AiOpsOne

CPS 234 → AWS Controls

A practitioner's mapping of every APRA CPS 234 requirement to the AWS services, AWS Config rules / Security Hub controls, and the audit evidence that satisfies it.

VERSION 1.0 · JUNE 2026 · AIOPSONE.COM · YOUTUBE @AIOPSONE

How to use this. Each row maps an APRA CPS 234 clause to the AWS control that demonstrates it and the exportable evidence an auditor will accept. Stand up the foundations below first — most rows light up from that baseline. This is practitioner guidance to accelerate your control mapping, not a substitute for your own CPS 234 risk assessment.

START HERE — THE FOUNDATIONS

Turn on **AWS Security Hub** with the **AWS Foundational Security Best Practices (FSBP)** and **CIS AWS Foundations** standards, enable **AWS Config** across every account and region, and centralise **GuardDuty** via an Organizations delegated admin. Then layer **AWS Audit Manager** with a custom CPS 234 framework to collect evidence continuously. Most Config rules referenced below (`securityhub-enabled`, `guardduty-enabled-centralized`) assume this baseline is live.

Para 13–14 Roles & responsibilities

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 13–14 Board ultimately accountable for information security; clearly defined roles and responsibilities.	AWS Organizations, IAM, IAM Identity Center, Service Control Policies	`iam-policy-no-statements-with-admin-access`; SCP guardrails enforced org-wide (no Config rule)	Org structure + SCP export; IAM Identity Center permission-set assignment report

Para 15–17 Information security capability

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 15–17 Maintain an information security capability commensurate with the threat, including for third parties that hold or manage assets.	GuardDuty, Security Hub, Amazon Inspector, IAM Access Analyzer	`guardduty-enabled-centralized`, `securityhub-enabled`, `iam-access-analyzer-enabled`; FSBP `Inspector.*`	GuardDuty coverage report; Security Hub security score; Inspector findings export

Para 18–19 Policy framework

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 18–19 Maintain an information security policy framework commensurate with exposures and vulnerabilities.	AWS Config conformance packs, Service Control Policies, AWS Audit Manager	Config **conformance pack** (Operational Best Practices for CIS / NIST as policy-as-code)	Conformance pack compliance summary; Audit Manager framework report

Para 20 Asset identification & classification

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 20 Classify information assets by criticality and sensitivity.	Resource Groups + tag policies, Amazon Macie, AWS Config inventory	`required-tags`; Macie sensitive-data discovery; FSBP `Macie.1`	Tag-policy compliance report; Macie classification findings; Config resource inventory

Para 21–22 Implementation of controls

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 21 · Identity Implement controls to protect assets, sized to the threat — strong identity and access management.	IAM, IAM Identity Center, Organizations	`iam-root-access-key-check`, `root-account-mfa-enabled`, `mfa-enabled-for-iam-console-access`, `access-keys-rotated`, `iam-password-policy`	Security Hub CIS score export; IAM credential report
Para 21 · Data Protect data at rest and in transit.	KMS, S3, EBS, RDS, ACM	`s3-bucket-server-side-encryption-enabled`, `s3-bucket-public-read-prohibited`, `encrypted-volumes`, `rds-storage-encrypted`, `kms-cmk-not-scheduled-for-deletion`	Per-resource Config rule compliance timeline
Para 21 · Network Boundary and network segmentation controls.	VPC, Security Groups, AWS WAF, Network Firewall	`restricted-ssh`, `restricted-common-ports`, `vpc-sg-open-only-to-authorized-ports`, `vpc-flow-logs-enabled`	Config compliance snapshot; VPC Flow Logs retention proof
Para 22 · Patching Vulnerability and patch management commensurate with the lifecycle stage.	Systems Manager Patch Manager, Amazon Inspector	`ec2-managedinstance-patch-compliance-status-check`; FSBP `Inspector.*`	SSM patch-compliance report; Inspector vulnerability export

Para 23–26 Incident management

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 23–24 Detect, respond to and recover from information security incidents in a timely manner.	GuardDuty, Security Hub, EventBridge, SSM Incident Manager	`guardduty-enabled-centralized`; EventBridge severity rules (no Config rule)	Incident Manager timeline; GuardDuty finding → response runbook
Para 25–26 Maintain logging sufficient to detect, analyse and respond to incidents.	CloudTrail, CloudWatch Logs, AWS Config	`multi-region-cloud-trail-enabled`, `cloud-trail-log-file-validation-enabled`, `cloud-trail-encryption-enabled`, `cw-loggroup-retention-period-check`	CloudTrail organization-trail config; log-retention policy export

Para 27–30 Testing control effectiveness

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 27–28 Test the effectiveness of controls systematically and on a risk basis.	Security Hub, Inspector, Prowler (open source), Audit Manager	Continuous Config evaluation; Security Hub FSBP / CIS standards scoring	Prowler assessment report; Security Hub standards score over time
Para 29–30 Escalate and remediate testing gaps; review after material change.	Security Hub automation rules, Config auto-remediation (SSM Automation)	Config **remediation actions** bound to non-compliant rules	Remediation execution history; before/after compliance delta

Para 31–32 Internal audit

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 31–32 Internal audit reviews the design and operating effectiveness of information security controls.	AWS Audit Manager, Config history, CloudTrail Lake	Audit Manager assessment against a custom CPS 234 framework	Audit Manager evidence collection; CloudTrail Lake queries; Config configuration timeline

Para 35–36 APRA notification

REQUIREMENT	AWS SERVICE(S)	CONFIG RULE / SECURITY HUB CONTROL	EVIDENCE ARTIFACT
Para 35 Notify APRA no later than 72 hours after a material information security incident.	EventBridge, Amazon SNS, SSM Incident Manager	EventBridge rule on GuardDuty / Security Hub severity → SNS (no Config rule)	Documented notification runbook; EventBridge → SNS delivery logs
Para 36 Notify APRA of material information security control weaknesses that cannot be remediated promptly.	Security Hub, AWS Audit Manager	Security Hub critical / high findings; Audit Manager weakness log	Security Hub critical-findings export; Audit Manager weakness register

Jayprakash Bilgaye · **AWS Certified Security – Specialty**