mysmartops

IRAP Security Assurance Programme

SaaS Provider — Multi-Cloud Kubernetes Pod Security

AWS EKS | Google GKE | Azure AKS

PROTECTED

IRAP Assessor Briefing | May 2026

A structured IRAP assessment service for SaaS providers running Kubernetes in the cloud — combining **automated evidence processing with qualified practitioner review**, across **42 PROTECTED baseline controls** covering Pod Security, multi-tenancy, data protection, incident response, and CI/CD pipeline security.

What We Deliver

A dedicated assessment pipeline for each cloud platform, supported by a structured evidence collection and practitioner review process. Each pipeline runs independently and produces a complete, versioned evidence package on every assessment cycle.

Three Dedicated Pipelines:

AWS EKS	Google GKE	Azure AKS

Two Supported Deployment Models:

Dedicated Cluster	Shared Cluster
One cluster per agency tenant. Full infrastructure isolation.	Multiple tenants on one cluster. Namespace and node-level isolation.

How Evidence Is Collected:

Platform Collection	Customer Submission
Configuration records, audit logs, policy state, and runtime data collected directly from the cloud platform.	Supporting evidence via the Compactor — our structured intake tool. Accepted formats include configuration exports, procedures, and architecture diagrams, within defined guardrails.

All evidence is reviewed and verified by a qualified practitioner before it enters the assessment pipeline. No evidence enters unverified.

Three Deliverables — Practitioner Reviewed:

- **Security Posture:** A scored summary per control family showing what passed, what did not, and by how much. Trend tracked across cycles. Validated by practitioner before release.
- **Control Narratives:** A plain-language explanation per control of what was found and whether it satisfies the ISM requirement. Drafted by pipeline, finalised by practitioner.
- **Findings Register:** A prioritised list of gaps with severity and remediation guidance. Confirmed and signed off by practitioner before delivery.

Control Coverage — 42 Assessed Controls

ID	Control Family	EKS	GKE	AKS
AC	Access Control (AC-2,3,4,6,17,24)	Full	Full	Full
IA	Identification & Auth (IA-2,4,5,8)	Full	Full	Full
SC	Boundary & Comms (SC-2,3,5,7,8,12,18,23,28)	Full	Full	Full
AU	Audit & Accountability (AU-2,3,9,11,12)	Full	Full	Full
SI	System Integrity (SI-2,3,4,7,12)	Full	Full	Full
CM	Config Management (CM-2,3,4,6,7,8)	Full	Full	Full
CP	Contingency Planning (CP-9,10)	Full	Full	Full
IR	Incident Response (IR-4,5,6)	Full	Full	Full
RA	Risk Assessment (RA-5)	Full	Full	Full
MP	Media Protection (MP-6)	Full	Full	Full
SA	Dev & Pipeline (SA-15)	Full	Full	Full

42 controls assessed across AWS EKS, Google GKE, and Azure AKS.

Scope: Pod Security · Multi-tenancy · Data protection · Incident response · CI/CD pipeline security.

Customer Responsibility (not assessed): SA-9 (External System Services) and SA-10 (Developer Configuration Management) are acknowledged in the assessment but fall outside pipeline scope. The SaaS provider is responsible for addressing these directly with their IRAP assessor.

Important: This assessment covers 42 controls relevant to Kubernetes-hosted SaaS workloads. It is a rigorous, platform-specific component of a broader IRAP assessment — not a substitute for one.

Why It Matters

Evidence you can stand behind

Every piece of evidence — whether collected from the platform or submitted by the customer — is verified by a practitioner before assessment begins. Nothing enters unreviewed.

Built for SaaS providers

The assessment is designed for organisations hosting agency data in Kubernetes. It addresses the real risks of that model — multi-tenancy, continuous deployment, data protection, and incident obligations — not just generic cloud security.

Both deployment models covered

Whether you run a dedicated cluster per agency or a shared cluster for multiple tenants, the assessment accommodates your architecture. Shared cluster assessments include additional controls for tenant isolation.

Incident response is in scope

Detection, handling, and reporting of security incidents are assessed — including the obligation to notify ASD when PROTECTED data is involved. Process evidence is submitted via the Compactor.

CI/CD pipeline security is in scope

The deployment pipeline is a path to production. Build environment hardening, change governance, and image integrity are assessed as part of the full picture — not treated as out of scope.

A tool that supports your assessor

The pipeline organises and drafts. A qualified practitioner owns the final outputs. Your IRAP assessor receives evidence that has been reviewed and verified — not raw machine output.

Assessment Metrics

Controls assessed	42 (PROTECTED)
Platforms	EKS · GKE · AKS
Pipelines	3 (dedicated)
Deployment models	Dedicated + Shared
Evidence intake	Platform + Compactor

The pipeline produces the draft. A qualified practitioner validates, refines, and finalises every deliverable before it reaches your IRAP assessor.

Evidence review	Practitioner verified
Deliverables	Posture · Narratives · Findings
ISM edition	2025 / NIST 800-53r5
Log retention	7-year documented
Customer resp.	SA-9, SA-10 noted

AC — Access Control	IA — Identity & Auth	SC — Boundary & Comms	AU — Audit	SI — System Integrity	CM — Config Management	CP — Contingency	IR — Incident Response	RA/MP/SA — Risk · Media · Pipeline

Use Cases & Customer Segment

SaaS Providers on Kubernetes | IRAP PROTECTED | Dedicated & Shared Cluster Models

Who This Is For

This assessment is designed for SaaS providers who run containerised applications on Kubernetes in the cloud and need to demonstrate their platform meets the Australian Government's PROTECTED security baseline.

Target Customer Profile

- **Hosting agency data** on behalf of one or more Australian Government customers
- **Seeking IRAP PROTECTED accreditation** as a prerequisite for government contracts
- **Running Kubernetes clusters** on AWS EKS, Google GKE, or Azure AKS
- **Deploying continuously** through automated CI/CD pipelines
- **Serving one or more tenants** on dedicated or shared cluster infrastructure

Six Core Use Cases

1. IRAP PROTECTED Accreditation

Controls: All 42 controls

The primary commercial driver. Formal assessment evidence that the Kubernetes platform meets the ISM PROTECTED baseline, suitable for submission to an IRAP assessor. Covers the full control set across all three platforms.

2. Continuous Accreditation Across Deployments

Controls: CM-2, CM-3, CM-4, CM-6, CM-7, AU family, RA-5

Accreditation is not a one-time event. Every significant platform change risks the accreditation status. Repeated assessment runs track posture over time, identify regressions, and provide evidence of remediation — supporting ongoing compliance without manual re-assessment effort.

3. Multi-Tenant Data Isolation Assurance

Controls: AC-3, AC-4, AC-24, SC-2, SC-3, SC-7, SC-28, AU-3

SaaS providers hosting multiple agency tenants on a shared cluster must demonstrate that each tenant's workloads, data, and audit trail are isolated from all others. Assessment covers both namespace-level and node-level isolation controls, with explicit treatment of cross-tenant risk.

Use Case Coverage Matrix

The matrix below shows how the 42 assessed controls map to each use case. All 42 controls contribute to the formal IRAP accreditation use case. Subsequent use cases draw on subsets of the control family depending on the specific risk being addressed.

Use Case	AC	IA	SC	AU	SI	CM	CP	IR	RA	MP	SA
IRAP Accreditation	●	●	●	●	●	●	●	●	●	●	●
Continuous Assessment	●	◐	●	●	◐	●	●	◐	●	◐	●
Multi-tenant Isolation	●	●	●	●	●	●	◐	◐	◐	◐	◐
Data Protection	●	●	●	●	●	◐	●	●	◐	●	◐
CI/CD Pipeline Security	◐	●	◐	●	●	●	◐	◐	●	◐	●
Incident Readiness	◐	◐	◐	●	●	◐	●	●	◐	◐	◐
Due Diligence Reporting	●	◐	●	●	◐	●	◐	●	●	◐	◐

● Primary coverage — control directly addresses this use case

◐ Supporting coverage — control partially addresses this use case

— Not directly relevant to this use case

Additional Use Cases

4. Data Protection Obligation

Controls: SC-8, SC-12, SC-28, SI-12, MP-6, AU-9, AU-11

When the SaaS provider manages agency data — not just hosts workloads — they carry specific data protection obligations. This includes encryption in transit and at rest, key lifecycle management, data retention, and secure deletion when a tenant offboards or data reaches end of life.

5. CI/CD Pipeline Security

Controls: CM-3, CM-4, SA-15, SI-7, SI-2, RA-5

The deployment pipeline is a direct path from development to production. Compromise of the CI/CD pipeline can bypass every cluster-level control. Assessment covers build environment hardening, change governance, secrets management in the pipeline, and image integrity from build through to deployment.

6. Incident Response Readiness

Controls: IR-4, IR-5, IR-6, SI-3, SI-4, CP-9, CP-10

PROTECTED systems handling agency data must demonstrate a tested incident response capability — including detection, containment, recovery, and reporting. IR-6 specifically addresses the obligation to notify ASD when a PROTECTED data breach occurs. Process evidence is submitted via the Compactor and reviewed by a practitioner.

Scope boundary: This assessment covers 42 controls relevant to Kubernetes-hosted SaaS workloads at the PROTECTED baseline. SA-9 (External System Services) and SA-10 (Developer Configuration Management) are documented as customer responsibilities and are not assessed by this service. This assessment is a rigorous component of a broader IRAP assessment — not a substitute for one.

IRAP Control Reference — Page 1 of 3

Access Control · Identification & Authentication · Boundary & Communications Protection | ISM 2025 / NIST SP 800-53 Rev 5

Control | Name	ISM Refs	Model	Definition	Evidence Sources & Assessment Approach
AC — Access Control				
AC-2 Account Management	ISM-0445 ISM-1175 ISM-1664	Both	Establishes lifecycle processes for creating, enabling, modifying, disabling, reviewing, and auditing user and service accounts across the system.	**Sources:** Configuration records, audit logs Assessment examines whether accounts are defined with appropriate roles, unused accounts are disabled, and account changes are recorded and traceable. Supporting access register documentation may be submitted via the Compactor.
AC-3 Access Enforcement	ISM-0430 ISM-1507 ISM-1508	Both	Enforces approved authorisations for access to system resources in accordance with applicable access control policies.	**Sources:** Configuration records, policy state Assessment verifies that access controls are actively enforced on workloads and namespaces, and that access is no broader than required.
AC-4 Information Flow Enforcement	ISM-0109 ISM-0110 ISM-0635	Both	Controls the flow of information within the system and between interconnected systems based on defined information flow policies.	**Sources:** Configuration records, policy state, audit logs Assessment examines whether network traffic between workloads is restricted by policy and flows are controlled at boundaries. In shared cluster deployments, cross-namespace and cross-tenant flows are explicitly assessed. Architecture diagrams may be submitted via the Compactor.
AC-6 Least Privilege	ISM-1507 ISM-1508 ISM-1175	Both	Allows only the minimum access required for each user or process to accomplish its assigned task.	**Sources:** Configuration records, policy state Assessment checks that workloads run without elevated permissions, unnecessary capabilities are removed, and access scope is tightly defined.
AC-17 Remote Access	ISM-1314 ISM-1173 ISM-1401	Both	Establishes usage restrictions and implementation guidance for all forms of remote access to the system.	**Sources:** Configuration records, audit logs Assessment verifies that remote access to cluster management is authenticated, restricted, and logged. Remote access policies may be submitted via the Compactor.
AC-24 Access Control Decisions	ISM-0430 ISM-1507 ISM-1508	Shared	Defines requirements for access control decisions where multiple subjects and objects are involved — particularly relevant where a single policy engine serves multiple tenants.	**Sources:** Configuration records, policy state Assessment verifies that access control decisions for workloads in a shared cluster correctly scope each tenant's access, and that one tenant cannot influence or override the access decisions of another.
IA — Identification & Authentication				
IA-2 Identification & Authentication (Org Users)	ISM-1173 ISM-0974 ISM-1546	Both	Uniquely identifies and authenticates all users and processes acting on their behalf before granting access to the system.	**Sources:** Configuration records, audit logs Assessment confirms all cluster access requires authentication through an approved identity provider and that anonymous access is disabled.
IA-4 Identifier Management	ISM-0445 ISM-1546 ISM-0418	Both	Manages system identifiers to prevent reuse, ensure uniqueness, and retire dormant identifiers within defined timeframes.	**Sources:** Configuration records, audit logs Assessment reviews whether service identities are uniquely assigned, not shared across workloads, and removed when no longer in use.
IA-5 Authenticator Management	ISM-0418 ISM-0421 ISM-1546	Both	Manages credentials used to authenticate users and processes, including provisioning, rotation, and revocation.	**Sources:** Configuration records, audit logs Assessment verifies credentials are rotated on schedule, not embedded in workload definitions, and that expiry is enforced. Credential management procedures may be submitted via the Compactor.
IA-8 Identification & Authentication (Non-Org Users)	ISM-1173 ISM-0974 ISM-1664	Both	Uniquely identifies and authenticates users outside the organisation, including external services and automated processes.	**Sources:** Configuration records, audit logs Assessment examines whether external service identities are individually credentialed, scoped to minimum access, and subject to the same controls as internal users.
SC — Boundary & Communications Protection				
SC-2 Application Partitioning	ISM-0109 ISM-0520 ISM-1491	Shared	Separates user functionality — including user interface services — from system management functionality.	**Sources:** Configuration records, policy state Assessment verifies that in shared cluster deployments, tenant workload namespaces are separated from cluster administration functions, and that tenants cannot access or influence cluster management services.
SC-3 Security Function Isolation	ISM-0109 ISM-0520 ISM-1491	Shared	Isolates security functions from non-security functions to prevent untrusted software from interfering with security mechanisms.	**Sources:** Configuration records, policy state Assessment confirms that shared cluster security functions — admission controllers, audit subsystems, policy engines — are isolated from tenant workloads and cannot be influenced or disrupted by any tenant.
SC-5 Denial-of-Service Protection	ISM-1236 ISM-0109 ISM-0521	Both	Protects the system against or limits the effects of denial-of-service attacks, including resource exhaustion.	**Sources:** Configuration records, runtime state Assessment verifies resource limits are defined for all workloads. In shared clusters, per-tenant resource quotas are assessed to confirm no single tenant can exhaust shared platform capacity.
SC-7 Boundary Protection	ISM-0109 ISM-0110 ISM-0520	Both	Monitors and controls communications at the external boundary and at defined internal boundaries between system components.	**Sources:** Configuration records, policy state, audit logs

				Assessment checks that network boundaries are explicitly defined and enforced. In shared clusters, inter-tenant boundary controls are assessed including shared ingress configuration. Network architecture diagrams may be submitted via the Compactor.
SC-8 **Transmission Confidentiality & Integrity**	ISM-0489 ISM-1139 ISM-0636	**Both**	Protects the confidentiality and integrity of information during transmission using cryptographic or equivalent safeguards.	**Sources:** Configuration records, runtime state Assessment confirms inter-workload and external communications are encrypted in transit and that plaintext transmission is not permitted.
SC-12 **Cryptographic Key Management**	ISM-0491 ISM-0492 ISM-0493	**Both**	Establishes and manages cryptographic keys including generation, distribution, storage, rotation, and revocation — both within the cluster and for dependent cloud data services.	**Sources:** Configuration records, audit logs Assessment verifies encryption keys are managed by the platform, rotated on schedule, and key access is restricted and audited. Covers both cluster-internal secrets and keys used by cloud data services outside the cluster. Key management policy documents may be submitted via the Compactor.
SC-18 **Mobile Code**	ISM-0619 ISM-0624 ISM-1288	**Both**	Defines acceptable code sources and technologies, and controls what code is permitted to execute within the system.	**Sources:** Configuration records, policy state Assessment confirms only images from approved sources are permitted to run, and unapproved or unsigned images are blocked before deployment.
SC-23 **Session Authenticity**	ISM-1254 ISM-0943 ISM-1139	**Both**	Protects the authenticity of communications sessions to prevent hijacking, replay, or tampering.	**Sources:** Configuration records, runtime state Assessment verifies management sessions and internal service communications use authenticated, integrity-protected channels.
SC-28 **Protection of Information at Rest**	ISM-0459 ISM-0460 ISM-1161	**Both**	Protects the confidentiality and integrity of stored information using cryptographic or equivalent safeguards.	**Sources:** Configuration records Assessment confirms stored data — secrets, configuration, persistent workload data, and data held in cloud services outside the cluster — is encrypted at rest using managed or customer-controlled keys.

Model key: **Both** = applies to dedicated and shared cluster deployments **Shared** = additional control for shared/multi-tenant clusters only **Cust. Resp.** = customer responsibility, documented but not assessed by this service

IRAP Control Reference — Page 2 of 3

Audit & Accountability · System Integrity · Configuration Management · Contingency Planning | ISM 2025 / NIST SP 800-53 Rev 5

Control | Name	ISM Refs	Model	Definition	Evidence Sources & Assessment Approach
AU — Audit & Accountability				
AU-2 **Audit Events**	ISM-0109 ISM-0580 ISM-1464	**Both**	Identifies events the system is capable of auditing and ensures logging is aligned with organisational and regulatory requirements.	**Sources:** Configuration records, audit logs Assessment verifies audit logging is enabled and configured to capture event types required under ISM for a PROTECTED workload.
AU-3 **Content of Audit Records**	ISM-0580 ISM-1536 ISM-0584	**Both**	Ensures audit records contain sufficient detail to establish what occurred, when, where, who was responsible, and what the outcome was.	**Sources:** Audit logs Assessment samples audit records to confirm they contain identity, action, resource, timestamp, and outcome. In shared cluster deployments, per-tenant audit attribution is explicitly assessed — records must be attributable to the correct tenant, not just the cluster.
AU-9 **Protection of Audit Information**	ISM-0583 ISM-0584 ISM-1536	**Both**	Protects audit records and audit tools from unauthorised access, modification, or deletion.	**Sources:** Configuration records, audit logs Assessment verifies audit logs are written to tamper-protected storage and that write access is separated from read access at the permission level.
AU-11 **Audit Record Retention**	ISM-0580 ISM-0585 ISM-1464	**Both**	Retains audit records for the period required to support investigation of past events and to meet regulatory obligations.	**Sources:** Configuration records Assessment confirms retention policies are configured for a minimum of 7 years, consistent with ISM requirements. Retention policy documentation may be submitted via the Compactor.
AU-12 **Audit Record Generation**	ISM-0580 ISM-1536 ISM-0584	**Both**	Ensures the system actively generates audit records for all defined auditable events at the required level of detail.	**Sources:** Configuration records, audit logs, runtime state Assessment confirms the audit subsystem is active, generating records continuously, and that gaps or failures in log generation are detected and alerted.
SI — System & Information Integrity				
SI-2 **Flaw Remediation**	ISM-1144 ISM-1690 ISM-1698	**Both**	Identifies, reports, and corrects system flaws; tests and applies updates to address vulnerabilities within defined timeframes.	**Sources:** Scan results, configuration records Assessment reviews whether workload images are scanned for known vulnerabilities and whether identified flaws are tracked and remediated within acceptable timeframes. Patch management procedures may be submitted via the Compactor.
SI-3 **Malicious Code Protection**	ISM-1417 ISM-0110 ISM-1288	**Both**	Implements protection mechanisms to detect and respond to malicious code at system entry and exit points and within the operating environment.	**Sources:** Configuration records, runtime state, audit logs Assessment confirms runtime threat detection is active on all cluster nodes and that alerts for suspicious behaviour are generated and routed to a monitoring function.
SI-4 **System Monitoring**	ISM-0109 ISM-0110 ISM-1537	**Both**	Monitors the system to detect attacks, indicators of compromise, and anomalous behaviour, and responds in accordance with defined procedures.	**Sources:** Audit logs, runtime state Assessment verifies monitoring is continuous, findings are surfaced to a responsible team, and coverage extends to workload-level activity. Monitoring procedures may be submitted via the Compactor.
SI-7 **Software & Information Integrity**	ISM-0303 ISM-1288 ISM-1697	**Both**	Employs integrity verification to detect unauthorised changes to software, configuration, and information, and takes defined action when violations are found.	**Sources:** Configuration records, policy state, scan results Assessment confirms only verified, approved images can be deployed and that the verification check is enforced automatically at deployment. Extended scope also covers integrity of the build pipeline that produces those images.
SI-12 **Information Management & Retention**	ISM-0580 ISM-0824 ISM-1465	**Both**	Manages and retains information within the system in accordance with applicable legislation, regulations, and organisational policies, including secure disposal when retention periods expire.	**Sources:** Configuration records, audit logs Assessment reviews data lifecycle management for agency data held by the SaaS provider — including retention schedules, archival processes, and secure deletion procedures when a tenant offboards or data reaches end of retention. Data lifecycle procedures must be submitted via the Compactor.
CM — Configuration Management				
CM-2 **Baseline Configuration**	ISM-1145 ISM-0301 ISM-1694	**Both**	Establishes, documents, and maintains a current baseline configuration of the system, reviewed and updated at defined intervals.	**Sources:** Configuration records, scan results Assessment compares current cluster and node configuration against an established secure baseline and identifies deviations. Baseline configuration documents may be submitted via the Compactor.
CM-3 **Configuration Change Control**	ISM-0301 ISM-1145 ISM-1531	**Both**	Establishes and documents a process for controlling changes to the system, ensuring changes are reviewed, approved, tested, and documented before implementation.	**Sources:** Configuration records, audit logs Assessment reviews whether changes to the cluster and deployment pipeline are governed by a documented change control process. CI/CD pipeline change logs and approval records may be submitted via the Compactor.
CM-4 **Security Impact Analysis**	ISM-0301 ISM-1145 ISM-1531	**Both**	Analyses changes to the system to determine potential security impacts prior to implementation.	**Sources:** Configuration records, audit logs Assessment verifies that security impact is considered and documented before changes are deployed to production. This includes changes pushed through the CI/CD pipeline. Security review records may be submitted via the Compactor.
CM-6 **Configuration Settings**	ISM-0301 ISM-1144 ISM-1694	**Both**	Establishes configuration settings that reflect the most restrictive mode consistent with operational requirements, and documents exceptions.	**Sources:** Configuration records, policy state

				Assessment verifies workload security profiles are set to the most restrictive applicable level and any exceptions are explicitly documented and justified.
CM-7 **Least Functionality**	ISM-1491 ISM-0303 ISM-1507	**Both**	Configures the system to provide only essential capabilities and prohibits or restricts all functions and access not required for operation.	**Sources:** Configuration records, policy state Assessment checks that workloads are configured with only required capabilities, elevated system permissions are not in use, and unnecessary access to host resources is blocked.
CM-8 **Component Inventory**	ISM-1653 ISM-0303 ISM-1491	**Both**	Develops and maintains an accurate, current inventory of system components that reflects the authorisation boundary and supports oversight.	**Sources:** Configuration records, scan results, runtime state Assessment verifies a current inventory of running workloads, images, and configurations is maintained and available for review. CMDB exports or inventory records may be submitted via the Compactor.
CP — Contingency Planning				
CP-9 **Information System Backup**	ISM-1511 ISM-1515 ISM-1516	**Both**	Conducts backups of system and user data at defined frequencies and verifies the integrity and availability of backup data at secure storage locations.	**Sources:** Configuration records, backup state records Assessment confirms automated backups are scheduled, stored securely, and integrity is verified. In shared clusters, per-tenant backup scope and recovery scope are explicitly assessed. Backup procedures and test evidence may be submitted via the Compactor.
CP-10 **System Recovery & Reconstitution**	ISM-1511 ISM-1515 ISM-1269	**Both**	Provides for the recovery and reconstitution of the system to a known, secure state following disruption, compromise, or failure.	**Sources:** Configuration records, backup state records Assessment reviews whether recovery procedures are documented, tested, and capable of restoring the system within defined time objectives. In shared clusters, per-tenant recovery scope is assessed. DR test records and runbooks must be submitted via the Compactor.

Model key: **Both** = applies to dedicated and shared cluster deployments **Shared** = additional control for shared/multi-tenant clusters only **Cust. Resp.** = customer responsibility, documented but not assessed by this service

IRAP Control Reference — Page 3 of 3

Incident Response · Risk Assessment · Media Protection · Pipeline Security · Customer Responsibilities | ISM 2025 / NIST SP 800-53 Rev 5

Control | Name	ISM Refs	Model	Definition	Evidence Sources & Assessment Approach
IR — Incident Response				
IR-4 **Incident Handling**	ISM-1784 ISM-0140 ISM-1685	**Both**	Implements an incident handling capability that includes preparation, detection, analysis, containment, eradication, and recovery from security incidents.	**Sources:** Audit logs, configuration records Assessment reviews whether a documented incident handling process exists and has been tested. The process must cover Kubernetes-specific incident scenarios including container compromise, credential theft, and workload tampering. Incident response plans and test evidence must be submitted via the Compactor.
IR-5 **Incident Monitoring**	ISM-1784 ISM-0140 ISM-1537	**Both**	Tracks and documents information system security incidents on an ongoing basis.	**Sources:** Audit logs, runtime state Assessment confirms that incidents are recorded, tracked to closure, and that a log of past incidents is maintained. Incident register or ticketing system records may be submitted via the Compactor.
IR-6 **Incident Reporting**	ISM-1784 ISM-0141 ISM-1685	**Both**	Requires personnel to report suspected security incidents to designated authorities within defined timeframes, including reporting obligations to external bodies where required.	**Sources:** Configuration records, audit logs Assessment verifies the provider has a documented process for reporting incidents to ASD and to affected agency customers. For PROTECTED data breaches, mandatory ASD notification obligations must be addressed. Incident reporting procedures must be submitted via the Compactor.
RA — Risk Assessment				
RA-5 **Vulnerability Scanning**	ISM-1144 ISM-1690 ISM-1698	**Both**	Scans for vulnerabilities in the system and hosted workloads at defined intervals, analyses results, and remediates confirmed vulnerabilities.	**Sources:** Scan results, configuration records Assessment confirms vulnerability scanning is integrated into the deployment process, results are reviewed, and critical vulnerabilities are addressed before reaching production.
MP — Media Protection				
MP-6 **Media Sanitisation**	ISM-0459 ISM-0824 ISM-1219	**Both**	Sanitises information system media — including digital storage — before disposal, reuse, or release, to prevent unauthorised disclosure of information.	**Sources:** Configuration records, audit logs Assessment reviews whether secure deletion procedures are in place for agency data when a tenant offboards, a storage volume is decommissioned, or data reaches end of retention. Deletion procedures and evidence of execution must be submitted via the Compactor.
SA — System & Services Acquisition				
SA-15 **Development Process, Standards & Tools**	ISM-0303 ISM-1531 ISM-1145	**Both**	Requires the development process to include security requirements, and that development tools, build environments, and pipelines meet defined security standards.	**Sources:** Configuration records, audit logs Assessment covers CI/CD pipeline hardening — build environment access controls, secrets management within the pipeline, dependency integrity checks, and pipeline change governance. Both platform-collected evidence and Compactor submissions are used.
CR — Customer Responsibility				
SA-9 **External System Services**	ISM-1401 ISM-1vulnerability ISM-1659	**Cust. Resp.**	Requires that external system services used by the organisation meet the same security requirements as internal services, and that agreements with external providers address security responsibilities.	**Sources:** Customer responsibility SA-9 is acknowledged as a control the SaaS provider must address directly with their IRAP assessor. It falls outside the scope of this assessment. The provider is responsible for documenting and evidencing the security requirements applied to all external cloud services and third-party integrations they depend on.
SA-10 **Developer Configuration Management**	ISM-0303 ISM-1531 ISM-1145	**Cust. Resp.**	Requires developers to perform configuration management for the system during development, which includes tracking and controlling changes to the system and maintaining the integrity of the system baseline.	**Sources:** Customer responsibility SA-10 is acknowledged as a control the SaaS provider must address directly with their IRAP assessor. It falls outside the scope of this assessment. The provider is responsible for documenting their developer-level configuration management practices, including source code management, branch protection, and developer access controls.

Model key: **Both** = applies to dedicated and shared cluster deployments **Shared** = additional control for shared/multi-tenant clusters only **Cust. Resp.** = customer responsibility, documented but not assessed by this service