tufin The Security Policy Company.

ISM Australia: Proactive Measures to Strengthen Your Organization's Cybersecurity Posture

The Australian Cybersecurity Centre (ACSC) issued the Australian Government Information Security Manual (ISM) detailing a list of cybersecurity principles and guidelines to help organisations protect sensitive assets. According to the ACSC, the cybersecurity **principles** provide strategic guidance on how organisations can protect their systems and data from cyber threats, grouped into four key activities — **govern, protect, detect, and respond.**

For the **cybersecurity guidelines**, the ISM provides an extensive list of practical guidance, addressing governance, physical security, personnel security, and information and communications technology security issues. Each guideline covers security risks and security controls that the ACSC consider relevant for mitigation.

This document maps the capabilities provided by Tufin Orchestration Suite^{TM} against some of the ISM cybersecurity guidelines to help organisations mitigate some of the listed cybersecurity risks.

How Tufin Orchestration Suite helps support ISM guidelines

Tufin Orchestration Suite (TOS) is a security and segmentation policy management solution that helps network, security, and cloud teams proactively embed and maintain security best practices across their hybrid environment (on-premises and cloud). This is achieved via security automation that drives optimised, least-privilege segmentation, and trusted and secure changes, while ensuring policy adherence and business continuity.

Tufin categorically maps to ISM guidelines in 9 key areas.

Tufin Orchestration Suite features mapped to ISM guidelines

Managing cybersecurity incidents

Handling and containing data spills. When a data spill occurs, organisations should inform data owners and restrict access to the data. In doing so, affected systems can be powered off, remove their network connectivity, or apply additional access controls to the data. It should be noted though, that powering off systems could destroy data that would be useful for forensic investigations. Furthermore, users should take appropriate actions in the event of a data spill such as not deleting, copying, printing or emailing the data.

Security Control ISM-0133: *When a data spill occurs, data owners are advised and access to the data is restricted.*

Post-incident analysis. Post-incident analysis following a targeted cyber intrusion can assist in determining whether an adversary has been removed from a system. This can be achieved, in part, by conducting a full network traffic capture for at least seven days. Organisations should then be able to identify anomalous behaviour that may indicate whether the adversary has persisted on the system or not.

Security Control ISM-1213: *Post-incident analysis is performed for successful targeted cyber intrusions; this includes storing full network traffic for at least seven days after a targeted cyber intrusion.*

Tufin: Key Features in Support of ISM

Once a security incident has been identified, one of the primary goals is containment. This prevents further propagation and damage while investigation and more permanent measures can be deployed. Often, containment will include blocking certain hosts, ports, or services by implementing new network security policies while the investigation continues.

Applying new security policies for incident containment poses two problems. First, designing and implementing these changes takes time and a thorough understanding of network topology — two things which analysts and incident responders often lack. In an enterprise network, blocking a new host, port, or service is not as simple as creating a workflow which says, "Block host X on network device Y". Depending on the location of the incident, "network device Y" could be any one of hundreds of network devices, or even more than one device.

Second, changes made during incident containment are frequently made outside of the organisation's usual change control process. While the urgency may require going outside standard change control processes, bypassing its safeguards may result in additional risk to the network such as critical services unintentionally being taken offline, or compliance violations, as changes are not properly logged.

Risk-free containment with Tufin

- Quarantine/restrict access to compromised devices using Tufin accurate topology and change automation capabilities. With Tufin, admins gain visibility and control over their multi-vendor access policies and can automatically block access to compromised assets or to the internet. Organizations can make changes to enforcement points across multiple vendors to prevent data spill and allow further time for investigation and remediation.

- Tufin provides unified real-time visibility and policy intelligence through integration with leading SOAR, ITSM, and IPAM solutions, accelerating incident response based on a rich set of real-time data. Security Operations and Incident Response (SOAR) integrations enable automated playbook-driven response.

- Tufin also provides users with an abstracted view of network security policies based on application connectivity requirements. Users can easily query an application and discover its connectivity dependencies. This provides insight into the applications hosted on an impacted system, and it can also provide visibility into the connectivity allowed to/from the host, providing clues as to possible attack vectors and how the threat may have propagated.

- In the cloud, Tufin provides analysts and incident responders with a comprehensive view of their hybrid, multi-cloud ecosystem and the dynamic policies which govern it. Cloud security policies, including those which may violate best practices or be overly permissive, can be viewed across the entire hybrid cloud. Tufin also provides a connectivity graph, to easily visualise connectivity between nodes, clusters, and virtual machines, etc., which can be crucial for scoping an incident in a dynamic environment.

Actionable network intelligence across environments

- Tufin consolidates and maintains the rule metadata history (e.g. violations, last modification date, last hit, certification status, etc.) of multiple vendors' access policies for rapid analysis
- With Tufin, admins are alerted on rule/object hit count spikes, which may indicate malicious activity. For preventive measures, admins can set rule hit count threshold alerts to be sent to stakeholders, as well as automated/semi-automated responses where, if a rule hits the threshold, access is blocked to allow for further investigation
- Conversely, low/no hit reporting can indicate unused rules that might be candidates for removal
- Vulnerability Management integrations (e.g. Tenable, Rapid 7, Qualys) combine CVSS scores and severity with network access information to detect at-risk assets, prioritise patching efforts, and automate mitigation

Access to systems and data by service providers

To perform their contracted duties, service providers may need to access an organisation's systems and data. However, without proper security controls in place, this access could leave organisations' systems vulnerable – especially when such access occurs from outside of Australian borders. As such, organisations should ensure their systems and data are not accessed or administered by service providers unless such requirements, and associated measures to control such requirements, are documented in contractual arrangements. In doing so, it is important that sufficient measures are also in place to detect and record any unauthorised access, such as customer support representatives or platform engineers accessing an organisation's encryption keys. In such cases, the service provider should immediately report the cybersecurity incident to organisations and make available all logs pertaining to the unauthorised access.

Security control:

- ***ISM-1073:*** *An organisation's systems and data are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so*
- ***ISM-1576:*** *If an organisation's systems or data are accessed or administered by a service provider in an unauthorised manner, organisations are immediately notified*

Tufin: Key Features in Support of ISM

With Tufin, admins can define an expiration date for access rules, ensuring 3rd-party access is only available for as long as it's needed. The Tufin Rule Lifecycle Management app helps automate the recertification/decertification process. The app automatically identifies expiring or expired rules, maps them to their owners, and triggers an automated recertification or decertification process across the relevant multi-vendor network access solutions.

- Use Tufin automated processes to certify, modify, disable and/or decommission rules to achieve certification
- Set parameters for certification which includes pre-scheduled notifications about expired rules such as notification timelines, how long the renewal process should take, if the decertification process should be implemented automatically or not, and more.

System-specific security documentation

Continuous monitoring plan. A continuous monitoring plan can assist organisations in proactively identifying, prioritising, and responding to security vulnerabilities. Measures to monitor and manage security vulnerabilities in systems can also provide organisations with a wealth of valuable information about their exposure to cyber threats, as well as assisting them to determine security risks associated with the operation of their systems. Undertaking continuous monitoring activities is important as cyber threats and the effectiveness of security controls will change over time.

The ISM focuses on three types of continuous monitoring activities: vulnerability assessments, vulnerability scans and penetration tests. A vulnerability assessment typically consists of a review of a system's architecture or an in-depth hands-on assessment while a vulnerability scan involves using software tools to conduct automated scans. In each case, the goal is to identify as many security vulnerabilities as possible. A penetration test is designed to exercise real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as the identification of compromising critical system components or data. Regardless of the continuous monitoring activities chosen, they should be conducted by suitably skilled personnel; personnel can be internal to an organisation or a third party. This ensures there is no conflict of interest, perceived or otherwise, and that activities are undertaken in an objective manner.

Security control ISM-1163:

- *Systems have a continuous monitoring plan that includes:*
- *Conducting vulnerability scans for systems at least monthly*
- *Conducting vulnerability assessments or penetration tests for systems at least annually*
- *Analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls using a risk-based approach to prioritise the implementation of identified mitigations*

Tufin: Key Features in Support of ISM

The challenge with vulnerability scans has always been that too many critical vulnerabilities are discovered and not enough resources are available to patch them. Organisations need a way to prioritise the vulnerabilities that should be patched first and find a way to mitigate the risk from other vulnerabilities until they can be fully addressed. By combining vulnerability measures (CVSS scores and severity) with insights into how these vulnerabilities may be accessed and exploited via the network, admins have the context to identify and address vulnerabilities that pose the greatest threat to critical business assets. Tufin allows you to:

- Facilitate a risk-based approach to mitigation by enhancing vulnerability data with network insights
- View a list of exposed vulnerable assets within the specified network segments and their vulnerability severity levels. Admins can also view the rules that govern access to/from a vulnerable asset, the underlying services exposing the vulnerabilities, and relevant firewalls that provide access.

- Determine how remediation/mitigation efforts are reducing the attack surface through a vulnerability dashboard that shows remediation and mitigation trends over time
- Remove all network access associated with vulnerable assets via Tufin's pre-configured server decommissioning workflow – an automated/semi-automated process to remove access to the vulnerable asset and mitigate the risk of unpatched vulnerabilities

Operating system hardening

Software firewall. Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from extracting important data, as they generally only control which ports or protocols can be used between different network segments. Many forms of malicious code are designed to take advantage of this by using common protocols such as Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Simple Mail Transfer Protocol and DNS. Software firewalls are more effective than network firewalls as they can control which applications and services can communicate to and from workstations and servers. The in-built Windows firewall should be used to control both inbound and outbound traffic for specific applications.

Security control ISM-1416: *A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.*

Tufin: Key Features in Support of ISM

Tufin integrates with host-based software firewall solutions, as well as next gen firewalls (NGFW) and other network security solutions, such as Palo Alto Networks Panorama, Fortinet FortiManager, Check Point SmartDashboard, SDN environments (e.g. VMware NSX-T, Cisco ACI), and more. For security policy orchestration and automation, having a vendor agnostic solution with broad integration into an organization's security stack helps organisations manage segmentation/micro-segmentation policies across their heterogeneous hybrid environment consistently via a single console.

For cloud-native environments, the Tufin solution is also vendor-agnostic and uses APIs to retrieve information available on the cloud platforms. For Kubernetes-managed environments, Tufin uses a light weight Network Monitor DaemonSet (read only) on every node 'Kite pod' in the cluster. Kite is a pod that communicates between the Cluster Module plugins and the Tufin application. It is installed on one node in the cluster, as determined by Kubernetes.

Guidelines for system management

Dedicated administration zones and communication restrictions. Administration security can be improved by segregating administrator workstations from the wider network. This can be achieved a number of ways, such as via the use of Virtual Local Area Networks, firewalls, network access controls and Internet Protocol Security Server and Domain Isolation. It is recommended that segmentation and segregation be applied regardless of whether privileged users have physically separate administrator workstations or not.

Security control ISM-1385: *Administrator workstations are placed into a separate network zone to user workstations.*

Restriction of management traffic flows. Limiting the flow of management traffic to only network zones explicitly required to communicate with each other can reduce the consequences of a network compromise and make it easier to detect if it does occur. Furthermore, although user workstations will have a need to communicate with critical assets such as web servers or domain controllers, it is highly unlikely they will need to send or receive management traffic to these assets.

Security control ISM-1386: *Management traffic is only allowed to originate from network zones that are used to administer systems and applications.*

Tufin: Key Features in Support of ISM

Tufin provides complete visibility into User IDs and their use within organisational security policies. With Tufin, you can set and manage segmentation policies that apply to individual User IDs, ensuring users' least privilege access across the entire hybrid environment, inclusive of network devices, regardless of the user's location.

- Use AD/LDAP user groups to run traffic simulation queries and set segmentation policies based on User ID.
- As users are added/removed from groups, or new groups are added, Tufin updates the policies accordingly, so your segmentation policy always reflects users' access permissions.
- Define global network security policy alongside rule properties and other variables (e.g. forbid using "Any" in either source/destination/services).
- Automatic Policy Generator (APG) recommends rules based on traffic data, permissiveness level, and security mandate.

System patching

When patches are not available. When patches are not available for security vulnerabilities, there are a number of approaches that can be undertaken to reduce security risks. In priority order, this includes resolving the security vulnerability, preventing exploitation of the security vulnerability, containing the exploitation of the security vulnerability, or detecting exploitation of the security vulnerability.

Security vulnerabilities might be resolved by:

- disabling the functionality associated with the security vulnerability
- engaging a software developer to resolve the security vulnerability
- changing to different software or ICT equipment with a more responsive vendor

Exploitation of security vulnerabilities might be prevented by:

- applying external input sanitization
- applying filtering or verification on output
- applying additional access controls that prevent access to the security vulnerability
- configuring firewall rules to limit access to the security vulnerability

Exploitation of security vulnerabilities might be contained by:

- applying firewall rules limiting outward traffic that is likely in the event of an exploitation
- applying mandatory access control preventing the execution of exploitation code
- setting file system permissions preventing exploitation code from being written to disk

Exploitation of security vulnerabilities might be detected by:

- deploying a Host-based Intrusion Prevention System
- monitoring logging alerts
- using other mechanisms for the detection of exploits using the known security vulnerability

Security controls:

- ***ISM-1690:*** *Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists*
- ***ISM-1691:*** *Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release*
- ***ISM-1692:*** *Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours if an exploit exists*
- ***ISM-1693:*** *Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month*

Tufin: Key Features in Support of ISM

There are scenarios where patching is not always an option. For example, a patch may not be available or, if available, performing a patch may require costly downtime. And yet, security standards and regulations may prevent use of the affected applications until known high-risk vulnerabilities are resolved. Using Tufin's Vulnerability Mitigation App, you can remove all network access associated with the vulnerable asset through Tufin's preconfigured server decommissioning workflow, an automated process initiated directly from the app.

- Vulnerability management integrations combine CVSS scores and severity with network access info to detect at-risk assets, prioritise patching efforts, and automate mitigation.
  - Automate risk mitigation by blocking access to the critical asset (e.g. port, service, host, etc.) until remediation efforts can be fully implemented
  - Prioritise vulnerability remediation efforts based on exposure of critical assets, as well as severity of vulnerabilities
  - Easily assess overall risk to critical assets resulting from vulnerabilities that are both accessible and exploitable
  - Monitor and measure risk exposure over time via a comprehensive dashboard that highlights overall vulnerability exposure networkwide, as well as the impact of mitigation and remediation efforts

Change management

Change management process and procedures. The use of a change management process ensures that changes to systems are made in an accountable manner with appropriate consultation and approval. Furthermore, a change management process provides an opportunity for the security impact of any changes to systems to be considered. In implementing changes to systems, it is important that change management procedures clearly articulate the steps to be taken for each part of the change management process.

Security control ISM-1211: A change management process, and supporting change management procedures, is developed and implemented covering:

- *identification and documentation of requests for change*
- *approval required for changes to be made*
- *assessment of potential security impacts*
- *notification of any planned disruptions or outages*
- *implementation and testing of approved changes the maintenance of system and security documentation*

Tufin: Key Features in Support of ISM

Tufin provides unlimited, fully customisable policy change automation workflows that automate security policy changes across the hybrid environment. These automated/semi-automated workflows speed up the time it takes to fulfil policy change requests, where Tufin translates between zones, tags, and namespaces, and from security group rules to firewall rules, and designs and implements the required access changes. By automating policy changes, users can expedite the change process, reduce human error, and ensure all policy access changes are compliant with security requirements.

- Recommend network changes based on accurate topology modelling, path analysis, and security policy
- Simulate the impacts of rule changes, prior to implementation, to ensure changes do not result in policy violation/s
- Zero-touch rule change implementation across all leading firewalls and routers, and cloud platforms in the hybrid environment
- View policies and compare revisions across all network devices and infrastructure components
- Identify devices that allow/block requested access, and highlight the changes needed for remediation
- Real-time change notification, tracking and revision control, provide full user accountability
- Detect and alert on unpermitted actions or actions that take place outside of the authorised change management and configuration orchestration processes
- Change automation integrations (e.g., ITSM solutions) providing unified change workflows, where opening a ticket in ITSM triggers a workflow within Tufin for automated change design and implementation
- Full accountability with granular automated audit trails of all access activity, rule and policy changes
- Automated processes for handling potential security policy violations (e.g., escalations for security approval, exceptions handling, and proposed remediation)

Database servers

Network environment. Placing database servers on the same network segment as an organisation's workstations and allowing them to communicate with other network resources exposes them to an increased possibility of compromise by an adversary. Alternatively, in cases where databases will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary security risk.

Security control:

- ***ISM-1270:*** *Database servers that require network connectivity are placed on a different network segment to an organisation's workstations*
- ***ISM-1271:*** *Network access controls are implemented to restrict database server communications to strictly defined network resources such as web servers, application servers and storage area networks*
- ***ISM-1272:*** *If only local access to a database is required, networking functionality of database management system (DBMS) software is disabled or directed to listen solely to the localhost interface*

Separation of production, test and development database servers. Using production database servers for test and development activities could result in accidental damage to their integrity or contents.

Security control ISM-1273: *Test and development environments do not use the same database servers as production environments.*

Tufin: Key Features in Support of ISM

With Tufin, users define the segments/micro-segments, and the traffic that should be blocked or allowed between these segments. In addition, users can also leverage Tufin's predefined compliance segmentation policies (such as NIST, NERC, PCI, etc.) to start building their segmentation policy matrixes based on security best practices.

- Create logical zones using subnets, IP addresses, security groups, namespaces, etc.
- Use FQDN, EDLs, and CloudGuard objects to define policies or automate changes to policies
- The Tufin Unified Security Policy matrix provides visual representation of the micro-segmentation policies for simplified security policy management
- Users can easily identify the gaps between actual vs. desired security posture, and start cleaning up the rule bases across their multi-vendor, heterogeneous environments

Network design and configuration

Network documentation. It is important that network documentation accurately depicts the current state of a network. This typically includes network devices such as firewalls, data diodes, intrusion detection and prevention systems, routers, switches, and critical servers and services. Furthermore, as this documentation could be used by an adversary to assist in compromising a network, it is important that it is appropriately protected.

Security control:

- ***ISM-0516:*** *Network documentation includes a high-level network diagram showing all connections into the network; a logical network diagram showing all network devices, critical servers and services; and the configuration of all network devices*
- ***ISM-0518:*** *Network documentation is updated as network configuration changes are made and includes a 'current as at [date]' or equivalent statement*
- ***ISM-1178:*** *Network documentation provided to a third party, or published in public tender documentation, only contains details necessary for other parties to undertake contractual services*

Tufin: Key Features in Support of ISM

Tufin provides full visibility and control of which apps, workloads, and network security enforcement points are currently deployed and how they are connected. Tufin topology map is created by connecting to multi-vendors' firewalls, routers, switches, and cloud services, and retrieving all routing tables, as well as taking into account all Network Address Translation (NAT) and port number translation, VPNs, Multiprotocol Label Switching (MPLS), IPV6, security groups, IPAM data and so on. This results in a precise and highly accurate model of your hybrid environment allowing admins to start monitoring actual traffic across environments immediately, and identify anomalies, such as misconfigurations, and potential threats.

- Centralis, real-time visibility via a single dashboard of apps and their dependencies, workloads, network platforms, and infrastructure assets
- Visualise traffic flows of network topology and application connectivity throughout on-premises, multi-cloud, and SDN environments
- View apps, objects, services, source and destination, tags, regions, etc.
- View app dependencies and share resources between apps
- Allow search for specific servers, apps, rules, and objects across all network devices
- Automate Application Discovery integration (e.g. Cisco Tetration) with real-time visibility into dependency mapping and connectivity monitoring to achieve application connectivity compliance, identify outages, and restore connectivity
- Deliver ongoing, network zone discovery and updates through IPAM integrations based on accurate IP/DNS zone information for rapid provisioning and updating of network segmentation policy

Network segmentation and segregation. Network segmentation and segregation is one of the most effective security controls to prevent an adversary from propagating through a network and accessing target data after they have gained initial access. Technologies to enforce network segmentation and segregation also contain logging functionality that can be valuable in detecting an intrusion and, in the event of a compromise, isolating compromised devices from the rest of a network.

Network segmentation and segregation involves separating a network into multiple functional network zones with a view to protecting important data and critical services. For example, one network zone may contain user workstations while another network zone contains authentication servers. Network segmentation and segregation also assists in the creation and maintenance of network access control lists.

Security controls:

- ***ISM-1181:*** *Networks are divided into multiple functional network zones according to the sensitivity or criticality of data or services*
- ***ISM-1577:*** *Organisation networks are segregated from service provider networks*

Disabling unused physical ports on network devices. Disabling unused physical ports on network devices such as switches, routers and wireless access points reduces the opportunity for an adversary to connect to a network if they can gain physical access to network devices.

Security control ISM-0534: Unused physical ports on network devices are disabled.

Blocking anonymity network traffic. Inbound network connections from anonymity networks (such as Tor, Tor2web and I2P) to an organisation's internet facing services can be used by adversaries for reconnaissance and malware delivery purposes with minimal risk of detection and attribution. As such, this traffic should be blocked provided it will not meaningfully impact accessibility for legitimate users. For example, some organisations might choose to support anonymous connections to their websites to cater to individuals who want to remain anonymous for privacy reasons. In such cases, it is suggested that traffic from anonymity networks be logged and monitored instead. Additionally, outbound network connections to anonymity networks could be indicative of malware calling to a command and control server or of data exfiltration. They rarely have legitimate business uses and should be blocked.

Security controls:

- ***ISM-1627:*** *Inbound network connections from anonymity networks to internet-facing services are blocked*
- ***ISM-1628:*** *Outbound network connections to anonymity networks are blocked*

Tufin: Key Features in Support of ISM

With Tufin, admins can consistently apply any level of segmentation to microservices, network zones, User IDs, or App IDs across the hybrid environment, while using the Tufin solution as an orchestrator between zones, tags, and namespaces, and from security group rules to firewall rules. This ensures segmentation is enforced across cloud environments and datacenters, following the workload anywhere its deployed.

By mapping apps/workloads/ business units/subnets connections (North/South and East/West traffic), you can start modelling security policies and segmentation options. For example, you can locate and prioritise low and high-value assets, view which assets are most connected, and apply an appropriate segmentation strategy and granular security policy. With an accurate network topology map, you essentially create a shared understanding of security concerns and requirements between the various stakeholders – app owners, developers, and network and security personnel.

Tufin provides a path to segmentation. In the cloud, it starts by monitoring traffic and automatically learning the app/workload communication flows, and creates an allow-list policy which you can then edit, using natural high-level language to define segmentation policies. The result is a policy baseline, including backlist, allow-list, rule properties, and flow restrictions. Further, the policy can be generated as a YAML file, so it can be easily embedded in the SDLC for shift-left security.

For IP, User ID, and app-based segmentation, you can use the Tufin Unified Security Policy matrix to a create policy that controls what traffic is allowed between zones/apps. To quick start your segmentation, you can use one of Tufin's predefined compliance segmentation policies whereby all rules can be compared to these policies. You can define exceptions to policies, if needed, and once defined, policies are automatically distributed and enforced.

- Monitor unusual network activities according to policy based on rule hit count, zone changes, or anomalous port-specific network behaviour
- Automatically detect unused rules and objects, shadowed and overly permissive rules, rule and server candidates for decommissioning
- Optimise of policies (rule clean up) by identifying misconfigured, expired, risky or unused rules, and objects
- Recommend network changes based on accurate topology modelling, path analysis, and security policy
- Automatically remove all access associated with decommissioned server from firewall policies
- Detect and alert on unauthorised traffic flow; apps can be quarantined, and traffic flows can be redirected, or blocked
- Identify network devices that allow/block requested access, and highlight the changes needed for remediation