algosec

Secure application connectivity.
Anywhere.

Whitepaper

ASD ISM

How AlgoSec supports Australian Government ISM guidelines

Version 01
May 2026

Version	Date	Changes	Author/Editor	Approved By
1	20-May-26	Initial document	JH	AN

Contents

Introduction and overview

The Australian Government Information Security Manual (ISM) provides cyber security guidance for protecting systems and data. AlgoSec helps organizations address the ISM areas that depend on network security policy, firewall and gateway posture, segmentation, monitoring evidence and controlled change processes.

This overview maps AlgoSec capabilities to ISM control themes where network visibility, access governance and policy automation can reduce operational risk and simplify audit preparation.

How AlgoSec supports ISM

AlgoSec provides visibility into application connectivity and security policies across hybrid environments, identifies risky or overly permissive access, supports firewall and gateway compliance reporting, and helps teams document, review and remediate network policy controls over time.

50	6
Mapped ISM controls	ISM guideline areas

Key outcomes

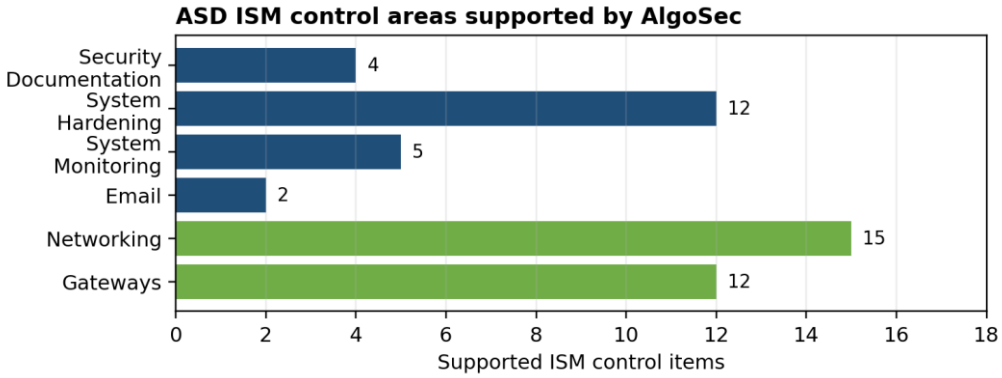
- Faster evidence gathering for network-centric ISM controls.
- Continuous visibility into firewall, gateway, routing and segmentation posture.
- Better prioritization of remediation by combining risk, vulnerabilities and connectivity context.
- Reduced exposure from unused, overly permissive, unauthorized or non-compliant access rules.

Scope note

AlgoSec supports ISM control implementation and evidence for network security policy management. ISM compliance also depends on governance, personnel, endpoint, application, incident response and operational processes that should be assessed separately

Control coverage summary

The mapping below summarizes ISM control areas where AlgoSec can provide visibility, risk analysis, policy governance or supporting evidence.



ISM guideline area	Relevant controls	How AlgoSec supports the area	Customer outcome
Security Documentation	ISM-0039, ISM-0888, ISM-1602, ISM-1163	Compliance reporting, scheduled analysis, real-time alerting, risk analysis and vulnerability scanner integration.	Current, reviewable security documentation and vulnerability-context evidence.
System Hardening	12 controls	Risk analysis, policy optimization, baseline compliance checks, access controls and SIEM/syslog support.	Identify device and policy hygiene gaps that may increase exposure.
System Monitoring	5 controls	Change History, log collection indicators, no-log rule checks, report retention and time-source baseline checks.	Traceable evidence for policy changes, monitoring posture and log-related controls.
Email	ISM-0267, ISM-0569	Allowed-services review, implicit deny assessment and risk checks for POP, IMAP and SMTP paths.	Validate that non-approved webmail and email bypass paths are controlled.
Networking	15 controls	Network Map, Connectivity Diagram, topology customization, access-control analysis, AppViz and baseline checks.	Document, govern and optimize segmentation and business-required access.
Gateways	12 controls	Gateway reporting, stateful inspection checks, anti-spoofing checks, user access controls, compliance reports and risk profiles.	Support gateway assurance across security domains and public boundaries.

What does this mean for organizations

- Network and gateway control evidence can be generated from current device, policy and topology data.
- Security teams can prioritize remediation using risk severity, exposure and application context.
- Compliance activities can shift from periodic manual collection to recurring review and validation.
- Control gaps can be linked to affected rules, devices or settings to guide remediation actions

1. Security documentation and continuous monitoring

AlgoSec helps maintain current security documentation and risk visibility for network security policy controls.

Control theme	ISM controls	AlgoSec support
Cyber security strategy and documentation	ISM-0039, ISM-0888, ISM-1602	Compliance reports, scheduled analysis and real-time alerts support documented security posture, recurring review and stakeholder notification of relevant changes.
Continuous monitoring plan	ISM-1163	Risk Analysis and vulnerability scanner integrations help assess vulnerabilities, determine potential impact and prioritize mitigations using risk and connectivity context.
Event logging policy and event details	ISM-0580, ISM-0585	Change History provides an independent audit trail for device activity, including dates, users, descriptions and equipment context.
Centralized logging, time source and retention	ISM-1405, ISM-0988, ISM-0859	Log collection indicators, no-log rule checks, report-retention settings and baseline checks help identify where logging controls need configuration or external SIEM support.

Relevant AlgoSec capabilities

- Compliance reports that show control status, settings and supporting details.
- Scheduled analysis to support recurring review of policy, topology and risk posture.
- Real-time alerting for relevant changes and security events.
- Change History for auditable firewall and gateway activity records.
- Vulnerability scanner integrations to connect scanner findings with actual network exposure.

Customer value

By connecting risk findings to network reachability and application context, AlgoSec helps teams focus on the vulnerabilities and policy gaps most likely to affect critical systems.

2. System hardening and secure administration

Control theme	ISM controls	AlgoSec support
Software version and device posture	ISM-1407	Risk Analysis helps identify unsupported or end-of-maintenance device software for remediation planning.
Configuration hardening and policy hygiene	ISM-0380, ISM-0383, ISM-0417	Policy optimization and risk checks highlight unused rules, covered rules, default password findings and similar hardening issues.
Authentication and access control	ISM-1546, ISM-1584	Role-based user management and per-device access controls help restrict access to authorized users over encrypted administrative paths.
Baseline-dependent checks	ISM-0421, ISM-1403, ISM-0853, ISM-0408	Baseline Compliance can support passphrase, account lockout, session and logon banner checks where baselines are configured.

3. Network documentation, segmentation and access control

AlgoSec provides current-state visibility into connectivity, topology and policy rules so organizations can assess whether access aligns with business need.

Control theme	ISM controls	AlgoSec support
Network documentation	ISM-0518, ISM-0516	Network Map and Connectivity Diagram help trace traffic, visualize network paths and document firewalls, routing and connectivity.
Segmentation and segregation	ISM-1181	Topology customization and policy analysis help define zones and assess whether traffic between zones aligns with sensitivity and criticality. Also Horizon AppViz provides a view of applications connectivity requirements, in the cloud and on-premises and enables application centric network segmentation.
Network access controls	ISM-0520, ISM-1182	Access Control and Allowed Services show what traffic is permitted within and between network segments, supporting least-privilege policy review.
Functional separation between servers	ISM-0385, ISM-1479	AppViz provides application-centric visibility into connectivity requirements to help minimize unnecessary server-to-server communication.
Network management traffic	ISM-1006	Allowed Services and access-control analysis help identify management services exposed between zones or from inappropriate sources.
IPv6 and SNMP controls	ISM-0521, ISM-1186, ISM-1428, ISM-1429, ISM-1430, ISM-1311, ISM-1312	Baseline Compliance and risk checks support review of IPv6, tunnelling and SNMP configuration where relevant device baselines are enabled.

Relevant AlgoSec capabilities

- Topology and connectivity views that show how systems, networks and security devices are connected.
- Traffic simulation and allowed-services analysis to validate whether existing or requested flows are permitted.
- Application-centric connectivity mapping to link network rules to business applications.
- Policy optimization to identify unused, disabled, risky, duplicate or overly broad rules.
- Controlled policy change workflows with risk and compliance checks before implementation.

Customer value

AlgoSec helps translate ISM segmentation requirements into operational evidence: zones, flows, application dependencies, risky access paths and remediation workflows.

4. Gateways, firewalls and email-control paths

Gateways and firewalls are central to many ISM control outcomes. AlgoSec helps validate gateway design, data-flow authorization, logging posture and rule-base hygiene.

Control theme	ISM controls	AlgoSec support
Gateway implementation and DMZs	ISM-0628, ISM-0637	Device reporting and topology views help evidence gateways between security domains and DMZ design for externally accessed services.
Authorized data flows and filtering	ISM-0631, ISM-1192	Firewall policy analysis, implicit-deny posture and stateful inspection checks support validation of authorized and filtered flows.
Ingress filtering and anti-spoofing	ISM-1427	Anti-spoofing checks identify whether gateway interfaces are configured to detect and prevent spoofed source addresses.
Gateway administration	ISM-0611, ISM-0616, ISM-1774	User management, role-based access, per-device permissions and connectivity views support least privilege, separation of duties and secure-path review.
Gateway logging and assessment	ISM-0634, ISM-1037	No-log rule checks, compliance reports, risk profiles and scheduled reporting support regular validation after configuration changes.
Evaluated firewall placement	ISM-1528, ISM-0639	Firewall and gateway inventory evidence helps show where firewalls protect public boundaries and security domains.
Email gateway controls	ISM-0267, ISM-0569	Allowed Services and Risk Analysis help verify non-approved webmail restrictions and prevent POP, IMAP or SMTP bypass of central email gateways.

Examples of control evidence and risk indicators

- Rules without logging that may reduce forensic visibility.
- Any-service, any-source or any-destination rules that increase exposure.
- Unsupported firewall management software or end-of-maintenance findings.
- Missing anti-spoofing, insecure firewall access or broad management access.
- Open email, database, remote-management or risky internal services that require business justification.

Customer value

AlgoSec helps identify what may be non-compliant, show which rules or settings contribute to the issue, and provide policy-management workflows to support remediation.

5. Recommended implementation approach

Activity	Purpose	AlgoSec output
Define the ISM assessment scope	Confirm applicable ISM release, network domains, cloud scope, gateways and assessment approach.	Scoped device groups, zones, applications and reporting boundaries.
Generate current-state evidence	Establish baseline visibility into devices, policies, routes, topology and risk posture.	ASD ISM report, compliance status, risk findings and topology views.
Validate segmentation and access	Confirm that traffic between zones and applications is business-required and appropriately restricted.	Connectivity diagrams, traffic simulations, access analysis and AppViz application flows.
Prioritize remediation	Focus effort on risk items with the greatest exposure and business impact.	Risk profiles, security ratings, risky-rule details and vulnerability-context findings.
Operationalize continuous review	Move from point-in-time evidence collection to recurring monitoring and controlled change.	Scheduled analysis, real-time alerts, Change History and policy change workflow evidence.

Control boundaries and assumptions

- AlgoSec supports ISM controls that depend on network security policy, firewall and gateway configuration, monitoring evidence and change governance.
- Some controls require customer-specific baselines, device support, integrations or manual verification.
- AlgoSec does not replace a full ISM assessment, IRAP assessment where required, endpoint hardening tools, SIEM platforms, patch management tools or organizational governance processes.
- Final compliance conclusions should be validated against the ISM release and assessment method selected by the organization
- This document is provided for informational purposes and is not legal, regulatory or audit advice. ISM applicability and compliance should be determined by the organization and its qualified assessor

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 100 times faster by automating application connectivity and security policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2300 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads.

AlgoSec Horizon platform utilizes advanced AI capabilities, enabling users to automatically discover and identify their business applications across multi-clouds, and remediate risks more effectively. It serves as a single source for visibility into security and compliance issues across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Additionally, organizations can leverage intelligent change automation to streamline security change processes, thus improving security and agility.

Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.