ROCKETLEAP

ROCKETLEAP CHEAT SHEET

ISO 27001:2022 on AWS

Every Annex A control with the AWS action you need to pass the audit.

Steffan Norberhuis · Rocketleap

For CISOs, CTOs, and platform leads heading into certification.

rocketleap.dev

INTRODUCTION

Rocketleap ISO27001 AWS Cheat Sheet

ISO 27001 is daunting. It demands a professional organization handling information security risks, changes to how you ship software, and concrete changes to your AWS infrastructure. But once you pass it, the standard becomes a serious business accelerator.

This cheat sheet is the shortcut for the AWS side. It lists every Annex A control with the concrete AWS action you need to satisfy it, drawn from our years of experience in building production-ready AWS infrastructure in dozens of companies with ISO 27001 certifications and heavily regulated industries.

How to read this

Each Annex A control sits on its own row. The *"What you need to do in AWS"* column lists the AWS-side actions required to help you implement that control. Controls marked *N.A.* have no specific action for your AWS infrastructure.

Rocketleap helps you focus on **building your SaaS** instead of getting AWS to work. It is a **turn-key solution** to build and operate AWS under ISO 27001, following **CIS AWS Benchmarks**, so you can pass certification without building all that technology yourself. Rocketleap covers **all the ISO 27001 applicable AWS controls**, and we work alongside you through the audit to make sure you pass.

A.5 — Organizational Controls (37)

#	Control	What you need to do in AWS
A.5.1	Policies for information security	Adopt the CIS AWS Foundations Benchmark as the AWS infosec policy.
A.5.2	InfoSec roles and responsibilities	Create dedicated information security roles with org-wide security-audit access in AWS. Create org-wide auditing tools using AWS Config.
A.5.3	Segregation of duties	Define least privilege using RBAC in AWS Identity Center.
A.5.4	Management responsibilities	Automatically inform management of non-compliance using AWS Config.
A.5.5	Contact with authorities	—
A.5.6	Contact with special interest groups	Subscribe to the AWS Security Bulletin. Subscribe to CIS Benchmark updates.
A.5.7	Threat intelligence	Implement Threat Detection with GuardDuty. Implement Threat Investigation with Amazon Detective.
A.5.8	InfoSec in project management	—
A.5.9	Asset inventory	Assign ownership and segregate information assets using AWS accounts. Implement information classification with classification-specific KMS keys.
A.5.10	Acceptable use	Implement information classification with classification-specific KMS keys. Access per classification restricted by KMS resource policies.
A.5.11	Return of assets	Automatically provision access through roles with SSO and AWS Identity Center. Deny any current sessions on deactivation.
A.5.12	Classification of information	Classify KMS keys on confidentiality, integrity, and availability.
A.5.13	Labelling of information	Label information through classification-specific KMS keys.
A.5.14	Information transfer	Enforce information transfer policy through classification-specific KMS keys.
A.5.15	Access control	Provision access through roles with SSO and AWS Identity Center. Assign least-privilege access per role using six access levels: read-data, write-data, delete-data, use-resource, administer-resource, read-config.
A.5.16	Identity management	Provision access through roles with SSO and AWS Identity Center. Split access to root user MFA and password across two distinct groups.

#	Control	What you need to do in AWS
A.5.17	Authentication information	—
A.5.18	Access rights	Provision access through roles with SSO and AWS Identity Center. Enforce change through Infrastructure as Code and GitOps.
A.5.19	Supplier relationships	—
A.5.20	InfoSec in supplier agreements	—
A.5.21	ICT supply chain	—
A.5.22	Monitoring of supplier services	—
A.5.23	InfoSec for cloud services	—
A.5.24	Incident management planning	Rehearse incident response regularly.
A.5.25	Assessment of security events	Investigate security events using Amazon Detective.
A.5.26	Response to incidents	Alert all information security events through on-call alerting. Investigate using Amazon Detective.
A.5.27	Learning from incidents	Conduct a post-mortem after every information security incident and track actions to closure.
A.5.28	Collection of evidence	Implement a CloudTrail organisation-wide trail. Implement forensic logging on all AWS resources. Implement a log-archive account that aggregates forensic information.
A.5.29	InfoSec during disruption	—
A.5.30	ICT readiness for business continuity	Define RTO and RPO. Use multi-AZ or multi-region. Implement 3-2-1-1 backup strategy with native resource backup and AWS Backup.
A.5.31	Legal / regulatory	Segregate information using accounts based on data sovereignty. Enforce data sovereignty using regional SCPs. Apply necessary regulatory compliance baselines in AWS Config.
A.5.32	Intellectual property rights	—
A.5.33	Protection of records	Make CloudTrail logs immutable. Implement a 3-2-1-1 backup policy with native resource backup and AWS Backup. Make backups immutable with AWS Backup.
A.5.34	PII protection	Implement information classification with classification-specific KMS keys. Enforce data sovereignty using region-specific SCPs.

#	Control	What you need to do in AWS
A.5.35	Independent review	—
A.5.36	Compliance with policies	—
A.5.37	Documented operating procedures	—

A.6 — People Controls (8)

#	Control	What you need to do in AWS
A.6.1	Screening	—
A.6.2	Terms and conditions of employment	—
A.6.3	InfoSec awareness, education, training	—
A.6.4	Disciplinary process	—
A.6.5	Responsibilities after termination	—
A.6.6	NDAs	—
A.6.7	Remote working	Use AWS Session Manager / Systems Manager or Client VPN access for remote working.
A.6.8	Event reporting	—

A.7 — Physical Controls (14)

#	Control	What you need to do in AWS
A.7.1–A.7.4	Physical perimeters, entry, facilities, monitoring	Outsourced to AWS following the shared responsibility model.
A.7.5	Protecting against physical and environmental threats	Use multi-AZ or multi-region.
A.7.6	Working in secure areas	—
A.7.7	Clear desk and clear screen	—
A.7.8	Equipment siting and protection	—
A.7.9	Security of assets off-premises	Outsourced to AWS following the shared responsibility model.
A.7.10	Storage media	Outsourced to AWS following the shared responsibility model.
A.7.11	Supporting utilities	Use multi-AZ or multi-region.
A.7.12	Cabling security	Use multi-AZ or multi-region.
A.7.13–A.7.14	Maintenance, disposal	Outsourced to AWS following the shared responsibility model.

A.8 — Technological Controls (34)

#	Control	What you need to do in AWS
A.8.1	User endpoint devices	—
A.8.2	Privileged access rights	Provision access through roles with SSO and AWS Identity Center. Implement Temporary Elevated Privileges. Block the root user by SCP.
A.8.3	Information access restriction	Provision access through roles with SSO and AWS Identity Center. Enforce public-access prevention per resource. Restrict access per classification with KMS.
A.8.4	Access to source code	—
A.8.5	Secure authentication	Provision access through roles with SSO and AWS Identity Center. Use OIDC for CI/CD pipelines.
A.8.6	Capacity management	Implement auto-scaling. Implement CloudWatch capacity alerts.
A.8.7	Protection against malware	Implement AWS Web Application Firewall (WAF). Implement AWS GuardDuty Malware Protection.
A.8.8	Technical vulnerability management	Implement AWS Inspector.
A.8.9	Configuration management	Enforce change through Infrastructure as Code and GitOps. Run drift detection to monitor configuration and review drift.
A.8.10	Information deletion	Add lifecycle policies based upon data retention policies.
A.8.11	Data masking	Implement CloudWatch data masking.
A.8.12	Data leakage prevention	Implement defense-in-depth network strategy. Add Resource Control Policies (RCPs) to prevent data leakage. Implement data encryption at rest for every resource. Implement data encryption in transit for every resource.
A.8.13	Information backup	Implement 3-2-1-1 backup strategy with native resource backup and AWS Backup. Use AWS Backup for automatic validation of backups.
A.8.14	Redundancy of processing facilities	Use multi-AZ or multi-region.
A.8.15	Logging	Implement a CloudTrail organisation-wide trail. Implement forensic logging on all AWS resources. Add CloudWatch Metric Log Filters for log-pattern alerting. Add Event Dead Letter Queues on event-driven flows.
A.8.16	Monitoring activities	Implement VPC Flow Logs. Implement Threat Detection with GuardDuty.
A.8.17	Clock synchronization	AWS-managed NTP.

#	Control	What you need to do in AWS
A.8.18	Privileged utility programs	Block the root user by SCP. Restrict admin roles by Temporary Elevated Privileges.
A.8.19	Software on operational systems	Implement immutable and reproducible pipelines for EC2, containers, and serverless.
A.8.20	Networks security	Implement a tiered VPC with public / private / isolated subnets. Protect any opening in the network perimeter with AWS WAF or mTLS to trusted peers. Apply least-privilege access with security groups and NACLs. Use VPC endpoints for AWS traffic.
A.8.21	Security of network services	Implement AWS Shield for DoS. Add AWS Web Application Firewall for automated attacks. Add Route 53 Resolver DNS Firewall.
A.8.22	Segregation of networks	Implement subnets per workload with segregation based upon NACLs. Implement one VPC per environment.
A.8.23	Web filtering	—
A.8.24	Use of cryptography	Implement information classification with classification-specific KMS keys at rest. Enable automatic KMS key rotation. Use ACM for TLS certificates. Enforce encryption in transit with resource policies.
A.8.25	Secure development lifecycle	Enforce change through Infrastructure as Code and GitOps. Use OIDC for CI/CD pipelines. Add quality gates in the pipeline for Infrastructure as Code (cdk-nag, lint, tests, secret + dependency scans).
A.8.26	Application security requirements	—
A.8.27	Secure system architecture	Implement AWS Config to verify real-time.
A.8.28	Secure coding	—
A.8.29	Security testing in dev and acceptance	—
A.8.30	Outsourced development	—
A.8.31	Separation of dev, test, production	Provision per environment and per workload an AWS account. Separate VPC per environment.
A.8.32	Change management	Enforce change through Infrastructure as Code and GitOps.
A.8.33	Test information	Separate production environment so production information is not used for test information.
A.8.34	Protection during audit testing	Implement AWS Config to verify real-time.