS regularly achieves third-party validation for thousands of global compliance requirements and continually monitors them to help customers meet security and compliance standards across industries including finance, retail, healthcare, and government. AWS provides a secure cloud environment with independently verified certifications, such as ISO 27001:2022 and PCI DSS, to meet customers' security and compliance needs. These programs provide customers with a baseline level of security and provide them with reports and tools to map their specific compliance requirements to the

AWS environment. Customers remain responsible for their own data and applications *in* the cloud. By taking advantage of AWS ISMS, customers can share portions of the risk.

**AWS responsibilities (security *of* the cloud)**

AWS maintains responsibility for protecting the infrastructure that runs AWS cloud services. This infrastructure consists of the hardware, software, networking, and facilities that run AWS cloud services. Key aspects include:

- Physical security of data centers
- Hardware and network infrastructure
- Virtualization infrastructure
- Operational security of AWS services
- Global network security
- Service and feature security configurations

**Customer responsibilities (security *in* the cloud)**

Customers maintain responsibility for security considerations within the AWS Cloud. The level of responsibility depends on the AWS services used, the integration of those services into their IT environment, and applicable laws and regulations. These responsibilities typically include:

- Data classification and accountability
- Identity and access management
- Operating system, network, and firewall configuration
- Client-side data encryption and data integrity authentication
- Server-side encryption
- Network traffic protection
- Platform, applications, identity and access management

# Establish an ISMS on AWS

Establishing an ISMS on AWS involves adapting ISO 27001:2022 principles to cloud-centric environments. Traditional ISMS models often assume static infrastructure and on-premises control boundaries, but cloud services introduce dynamic scaling, abstracted infrastructure, and shared responsibility. To operate effectively on AWS, organizations should automate routine tasks, clearly assign ownership for each part of the system, and regularly review their security measures to maintain compliance.

Defining the ISMS scope in AWS

ISO 27001:2022 requires clearly defined ISMS boundaries. Traditionally, organizations with an on-premises infrastructure scope their ISMS using physical, process, network, and system boundaries. In AWS, the ISMS can be scoped using:

AWS accounts and AWS Regions:

- Use AWS Organizations and AWS Control Tower to group accounts by workload or compliance needs.
- Apply service control policies (SCPs) to enforce guardrails across organizational units (OUs). Guardrails are implemented with security controls designed to prevent operational risks.

**Network boundaries**: Use Amazon Virtual Private Cloud (Amazon VPC) to create logically isolated virtual networks, security groups for network micro-segmentation, AWS PrivateLink and VPC endpoints with AWS Identity and Access Management (IAM) permissions for secure and controlled private access between VPCs and AWS services, and AWS Direct Connect for private connections between AWS and customer's own physical infrastructure.

**Applications and data**: Track assets and resources using AWS Systems Manager inventories, AWS Config resource discovery, AWS Resource Explorer to search and discover AWS resources, and Amazon Macie for sensitive data discovery.

**Third-party integrations**: Secure data flows and APIs using PrivateLink, AWS Certificate Manager (ACM) for encryption in transit, and AWS IAM Identity Center for federated access management.

# Integrating with AWS security architecture

For organizations with AWS infrastructure, the ISMS should integrate with AWS services for identity, infrastructure, and operations management. This can be achieved by using services such as:

- IAM for role-based access and policies
- AWS Config for control monitoring and auditability
- Amazon GuardDuty and Amazon Inspector for threat detection and vulnerability management
- Systems Manager for configuration and patch orchestration.
- AWS CloudTrail for audit trails of actions by users, roles, or AWS services

This integration keeps the ISMS current with the AWS environment and helps organizations respond quickly to incidents and control failures.

# Using AWS services to comply with the ISO/IEC 27001:2022 clauses

ISO 27001:2022 clauses 4–10 define the core requirements of an ISMS. AWS provides services that help organizations implement these requirements and demonstrate conformity on a scale. This section outlines how AWS services align with each clause to support ISMS implementation across AWS and hybrid environments.

## Clause 4: Context of the organization

When implementing ISO 27001:2022 in AWS or hybrid environments, organizations must first take a holistic view of their business context, including how their AWS workloads interact with third-party services, and with on-premises systems if applicable. Organizations need to map out stakeholders who interact with or depend on their information assets, from cloud service providers like AWS to end users and regulators, understanding how these relationships impact security requirements across their entire technology landscape. Stakeholder requirements become more complex in hybrid deployments, requiring careful consideration of data sovereignty, access management, and regulatory compliance across multiple environments. Defining the ISMS scope becomes critical when using AWS, because organizations must clearly delineate which AWS services fall within scope and how they interact with other systems and services. Take special care to address the boundaries between AWS and other environments and how data flows between them, and where security responsibilities lie. When documenting the ISMS scope and any exclusions, organizations must consider how cloud services impact their security posture and clearly articulate how AWS controls integrate with their overall security framework, including any compensating controls needed for hybrid operations.

Organizations should establish an ISMS that can adapt to the dynamic nature of cloud environments while maintaining consistent controls across their AWS or hybrid footprints, ensuring that security policies remain effective regardless of where data resides or how it is processed. Customers should use services like AWS Config, CloudTrail, Amazon CloudWatch, and AWS Security Hub to establish consistent context awareness across their hybrid landscape. The foundation of a successful hybrid ISMS relies on understanding how cloud adoption transforms traditional security boundaries and requires adjusted governance approach.

## Clause 5: Leadership, policy, and governance

Clause 5 focuses on leadership commitment, establishing an information security policy, and assigning roles and responsibilities to maintain alignment between the ISMS and organizational objectives. AWS facilitates leadership's ability to govern and oversee information security through services like IAM, which enables clear definition and enforcement of roles, responsibilities, and access controls. AWS Organizations allows centralized management and policy enforcement across multiple AWS accounts, helping leaders provide consistent security policies at scale. Additionally, AWS Audit Manager helps leadership monitor compliance status and readiness for audits, supporting informed decision-making and demonstrating leadership's commitment to information security governance.

## Clause 6: Planning – Risk assessment and information security objectives

Clause 6 requires organizations to identify and assess information security risks, determine appropriate treatment options, and set measurable objectives for managing those risks. AWS offers several services to support this planning process. GuardDuty provides continuous intelligent threat detection and anomaly monitoring, helping organizations proactively identify potential risks within their AWS environment. Security Hub aggregates and prioritizes findings from GuardDuty, Amazon Inspector, and

other security services, offering a consolidated view of security risks to inform risk assessments. AWS Config enables continuous monitoring of configuration compliance and detects changes that might introduce security risks, which is critical for maintaining secure baselines and meeting regulatory requirements. CloudWatch provides risk planning capabilities through resource health monitoring that tracks infrastructure performance and availability metrics, CloudWatch Logs Insights that enables deep analysis of log data to identify operational issues and security anomalies, CloudWatch observability that delivers end-to-end visibility across distributed applications, and CloudWatch Investigations that provide automated root cause analysis for performance and availability incidents, collectively enabling proactive risk identification and evidence-based planning for availability and performance-related risks. These services collectively provide the data and insights needed to assess current risks, define risk treatment plans, and set informed security objectives.

## Clause 7: Support – Resources, awareness, and communication

**Resources**: Sustaining an ISMS requires financial, human, and technical resources. AWS simplifies this through AWS Cost Explorer for tracking resource usage, IAM Identity Center to track permissions, and AWS Service Catalog to manage IT resources.

**Training and awareness**: Organizations can use AWS-provided learning platforms like AWS Skill Builder and AWS Learning Paths to maintain the knowledge required for staff to manage and secure AWS environments.

**Automated notifications**: Amazon Simple Notification Service (Amazon SNS) and Amazon Simple Email Service (Amazon SES) can be used to distribute reminders, security alerts, and updates. AWS Chatbot can deliver notifications directly to collaboration tools like Slack or Amazon Chime for fast response.

**Secure communication channels**: Customers can use AWS services for clear, secure communications internally (between technical and business stakeholders) and externally (with regulators, auditors, or vendors). Customers can use Amazon WorkMail or Amazon SES for external customer or partner communications, or creating a support case with AWS Support for escalations and technical assistance.

## Clause 8: Operation

Clause 8 focuses on the effective implementation and control of the ISMS to manage risks and maintain secure operations. AWS supports this by providing a broad set of cloud services that help organizations operationalize their ISMS. AWS CloudFormation and Systems Manager automate infrastructure and application deployment, ensuring consistency and control that meet operational planning requirements. Continuous monitoring services such as AWS Config, CloudWatch, and Security Hub enable ongoing assessment of the organization's security posture and identification of new risks, facilitating regular risk reassessment. AWS security services, including IAM, AWS Key Management Service (AWS KMS), GuardDuty, and AWS Shield, enable effective risk treatment by enforcing access controls, data protection, threat detection, and incident prevention. Additionally, AWS Backup and CloudTrail support data availability, integrity, and audit logging, and helps maintain documented and verifiable operational processes.

### Clause 9: Performance evaluation

Clause 9 focuses on monitoring, measuring, analyzing, evaluating, and reviewing the performance of the ISMS to maintain its effectiveness and continual improvement. AWS provides a range of services that organizations can use to collect and analyze operational and security data critical for performance evaluation. Tools like CloudWatch and AWS Config deliver real-time monitoring and compliance tracking, while Security Hub aggregates security findings for a consolidated view of the environment's security posture. CloudTrail records audit logs of account activity, supporting internal audits and forensic investigations. For formal audit management and evidence collection, Audit Manager automates assessments against ISO 27001:2022 requirements, streamlining the internal audit process. These services collectively provide the data, insights, and automation necessary for management reviews and continuous assessment, so that organizations can make informed decisions that enhance the effectiveness and maturity of their ISMS.

### Clause 10: Improvement

Clause 10 emphasizes the need for organizations to identify and address nonconformities promptly and to continually improve the effectiveness of their ISMS. AWS offers a range of services that help detect, analyze, and respond to security incidents and operational issues. For instance, CloudTrail and CloudWatch provide detailed logging and monitoring to identify anomalies and trigger alerts. Security Hub and GuardDuty enable continuous threat detection and consolidated security findings, facilitating quick identification of potential nonconformities. When incidents occur, Systems Manager can help automate remediation actions to correct issues and prevent recurrence. Additionally, the audit capabilities provided by AWS through Audit Manager support the assessment and improvement of controls based on audit results.

Continuous improvement is embedded through tools like AWS Well-Architected Review, AWS Trusted Advisor, and custom Amazon QuickSight dashboards, each reinforcing an iterative, data-driven approach to enhancing ISMS maturity.

## Implementation of specific controls

Implementing ISO 27001:2022 controls across each thematic area can be significantly simplified through the strategic use of AWS services. The following section highlights a selection of controls and the corresponding AWS services that can be used to support the efficient, consistent, and auditable operation of these controls.

### A.5 – Organization controls

Organizational controls focus on establishing governance mechanisms that define how information is classified, protected, monitored, and managed throughout its lifecycle. In AWS environments, these controls are implemented through consistent resource management practices, automated monitoring,

and integrated security services that support information classification, incident management, business continuity, and compliance with applicable policies and standards. The following examples describe how AWS services can be used to support selected organizational controls defined in ISO 27001:2022.

**A.5.9 – Inventory of information and other associated assets**

Organizations need automated discovery and continuous tracking to maintain accurate asset inventories. AWS Resource Explorer provides centralized discovery and search capabilities across AWS resources, enabling organizations to locate and catalog assets across multiple accounts and Regions with advanced filtering and cross-account visibility that supports complex enterprise architectures. AWS Systems Manager Inventory automatically collects detailed configuration and metadata from Amazon Elastic Compute Cloud (Amazon EC2) instances, hybrid environments, and managed resources, providing real-time visibility into software installations, network configurations, and system details that support vulnerability management and compliance auditing. AWS Config continuously tracks resource configurations, relationships, and changes, creating an auditable record of asset states and dependencies while enabling automated compliance checking against organizational standards and regulatory requirements. Customers can also use resource groups and Tag Editor to enable systematic organization and classification of assets through standardized tagging strategies, and lastly the AWS Billing Console provides cost-based asset visibility and usage patterns to complete a thorough inventory framework.

**A.5.12 – Classification of information**

Organizations should establish a structured methodology for labeling and protecting information based on sensitivity and business impact. In an AWS environment, this can be achieved by implementing standardized tagging strategies through Organizations and using AWS Config to monitor for untagged or misclassified resources. Tags such as *Confidential* or *Public* should align with specific security measures like access control or encryption to maintain consistency and enforce protection requirements across the organization.

**A.5.18 – Access rights**

Managing access rights on a scale requires frameworks that balance security with operational efficiency while maintaining granular control over resource permissions. AWS offers several services that support customers with managing their identities across AWS services and resources. IAM provides fine-grained access control through policies, roles, and permission boundaries. These enforce least privilege, support temporary access patterns, and provide audit trails for compliance reporting and security analysis. Customers can use IAM Identity Center to connect to existing identity sources, use identity federation, and manage access at scale through single sign-on functionality. Amazon Cognito provides customer identity and access management for web and mobile apps, including authentication, authorization, and external user access management. Customers that want to migrate their active directory dependent workloads can use AWS Directory Service without the infrastructure management overhead. It provides a fully managed Microsoft Active Directory (AD) so customers can use existing AD investments, skills, and applications. AWS Control Tower establishes enterprise-wide access governance through automated

account provisioning, guardrails implementation, and centralized logging that help maintain consistent security baselines across organizational accounts and Regions. With AWS Resource Access Manager (RAM) organizations can share resources securely across AWS accounts and organizational units. RAM provides controlled access to VPCs, subnets, and other resources while maintaining centralized governance and preventing unauthorized resource exposure. These services support scalable access management while maintaining security standards and reducing unauthorized access risks.

**A.5.24 – Incident management**

Incident management capabilities must be prepared, practiced, and automated to reduce response time and impact. In AWS, organizations should configure CloudWatch alarms to support incident management by monitoring key metrics and thresholds, which can be paired with Amazon EventBridge to create an event-driven notification system that routes data from applications to defined targets. This can be paired with Amazon SNS or Amazon SES to generate alerts, or rules can be created in EventBridge that supports automated response and remediation. Customers can create pre-configured response plans in Systems Manager Incident Manager to automatically take action based on these events, such as triggering AWS Systems Manager Automation runbooks. After an incident has been identified, customers can use Amazon Detective to more quickly identify root causes by automatically collecting log data and build a linked set of data that enables faster and more efficient security investigations. Customers that want accelerated, continuous, expert-led investigation and containment of security events should sign up for AWS Security Incident Response to streamline their incident response program. A well-practiced incident response plan that integrates AWS tools supports faster containment and recovery, in alignment with ISO 27001:2022 requirements for structured incident handling.

**A.5.26 – Response to information security events**

Responding to security incidents requires coordinated capabilities that minimize impact, preserve forensic evidence, and maintain business continuity throughout investigation and recovery. As noted in control 5.24, AWS Security Incident Response provides structured playbooks and response capabilities that integrate with AWS services to run predefined incident response workflows. These workflows enable rapid containment and remediation of security events and preserve audit trails for post-incident analysis. Detective uses machine learning and graph analytics to investigate security findings. It analyzes relationships between AWS resources, user activities, and network behaviors, giving security teams context for root cause analysis through interactive visualizations and automated correlation. AWS Security Lake centralizes security data from multiple sources into a purpose-built data lake using the Open Cybersecurity Schema Framework (OCSF. Organizations can use Security Lake for advanced analytics, threat hunting, and cross-service correlation, with normalized data formats that support incident response decisions. AWS Elastic Disaster Recovery (AWS DRS) and AWS Clean Rooms provide specialized response capabilities for data protection scenarios, with AWS DRS enabling rapid recovery from ransomware or data corruption incidents, while AWS Clean Rooms supports secure incident investigation and data sharing with external parties without exposing sensitive information.

**A.5.30 – ICT readiness for business continuity**

To maintain availability and resiliency, organizations must incorporate business continuity into cloud architecture. AWS supports this through features like multi-Availability Zone (multi-AZ) and multi-Region deployments for services such as Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB, and Amazon Elastic Container Service (Amazon ECS). Amazon Simple Storage Service (Amazon S3) cross-Region replication can help maintain data redundancy, while Amazon Route 53 health checks and failover policies maintain application availability. AWS Backup allows for scheduled backups and centralized recovery plans across services. Business continuity testing should include simulated outages and recovery drills, using CloudFormation to restore infrastructure from templates and verify recovery time objectives (RTOs) and recovery point objectives (RPOs).

**A.5.33 – Protection of records**

Protecting records against data corruption, ransomware, and accidental deletion requires immutable storage and geographic distribution to maintain operational continuity and regulatory compliance. Amazon S3 Object Lock provides write once read many (WORM) functionality with legal hold and retention policies that prevent record modification or deletion for specified periods. This supports regulatory requirements such as SEC Rule 17a-4 and CJIS while providing tamper-proof integrity through cryptographic verification and audit trails. AWS Backup Vault Lock extends immutable protection across multiple AWS services by preventing backup deletion or modification, even by privileged users. It enforces minimum and maximum retention periods and maintains data integrity for compliance and forensic analysis. Cross-Region replication distributes protected records to geographically distant AWS Regions while preserving encryption and access controls, supporting disaster recovery and business continuity during regional disruptions. AWS DRS complements these protections through rapid environment restoration that maintains record accessibility and operational continuity during major incidents while preserving compliance posture throughout recovery.

**A.5.36 – Compliance with policies, rules, and standards for information security**

Organizations must identify and document applicable regulatory, contractual, and statutory requirements, and maintain alignment between their AWS workloads and these obligations. AWS Artifact provides on-demand access to compliance reports, including SOC 2, ISO 27001:2022, FedRAMP, and GDPR-related documentation. AWS Config conformance packs can be used to implement controls that map to regulatory requirements, while Audit Manager enables continuous evidence collection and assessment tracking. Responsibilities should be mapped clearly under the shared responsibility model, and third-party agreements should be reviewed for jurisdictional issues related to data residency or transfer across Regions.

## A.6 – People

People-related controls address how access is managed throughout the employment lifecycle. In AWS environments, centralized identity services, automation, and audit logging support timely access changes and removals.

### A.6.7 – Remote working

Remote work requires security controls that extend beyond the traditional network perimeter. Organizations need solutions that maintain consistent security standards regardless of user location or device. Site-to-Site VPN and AWS Client VPN establish encrypted network connections that extend organizational security perimeters to remote locations. These services provide secure tunnels for data transmission while enforcing network-level access controls and maintaining audit trails of remote connectivity sessions. Amazon WorkSpaces provides a fully managed virtual desktop infrastructure (VDI) that centralizes applications and data within AWS. Organizations can use WorkSpaces to provide secure desktop experiences to remote users without storing sensitive information on local devices, while enforcing policies centrally across distributed workforces. Amazon AppStream 2.0 enables secure application streaming without requiring full desktop virtualization, so that organizations can deliver specific applications to remote users while maintaining complete control over data access, preventing local data storage, and supporting compliance with data residency requirements. With these services, organizations maintain control over data and applications while providing flexible, secure access from multiple locations with appropriate authentication and monitoring.

## A.8 – Technological controls

Technological controls address the protection of information systems, applications, and data through technical safeguards. In AWS environments, these controls are implemented using managed services that support secure access, vulnerability management, monitoring, and auditability.

### A.8.1 – User endpoint devices

Centralized computing architectures reduce endpoint security risks by moving processing and data storage from local devices to managed cloud infrastructure. WorkSpaces provides fully managed virtual desktop infrastructure that reduces endpoint security risks by centralizing applications, data, and processing within AWS data 24centers. This reduces the likelihood that sensitive information resides on potentially compromised local devices, while supporting centralized policy enforcement, patch management, and compliance monitoring across distributed workforces. AppStream 2.0 delivers secure application streaming that prevents software installation on local devices, eliminating some malware vectors and data download risks while maintaining improved organizational control over application access, user sessions, and data handling policies through centralized management and monitoring capabilities. Both services also integrate with IAM for multi-factor authentication, session recording, and network access controls. This helps create a zero trust endpoint security model that reduces attack surfaces and traditional endpoint vulnerabilities through virtualization and isolation. These services enable organizations to maintain strict security controls over user access while supporting flexible work arrangements, ensuring that endpoint device security risks are minimized through centralized management and improved data isolation from potentially compromised local systems.

**A.8.2 – Privileged access rights**

Compromised privileged accounts pose serious risks, potentially allowing attackers to bypass security controls and access critical systems. Customers can use the same identity services listed above under A.5.18 to maintain granular privileged access management. These services provide granular management through fine-grained policies, administrative boundaries, and permission boundaries that enforce separation of duties and prevent privilege escalation, while supporting both temporary elevated access through role assumption and permanent privileged user management with detailed audit trails. AWS Organizations enhances privileged access governance through SCPs that establish organization-wide guardrails, preventing even privileged users from performing unauthorized actions across member accounts, while enabling centralized billing, compliance monitoring, and cross-account administrative delegation with appropriate controls. Combined, these services enforce least privilege, support continuous monitoring and audit capabilities, and maintain alignment between administrative access rights and organizational security policies and compliance requirements. A.8.3 – Information access restriction

Controlling access to information, especially sensitive information, is a core preventative measure to manage an organization's risk. Customers can use IAM to implement formal authorization processes for granting, reviewing, and revoking access rights based on need-to-know, supporting both role-based access control (RBAC) and attribute-based access control (ABAC) models. Customers can use IAM Access Analyzer to continuously validate that access policies align with least privilege requirements and identify unintended access to resources. S3 bucket policies, S3 Access Points, and S3 Object Lock provide granular control over data access based on user identity and resource attributes to address information access restriction requirements. For sensitive authentication data, customers can use AWS Secrets Manager and Systems Manager Parameter Store to securely store and control access to credentials and configuration data. Macie automatically discovers and classifies sensitive information to support access restriction decisions and help customers identify where sensitive data resides. Database access controls can be implemented through Amazon RDS IAM database authentication and Amazon Redshift fine-grained access controls to restrict information access at the row and column level. IAM access advisor provides visibility into service and action last-accessed information, enabling customers to identify and remove unnecessary permissions as part of regular access rights reviews required under A.8.3.

**A.8.4 – Access to source code**

Managing access to source code is critical for protecting intellectual property and ensuring secure development practices. Organizations can use AWS CodeCommit to host private Git repositories with granular access controls managed through IAM. Access permissions should be based on job function, and audit logs from CloudTrail should be enabled to track user activity within the repository. These logs can be analyzed using Amazon Athena or exported to a security information and event management (SIEM) solution for forensic review or policy violation detection.

**A.8.5 – Secure authentication**

Strong authentication requires balancing security with user experience across applications and user populations. Customers can use the same identity services listed previously under A.5.18 to maintain

granular privileged access management. Passwords are transmitted through secure encrypted means by the identity services, and IAM supports AWS Multi-factor authentication to enhance the secure authentication process.

These services support zero-trust security models, enforce strong identity verification, and provide flexibility to implement authentication controls aligned with organizational security policies and compliance requirements.

**A.8.6 – Capacity management**

Capacity management requires organizations to monitor resource usage, plan for demand changes, and scale infrastructure while maintaining security controls. CloudWatch provides monitoring and alerting for infrastructure performance metrics. Organizations can use CloudWatch dashboards, historical trend analysis, and configurable alarms to track usage patterns and plan capacity requirements. AWS Auto Scaling adjusts compute capacity based on demand metrics and scaling policies. Security groups, IAM roles, and other security controls apply consistently to newly launched instances, so security posture is maintained during scaling events. AWS Trusted Advisor analyzes account configurations and provides recommendations for capacity optimization, security improvements, and cost reduction based on AWS best practices. Together, these services help organizations maintain application availability and performance while controlling costs and preserving security controls during demand fluctuations.

**A.8.7 – Protection against malware**

Control A.8.7 requires organizations to implement measures that prevent and detect malicious software across their information systems, preserving data integrity and operational continuity. GuardDuty uses machine learning, anomaly detection, and integrated threat intelligence to identify malicious activity and suspicious behavior across AWS accounts. GuardDuty findings can then be routed to Security Hub and integrated with incident response workflows for automated remediation. Amazon Inspector performs automated security assessments of applications and infrastructure to identify software vulnerabilities, configuration weaknesses, and potential attack vectors that malware could exploit, providing prioritized findings with remediation guidance and continuous compliance monitoring. AWS Marketplace offers certified security solutions from leading vendors that provide additional malware protection capabilities, including endpoint detection and response (EDR), network security appliances, and specialized threat hunting tools that integrate with AWS services to create layered defense strategies. Customers can also combine AWS security services with third-party tools to strengthen threat detection, vulnerability management, and incident response.

**A.8.8 – Management of technical vulnerabilities.**

A proactive approach to identifying and mitigating technical vulnerabilities is essential to reduce attack surface. AWS offers Amazon Inspector for automated vulnerability assessments across Amazon EC2, AWS Lambda, and container environments. Patch automation and compliance monitoring can be managed with Systems Manager Patch Manager and AWS Config rules, respectively. Security Hub aggregates findings and maps them to compliance frameworks, so organizations can prioritize patching

based on exposure and criticality. This end-to-end workflow supports addressing technical vulnerabilities in alignment with ISO 27001:2022 requirements for risk-based remediation.

**A.8.9 – Configuration management**

Cloud and enterprise environments evolve continuously, and even minor, unauthorized configuration changes can introduce security weaknesses, erode compliance postures, and destabilize critical operations. AWS Config continuously monitors and records configuration changes across AWS resources, providing automated compliance evaluation against organizational standards, detection of configuration drift, and detailed audit trails that support forensic investigations and regulatory reporting. This continuous monitoring preserves visibility into resource relationships and dependencies, enabling organizations to maintain an accurate and current inventory of their AWS environments.

Patch levels are a core component of a system's software configuration baseline. AWS Patch Manager automates patching for managed nodes by applying security-related updates and other patch types across cloud and hybrid environments. Organizations implementing a patch management program can use Patch Manager to create patch policies that define approved patches, patch baselines, and maintenance windows, enforcing consistent security baselines across their AWS and on-premises infrastructure. Patch Manager integrates with AWS Systems Manager Compliance to assess patch compliance status across managed nodes, providing organizations with a centralized view of patching posture. Automated remediation workflows can be configured to detect and remediate non-compliant nodes, while unified dashboards in Systems Manager provide accurate inventory tracking and compliance reporting to support audit and regulatory requirements.

Service Catalog further strengthens control by enabling the deployment of pre-approved, compliant infrastructure patterns through governed service portfolios, ensuring new resources conform to organizational security policies at provisioning time and reducing configuration drift before it occurs. These services enforce security baselines, support continuous compliance monitoring, and maintain alignment between infrastructure changes and organizational policies while sustaining audit readiness at scale.

**A.8.10 – Information deletion**

Secure deletion of information is essential to prevent unauthorized recovery of sensitive data. In AWS services, this can be implemented by enabling object versioning and lifecycle rules in Amazon S3 to permanently delete objects after a retention period. For encrypted data, organizations should revoke KMS encryption keys to render the underlying data unreadable. Systems Manager can automate secure deletion workflows across EC2 instances or attached Amazon Elastic Block Store (Amazon EBS) storage volumes. Deletion logs should be captured through CloudTrail to verify policy enforcement and provide audit evidence.

**A.8.11 – Data masking**

Sensitive data exposure in non-production environments creates significant compliance and security risks for organizations, and should apply data masking techniques to limit exposure of sensitive

information in non-production environments while preserving data utility for development and testing purposes. AWS Glue DataBrew provides visual data preparation with built-in masking and anonymization functions. Users can apply consistent masking rules, generate synthetic data that preserves statistical properties, and create masked datasets for non-production environments without specialized expertise. Amazon RDS and Redshift provide native data masking through dynamic masking, column-level encryption, and query-level controls. These features protect sensitive data based on user roles and prevent unauthorized access to plaintext information. These services integrate with IAM and AWS KMS to provide access controls and encryption key management, while supporting audit logging and compliance reporting for data access and masking operations. Organizations can use these capabilities to implement data protection strategies that safeguard sensitive information throughout their lifecycle while supporting legitimate business use cases and maintaining compliance with data privacy regulations.

**A.8.12 – Data leakage prevention**

Data breaches cost organizations millions in damages and regulatory penalties each year, making leakage prevention especially important for protecting confidential information throughout the data lifecycle. Macie uses machine learning and pattern recognition to discover, classify, and protect sensitive data stored in Amazon S3, providing continuous monitoring for personally identifiable information (PII), financial data, and intellectual property while generating detailed findings and alerts when sensitive data is exposed or accessed inappropriately. GuardDuty watches for data exfiltration attempts and malicious communications by analyzing network traffic in VPC Flow Logs, Route 53 DNS queries, and CloudTrail activity. It spots suspicious data movement patterns and generates alerts that can tie into automated incident response capabilities. Organizations use these logs to monitor data flows, identify unusual transfer patterns, and investigate potential data leakage incidents. Automated data discovery, behavioral analysis, and network monitoring work across these services to protect sensitive information and support data protection regulations and organizational security policies.

**A.8.13 – Information backup**

Business continuity depends on backup strategies that protect against data loss, data corruption, and system failures while maintaining backup integrity and supporting an organization's recovery time objectives. AWS Backup provides centralized backup management across AWS services with automated backup scheduling, lifecycle management, and cross-Region backup replication, that organizations can use to implement consistent backup policies, monitor backup compliance, and maintain protection of critical data according to business requirements and regulatory standards. Amazon RDS automated backups create continuous, point-in-time recovery capabilities with automated daily backups and transaction log backups, providing up to 35 days of backup retention with the ability to restore databases to a point within the retention period while maintaining backup encryption and cross-Region backup copying for disaster recovery scenarios. S3 Cross-Region Replication and Same-Region Replication replicates objects across multiple locations with versioning support, providing durable backup storage with 99.999999999% (11 nines) durability and the ability to maintain multiple copies of critical data across geographically distributed AWS Regions. Organizations can use these services to implement robust backup and recovery strategies that protect against various failure scenarios, support

compliance requirements for data retention and availability, and support the continuation of business operations even in the event of significant system failures or disasters.

**A.8.14 – Redundancy of information processing facilities**

Control A.8.14 requires sufficient redundancy in information processing facilities to meet availability requirements. AWS multi-AZ deployments provide automatic failover capabilities for databases and applications across multiple Availability Zones within a Region, maintaining service availability during infrastructure failures and helping to ensure that infrastructure failures do not impact service availability. This also supports maintaining synchronous data replication and automated recovery processes that minimize downtime and data loss. Auto Scaling distributes application workloads across multiple Availability Zones and adjusts capacity based on demand patterns, and automatically replaces failed instances to maintain application availability during infrastructure failures. Route 53 provides DNS-level redundancy and health checking capabilities that route traffic away from failed endpoints to healthy alternatives, supporting both active-active and active-passive failover configurations with global load balancing and latency-based routing that supports optimal user experience across geographically distributed infrastructure. Together, these services address single points of failure, provide automatic failover, and maintain the availability and security of information processing facilities during infrastructure disruptions or regional outages.

**A.8.15 and A.8.16 – Logging and monitoring**

Logging and monitoring help detect unauthorized activities, support forensic investigations, and maintain risk visibility. CloudTrail provides immutable audit logging of API activities with data events capturing granular activity information such as object-level operations in S3 buckets and DynamoDB tables. VPC Flow Logs record network traffic details including source and destination addresses, ports, and protocols for comprehensive network monitoring. ELB Access Logs capture application-layer request information including client IP addresses, response codes, and processing times. S3 server access logs provide detailed object-level access records with requester authentication details and operation timestamps for S3 bucket activity. CloudWatch Logs aggregates system and application logs from AWS services and applications such as EC2 instances, Lambda functions, and on-premises systems with configurable retention policies and real-time streaming capabilities. GuardDuty analyzes CloudTrail events, VPC Flow Logs, and Route 53 DNS logs using machine learning algorithms to detect malicious activities including compromised instances and data exfiltration attempts. And Security Hub serves as a centralized dashboard that aggregates findings from GuardDuty, Amazon Inspector, Macie, and AWS Config to provide unified security posture visibility with automated compliance checking against industry standards. These services create an integrated logging and monitoring framework. They capture activities across network, application, and infrastructure layers. They also provide threat detection and automated incident response to help meet ISO 27001:2022 compliance requirements.

**A.8.17 – Clock synchronization**

Accurate time synchronization across distributed systems prevents security vulnerabilities, maintains audit trail integrity, and supports compliance requirements that depend on precise timestamp

correlation for forensic analysis and regulatory reporting. EC2 instances can be configured to automatically synchronize with the Amazon Time Sync Service, a fleet of managed Network Time Protocol (NTP) servers that provide highly accurate time references derived from atomic clocks. This maintains consistent timekeeping across compute resources while eliminating the complexity of managing dedicated time infrastructure. AWS managed services including Amazon RDS, Lambda, Amazon ECS, and Amazon Elastic Kubernetes Service (Amazon EKS) maintain automatic time synchronization with AWS time sources, providing consistent timestamps across application logs, database transactions, and security events without requiring manual configuration or ongoing maintenance. Time Sync Service delivers microsecond-accurate time synchronization through a leap-second-smeared time source that prevents time discontinuities during leap second events and maintains consistent time references for distributed applications even during global time adjustments. These capabilities mitigate time drift, maintain accurate audit trails for compliance reporting, and provide precise timestamp correlation for security monitoring and incident investigation.

**A.8.18 – Use of privileged utility programs**

Privileged utility programs such as administrative tools and diagnostic commands should be tightly controlled in cloud environments. To this end, IAM policies can be used to explicitly restrict usage of administrative actions for AWS services, whether by API or AWS Command Line Interface (AWS CLI) commands. Logs of this activity are generated by CloudTrail, and customers can use CloudTrail Insights to identify and respond to unusual activity. For critical systems like Amazon EC2 or Amazon RDS, customers can add an additional layer of security by using Session Manager for EC2 instances or Session Manager port forwarding with a bastion host for RDS instances. Session logging can then be enabled, and the logs sent to CloudWatch and be analyzed using CloudWatch Logs Insights and log anomaly detection to identify suspicious behavior. Customers can also use IAM Access Analyzer to identify unintended access to resources and data, which can be a security risk.

**A.8.19 – Installation of software on operational systems**

Unauthorized software installations create significant security vulnerabilities and compliance risks. Customers should use centralized control mechanisms that enforce approved software policies and restrict installations to authorized and approved software while supporting legitimate business requirements. Systems Manager can be used to inventory EC2 instances and record systems inventory data in AWS Config, and AWS Config Managed Rules to define compliance rules based on that inventory data and detect unauthorized applications. Systems Manager also provides software installation management through Patch Manager for automated patching, AWS Systems Manager Distributor for secure software package deployment, and Run Command for controlled software installation across EC2 instances and hybrid environments with detailed logging and compliance reporting. Service Catalog supports standardized software deployment through pre-approved, governed portfolios that help ensure only authorized applications are installed on operational systems. Self-service capabilities within Service Catalog maintain security controls and organizational policies during deployment. Systems Manager Session Manager addresses the need for direct system access during software installations, providing secure, auditable remote management capabilities that maintain forensic integrity and prevent unauthorized administrative access to operational systems. These services enforce software

installation policies, maintain system integrity, and provide audit trails for regulatory compliance while supporting efficient software lifecycle management.

**A.8.20 – Network security**

Protecting network boundaries and internal communication pathways is crucial to securing workloads in AWS. Organizations should design their network architecture using VPCs with separate public and private subnets, enforcing least privilege routing. Security groups and network access control lists (ACLs) should be configured to allow only necessary traffic. For centralized control and segmentation, AWS Transit Gateway and AWS Network Firewall can be used to inspect and control east-west and north-south traffic. VPC Flow Logs should be enabled to monitor network behavior and detect anomalies, while GuardDuty provides threat detection on network traffic, aiding in early detection of suspicious behavior.

**A.8.21 – Security of network services**

Organizations must identify and implement security mechanisms for network services, whether managed internally, outsourced, or consumed as cloud services. PrivateLink enables secure, private connectivity between VPCs and AWS services without traversing the public internet, eliminating exposure to internet-based threats while providing dedicated network paths with built-in encryption and access controls that maintain data confidentiality and integrity. VPC endpoints extend PrivateLink capabilities by creating secure, scalable connections to AWS services directly from private subnets, reducing attack surface by eliminating internet gateways and NAT devices while providing granular policy controls that restrict service access based on organizational requirements. Transit Gateway centralizes network connectivity management across multiple VPCs, on-premises networks, and AWS services, enabling secure inter-network communication with centralized routing policies, network segmentation controls, and monitoring that supports compliance auditing and security analysis. The result is isolated sensitive traffic, encrypted communication channels, and network service interactions aligned with organizational security policies.

**A.8.22 – Segregation of networks**

Organizations should segment their networks into security zones based on information classification and trust levels. VPCs provide fundamental network isolation through logically separated cloud environments with customizable IP address ranges, subnets, and routing tables that create secure network boundaries with complete control over inbound and outbound traffic flows. Security groups function as virtual firewalls that control traffic at the instance level through stateful packet filtering, enabling granular access controls based on protocols, ports, and source/destination specifications while supporting dynamic rule updates and logging for security analysis. Transit Gateway enhances network segregation by enabling centralized connectivity management with route table isolation, network access control lists (network ACLs), and cross-account network sharing capabilities that maintain security boundaries while supporting complex enterprise network architectures. These services integrate with

Network Firewall, VPC Flow Logs, and GuardDuty for network monitoring, threat detection, and forensic analysis that validate segregation effectiveness and support compliance requirements.

**A.8.23 – Web filtering**

Organizations should manage access to external websites to reduce exposure to malicious content and enforce acceptable use policies. Network Firewall provides stateful network traffic inspection with customizable filtering rules that block malicious domains, prevent data exfiltration, and enforce acceptable use policies through deep packet inspection, intrusion detection, and threat intelligence integration. Amazon Route 53 Resolver DNS Firewall enables DNS-level content filtering by blocking access to malicious or inappropriate domains before connections are established, providing centralized policy management across multiple VPCs with support for custom domain lists, threat intelligence feeds, and logging for compliance reporting. Both services integrate with AWS security services including GuardDuty, Security Hub, and CloudTrail to provide coordinated threat detection, automated incident response, and audit trails that support forensic analysis and regulatory compliance. These filtering capabilities extend to hybrid environments through Direct Connect and VPN connections, maintaining consistent web filtering policies across locations with centralized management and reporting.

**A.8.24 – Use of cryptography**

Organizations implementing AWS services must establish data protection measures across their cloud infrastructure, incorporating both in-transit and at-rest security controls to protect data confidentiality, integrity, and security. AWS offers data protection and encryption options for an organization's resources and workloads. Encryption in transit should be implemented using Transport Layer Security (TLS) 1.2 or later encryption whenever possible, especially when data leaves protected environments. Customers have the ability to enforce encryption in transit at multiple locations. All AWS service API endpoints enforce a minimum TLS protocol level of 1.2 for communications to AWS services. The Elastic Load Balancing service helps customers distribute their own network traffic and improve application scalability. Both Application Load Balancers (ALB) and Network Load Balancers (NLB) offer security policies for ALBs and NLBs that can be configured to enforce the use of TLS 1.2 or greater. ACM can be used to provision, manage, and deploy public and private SSL/TLS certificates to be used in these TLS connections and securely terminate traffic for compute workloads. Customers can enable ALB access logs and NLB access logs for information about the TLS requests sent to the respective load balancing instance, use the logs to analyze TLS traffic patterns and troubleshoot issues.

To avoid public internet exposure to VPCs customers can use PrivateLink to establish private connections from VPCs to AWS services. VPC Endpoint policies can control which AWS principals can use the endpoint to access an AWS service. Similar in nature to PrivateLink, Direct Connect offers private physical connections between customer locations and AWS services. MAC Security (MACsec) can be implemented to provide point-to-point encryption on Ethernet links. For organizations requiring secure site-to-site connectivity, AWS VPN is a scalable secure VPN service to with both Client and Site-to-Site options for remote workforce and locations respectively.

symmetric and asymmetric keys, including a post-quantum TLS option for API connections. AWS file storage services such as Amazon Elastic File System (Amazon EFS) and Amazon FSx, database services

such as Amazon RDS and DynamoDB, Amazon S3 object storage, and Amazon EBS block storage, all support KMS encryption with AWS-managed or customer-managed keys. AWS recommends customers use their own customer managed keys for the highest level of control and customization. Customer managed keys offer more flexibility in setting key rotation schedules, strict control over key usage, and the ability to share keys or control access through key policies, detailed auditing capabilities, or the ability to integrate key management with existing processes and tools. AWS best practices include employing separate KMS keys for data with different classification levels, distinct KMS keys for each application, and in some use cases a different key per AWS service.

AWS Config can be configured to monitor these settings and alert when a resource is changed and no longer meets the desired baseline configuration.

**A.8.25 – Secure development life cycle**

Organizations should integrate security requirements and controls into each phase of the software development lifecycle. Customers can incorporate the AWS Developer Tools into their software development life cycle (SDLC) to enhance their workflows. AWS CodePipeline orchestrates secure development workflows with automated security gates, vulnerability scanning integration, and approval processes that prevent insecure code from reaching production environments while maintaining development velocity and supporting compliance auditing. AWS CodeBuild provides secure, isolated build environments with integrated security scanning capabilities, dependency vulnerability analysis, and secure artifact management. This helps reduce the risk that build processes have introduced malicious code or expose sensitive information during compilation and packaging phases. AWS CodeDeploy enables controlled, secure deployment processes with blue-green deployment strategies, rollback capabilities, and integration with security monitoring tools that minimize deployment risks while providing detailed audit trails for change management and compliance reporting. Together, these services embed security controls throughout the software development process, from initial code commit through production deployment, maintaining consistent security requirements across development activities.

**A.8.26 – Application security requirements**

AWS WAF (web application firewall) provides application-layer protection with customizable rules that block common attacks, including SQL injection, cross-site scripting, and OWASP Top 10 vulnerabilities It also supports rate limiting, geo-blocking, and bot management capabilities that adapt to evolving threat patterns. Shield delivers distributed denial-of-service (DDoS) protection with automatic attack detection and mitigation, providing continuous protection for applications and infrastructure while offering advanced reporting and forensic analysis capabilities that support incident response and compliance documentation. Amazon Inspector can be configured to scan running applications automatically, to find vulnerabilities, configuration weaknesses, and security gaps. You receive prioritized findings with specific remediation steps. Continuous monitoring helps you maintain security standards throughout the application lifecycle. These services integrate with CloudTrail, CloudWatch, and Security Hub to provide security monitoring, automated incident response, and detailed compliance reporting that demonstrates application security effectiveness and regulatory adherence.

**A.8.27 – Secure system architecture**

Secure system architecture requires establishing and applying design principles that address security throughout the system development lifecycle. The AWS Well-Architected Framework provides security guidance through the Security Pillar, offering detailed best practices, architectural principles, and review methodologies that help organizations design and implement secure, resilient systems while maintaining operational efficiency and cost optimization. AWS Architecture Center offers extensive documentation, whitepapers, and case studies that demonstrate secure architectural approaches across industries and use cases, while the AWS Solutions Library provides pre-built, tested solutions that incorporate security best practices and compliance requirements for specific business scenarios. AWS reference architectures—available in the Architecture Center—deliver pre-validated, secure design patterns for common use cases including multi-tier applications, data analytics platforms, and hybrid cloud environments, providing detailed implementation guidance with security controls, compliance considerations, and operational best practices that accelerate secure deployment. These resources create an architectural security framework that enables organizations to design, implement, and maintain secure systems that align with industry standards, regulatory requirements, and organizational security policies while using proven patterns and expert guidance.

**A.8.29 – Security testing in development**

Validating that a secure software development life cycle is functioning properly is key to reducing the risk and impact of security flaws and quality issues in applications. Amazon Inspector provides automated security testing for applications and infrastructure with vulnerability assessments, configuration analysis, and compliance checking, and can be incorporated into development workflows. Amazon Inspector Code Security can be integrated with code repositories like GitHub and analyze source code for software vulnerabilities and unintended network exposure. Code Security supports more than 15 languages for static application security testing (SAST), 8 languages for software composition analysis (SCA), and 3 languages for infrastructure as code (IaC). Customers can also use Amazon Q Developer to perform code reviews using both generative AI and rule-based automated reasoning. As security policies are updated and detectors are added, reviews incorporate new detectors to support compliance of application code with the most up-to-date policies. AWS Security Agent and AWS DevOps Agent integration tools enable continuous security monitoring and testing across development environments, providing real-time vulnerability detection, configuration drift monitoring, and compliance validation that maintains security standards throughout the development lifecycle. These services integrate with popular development tools, continuous integration and delivery (CI/CD) pipelines, and security orchestration platforms to provide security testing automation that scales with development velocity while maintaining detailed audit trails and compliance reporting capabilities.

**A.8.31 – Separation of environments**

Organizations should maintain separate environments for development, testing, and production to prevent unauthorized access and data contamination across operational contexts, and limit the security blast radius of an event. AWS Organizations provides foundational environment separation through account-level isolation with SCPs that enforce organizational boundaries, can prevent cross-

environment resource access, and maintain strict governance controls. Separate VPCs within and across accounts create network-level isolation with independent IP address spaces, routing tables, and security group configurations that restrict traffic flow between environments unless explicitly authorized. VPCs also support secure connectivity options for approved inter-environment communication. IAM enhances environment separation through role-based access controls, cross-account access policies, and permission boundaries that restrict user and application access to resources appropriate to their operational context, while maintaining detailed audit trails for compliance reporting. These services create an environment separation framework that provides multiple layers of isolation, prevents accidental or malicious cross-environment access, and maintains appropriate security boundaries between development, testing, and production environments while supporting legitimate business workflows and compliance requirements.A.8.32 – Change management

Changes to information processing facilities and systems should follow defined change management procedures to preserve security and operational integrity. AWS Config monitors and records configuration changes across AWS resources with automated compliance checking against organizational standards, providing detailed change history, relationship mapping, and drift detection that supports forensic analysis and regulatory reporting requirements. CloudTrail captures audit logs of API calls and administrative actions across AWS accounts, creating immutable records of who made changes, when they occurred, and what resources were affected, while supporting log file integrity validation and long-term retention for compliance and security analysis. Systems Manager Change Manager provides structured change approval workflows with automated pre-checks, scheduled change windows, and rollback capabilities that help support changes follow organizational processes while maintaining detailed documentation and audit trails for compliance reporting. These services integrate with Security Hub, Amazon SNS, and third-party ITSM tools to provide automated change notifications, security impact analysis, and change management reporting so customers can maintain alignment between system modifications and organizational policies, security requirements, and regulatory compliance obligations.

**A.8.33 – Test information**

Organizations must protect test information by controlling its selection, use, and retention, particularly when test data is derived from production systems containing sensitive information. Test environments require realistic data for effective validation but must also protect sensitive information from unauthorized access. Amazon RDS snapshots—both automated and manual—provide point-in-time database copies that can be restored to separate test environments with encryption, access controls, and automated lifecycle management that maintains test data currency while maintaining production data security and compliance standards. DynamoDB backups offer continuous and on-demand backup capabilities with cross-Region replication and point-in-time recovery that enables creation of isolated test datasets while preserving data relationships, performance characteristics, and application compatibility requirements. Glue DataBrew and native database masking features provide data anonymization and synthetic data generation capabilities that create realistic test datasets without exposing sensitive information, supporting compliance with privacy regulations while maintaining data utility for testing purposes. These services enable organizations to implement test data management strategies that provide developers and testers with realistic, current data while ensuring that sensitive

information remains protected, privacy requirements are met, and test environments support effective application validation without compromising production data security or regulatory compliance.

# Conclusion

ISO 27001:2022 certification is achieved through a formal audit process; however, maintaining certification requires the continual operation, monitoring, and improvement of an ISMS. Organizations operating on AWS must go beyond implementing individual technical controls and demonstrate effective governance, risk-based decision-making, and consistent execution of ISMS processes over time.

This guide has demonstrated how AWS services can be used to support ISO 27001:2022 clauses 4–10 and selected Annex A controls across organizational, people, and technological domains. By integrating AWS identity, monitoring, automation, and security services into their ISMS, organizations can improve consistency, scalability, and auditability across cloud and hybrid environments while operating under the AWS shared responsibility model.

When applied appropriately, AWS services can help organizations scale their ISMS, improve visibility into security posture, and reduce the operational overhead associated with maintaining compliance. Responsibility for defining scope, assessing risk, documenting controls, and demonstrating conformity remains with the customer. Key takeaways:

- Use the AWS shared responsibility model to clearly define control ownership and ISMS scope.
- ISO 27001:2022 certification is obtained through an initial audit and maintained through continual ISMS operation and improvement.
- Use AWS services such as IAM, AWS Config, CloudTrail, Security Hub, AWS KMS, and AWS Backup to support control implementation, monitoring, and evidence generation.
- Integrate ISMS activities into day-to-day cloud operations, including change management, incident response, vulnerability management, and backup processes.
- Maintain traceable mappings between ISO 27001:2022 clauses, Annex A controls, and implemented AWS services through a documented Statement of Applicability (SoA).
- Prepare for audits continuously by embedding monitoring, logging, and review activities into the operating model rather than relying on periodic, manual assessments.

# Next steps

Now that you understand how AWS services can support ISO 27001:2022 implementation, the following actions can help you operationalize your ISMS in AWS environments and prepare for certification readiness:

- Establish and validate the ISMS scope in AWS: Begin by defining the organizational, technical, and geographic boundaries of your ISMS. Use AWS Organizations and AWS Control Tower to identify in-scope AWS accounts and organizational units, and use AWS Config resource inventory to enumerate workloads, Regions, and critical assets included within the certification boundary. Document scope exclusions and shared-responsibility considerations to support audit defensibility.
- Obtain AWS assurance documentation and shared-responsibility evidence: Access AWS Artifact to download ISO 27001:2022 certification reports, Statements of Applicability, and supporting assurance documentation relevant to AWS services used within your environment. Integrate these reports into your evidence repository to demonstrate inherited controls provided under the AWS shared responsibility model.
- Develop a control implementation and evidence collection strategy: Create an ISO 27001:2022 control mapping aligned to your architecture by using AWS Audit Manager custom frameworks. Map Annex A controls to the AWS services deployed in your environment and define automated evidence collection sources such as CloudTrail logs, AWS Config compliance records, and Security Hub findings to reduce manual audit preparation efforts.
- Implement centralized security logging, monitoring, and continuous compliance validation: Enable organization-wide CloudTrail trails, AWS Config conformance packs, and AWS Security Hub aggregation across all in-scope accounts. Establish automated alerting, remediation workflows, and periodic compliance reviews to demonstrate ongoing ISMS operation rather than point-in-time compliance activities.
- Perform readiness validation and engage compliance specialists: Conduct internal readiness assessments and architecture reviews to confirm that implemented controls operate effectively and produce audit-ready evidence. When needed, collaborate with AWS Security Assurance Services, AWS partners, or your AWS account team to review control design decisions, shared-responsibility mappings, and certification preparation activities prior to formal external audit engagement.

# Contributors

Contributors to this document include:

Ted Tanner, Principal Assurance Consultant, AWS Security Assurance Services

Satish Uppalapati, Associate Assurance Consultant, AWS Security Assurance Services

Viktor Mu, Sr. Assurance Consultant, AWS Security Assurance Services

Lola Quadri, Sr Assurance Consultant, AWS Security Assurance Services

# Document revisions

| Date | Description |
|---|---|
| **March 2026** | First publication |