Compliance Guide:
ASD ISM OVERVIEW

Huntsman®
Defence-Grade Security Platform

Australian Information Security Manual

Mapping to the Principles using Huntsman®

INTRODUCTION

In June 2010, The Australian Government Protective Security Policy Framework (PSPF) prompted government agencies to develop a security culture, to: i) protect their capacity to function properly ii) provide safety for stakeholders iii) maintain public confidence and iv) safeguard information they retain.

The Australian Signals Directorate (ASD) has since released its more prescriptive Information Security Manual 2014 (ISM) based on observations of activity on Australian Government IT networks. The ISM is designed to assist government agencies to apply a risk-based approach to protecting their information and ICT systems[1] yet its advice is just as relevant to the private sector.

This overview summarises the main principles from Section 2 of the ISM and shows how Huntsman® SIEM technology supports compliance with many of them. A detailed mapping guide to section 3, ISM Controls, is available on request.

ISM OBSERVATIONS

The ISM notes that, while information technology provides significant commercial enablement and efficiencies, public and private networks are subject to unprecedented levels of cyber security threat from individuals, interest groups, criminal organisations and nation states. Further, with Australia's increasing commercial reliance on the Internet, the potential risks are increasing as perpetrators exploit vulnerable environments and new technologies. The ISM details important information about cyber threats and provides principles and controls to protect agency systems and their information.

ISM KEY QUESTIONS

The ASD observes that malicious cyber activity will continue to impact Australia's national security, prosperity and social well-being into the future. To deal with increasingly sophisticated targeted attacks, it's recommended that organisations implement risk-based IT security strategies, and ask themselves five key questions when assessing and managing their IT risk status:

1 Executive Companion, Australian Government Information Security Manual, Commonwealth of Australia, 2012

- Are we ready to respond to targeted cyber security incidents?
- What would a cyber security incident cost our organisation?
- Who might benefit from having access to our information?
- What controls do we have in place to protect ourselves from serious threats?
- Is the behaviour of our staff helping us foster a strong security culture?

The answers to these questions will help organisations to establish the nature and extent of their IT security risk, to review the effectiveness of existing actions, and to improve their response readiness to a cyber-attack.

COMPLIANCE WITH ISM

The success of any IT security monitoring and protection program hinges on integrating your people, technology and processes effectively, to monitor ongoing compliance with guidelines, principles, policies and regulations. In relation to compliance with the principles and controls of the ISM, technologies like Huntsman® can play a vital role.

The Huntsman® platform is particularly effective in this role, as it helps to comply with a number of ISM principles by accepting and analysing data that measures the governance of IT systems and users. As a sophisticated policy management engine, Huntsman® also helps to manage a number of the ASD's 10 Top Mitigation strategies and determine their effectiveness in your organisation.

PROTECTION AS WELL

Huntsman® has distinct advantages over many other Security Information Event Management (SIEM) systems because it is an automated behavioural analysis engine. This means that, as well as incorporating the functionality of an effective SIEM, it applies behavioural technology to establish normal activity across the enterprise, and to identify and alert on events that stray from the norm.

The net result is that, in a single product, Huntsman® directly addresses the specific functional requirements detailed in the ISM, and also provides broader threat detection capabilities, proactive monitoring and real time alerting.

RAPID RESULTS

Huntsman® ships with built-in support for most common network devices and also offers straightforward log collection for bespoke applications. As Huntsman® automatically identifies threats across any network, environment or system based on deviation from normal activity rather than recognition of predefined signatures, there is no need for ongoing signature databases or tuning to respond to new threats. This significantly reduces the resources and costs required to implement and operate Huntsman® compared to most other SIEM systems.

In addition, Huntsman® is easy and fast to use, so analysts and investigators can drill down and analyse the root cause of incidents quickly, enabling cyber-attacks to be intercepted before costly damage can occur.

PROVEN TRACK RECORD

Huntsman®'s advanced capability has been proven in mission-critical environments for over a decade, protecting defence, intelligence, border control, law enforcement and infrastructure in government, and finance, communications and manufacturing in corporate environments worldwide. Huntsman® adaptive architecture and easy scalability also ensure the flexibility to meet future challenges of the changing threat landscape.

MAPPING TO ISM WITH HUNTSMAN

The ISM is divided into three sections. The following guide maps to the second section, ISM Principles, and identifies where the technology can specifically assist in meeting the compliance requirements of ISM 2014.

This mapping guide is designed to help organisations to meet the requirements for the ISM as part of a formal IT Security management process. However, before considering these requirements, it's recommended that you devise your own risk assessment process to establish the likelihood and impact levels (ILs) in your organisation, when assessing the suitability of risk mitigations contained in the ISM.

Table 1.0	**Mapping to the ISM with Huntsman®**
System Accreditation	
	Huntsman® helps prepare an organisation for audit by providing reports on compliance status and highlighting systems that are non-compliant. The Huntsman® forensic repository simplifies the audit process by providing easily accessible information for auditors to demonstrate that appropriate controls have been implemented.
Information Security Monitoring	
	Huntsman® shows changes that have been made across an organisation, allowing the true state of security posture to be illustrated continuously. Huntsman® prioritises information based upon the organisation's security assets, including information about vulnerabilities & patching to highlight the items of greatest risk.
Cyber Security Incidents	
	Huntsman® identifies cyber security incidents that other technologies can miss, by combining information from signature- and pattern-based technologies via its patented Behavioural Anomaly Detection engine. Huntsman® not only raises awareness of potential security breaches, but provides security personnel with a powerful tool to investigate issues in a timely manner. The fully-integrated incident management system within Huntsman® provides the ability to report on how quickly issues are addressed, which systems have been affected and the trends of attacks over time.

Personnel Security

Huntsman® shows policy violations in real time allowing inappropriate use of services, including internet access, to be identified as they happen. Huntsman® reports on patterns of misuse allowing security awareness training to be targeted to the departments where most needed.

Communications Infrastructure

Huntsman® identifies improperly-configured devices that may be 'leaking' information. Huntsman® shows where these devices are and how long they have been active. Huntsman® also alerts on changes to devices that increase their risk profile, allowing remediation to take place before a data spill occurs.

Media Security

Huntsman® alerts when removable media is connected to systems and identifies the system user that inserted the device. Huntsman® also automatically responds to the attachment of removable media, thereby helping to minimise the risk of data loss.

Software Security

Huntsman® monitors the use of applications and the installation of patches and updates. The restriction of application use to the minimum requirement can be verified by Huntsman®. Suspicious activity from applications, such as attempts to send data to an external actor, are automatically detected using the patented Behavioural Anomaly Detection engine.

Access Control

Huntsman® monitors access attempts, both successful and not, facilitating the examination of who accessed what and when. Huntsman® alerts on policy violations such as system users accessing protected systems remotely or the use of shared accounts. Suspicious access patterns can be investigated and alerts can be generated for abnormalities using the patented Behavioural Anomaly Detection engine.

Cryptography

Huntsman® protects cryptographic systems from being compromised, to ensure that encryption is not disabled or weakened. Huntsman® alerts if cryptographic algorithms not approved by ASD are detected.

Network Security

Huntsman® monitors network activity and provides a visual representation of this data to yield a simple-to-understand overview of complex environments. Huntsman® ensures that high risk items are blocked and retains a reliable, auditable trail of what has been filtered. Logical network separation, such as the division between voice and data, is affirmed by Huntsman® which alerts when traffic breaks partition boundaries. Suspicious activity detected on a priority asset, by its patented Behavioural Anomaly Detection engine, allows an immediate response.

Cross Domain Security

Huntsman® ensures that appropriate filters are in place on gateways, as well as providing an evidential, auditable trail of blocked and permitted content. The flow of information between security domains is presented graphically to assist with comprehension of extensive data. The volume and direction of data crossing the gateway is monitored for suspicious activity by the patented Behavioural Anomaly Detection engine. Huntsman® highlights changes to a security domain connected to a gateway that can affect the security of other connected domains.

Working Off-Site

Huntsman® ensures that policies are followed by remote users as well as on-site system users. Huntsman® identifies users' activities whether they are connecting to systems from public locations like airport lounges, or cafes, and tracks the remote activities. Automated responses can be applied for unusual remote connections and anything suspicious about the remote location or session can be detected by the Huntsman® Behavioural Anomaly Detection engine.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman