Information security manual

Guidelines for security assurance

Last updated: June 2026

Security monitoring

Security monitoring activities

These guidelines are intended for security-relevant event logs. They are not intended for non-security-relevant event logs, such as operating system and application performance-related event logs.

Detecting cyber security events

One of the core elements of detecting cyber security events is the availability of appropriate data sources, such as event logs. The following types of event logs can be used by an organisation to assist in detecting cyber security events:

- **Artificial intelligence (AI) applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Cross Domain Solutions:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Databases:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Domain Name System services:** May assist in identifying attempts to resolve malicious domain names or Internet Protocol addresses indicating an exploitation attempt or successful compromise.
- **Email servers:** May assist in identifying users targeted with phishing emails, helping to identify the initial vector of a compromise.
- **Gateways:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Mobile applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Multifunction devices:** May assist in identifying anomalous or malicious user behaviour indicating a cyber security incident.

- **Operating systems:** May assist in identifying anomalous or malicious activity indicating an exploitation attempt or successful compromise.
- **Remote access services:** May assist in identifying unusual locations of access or times of access indicating an exploitation attempt or successful compromise.
- **Security products:** May assist in identifying anomalous or malicious code or network traffic indicating an exploitation attempt or successful compromise.
- **Server applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **System access:** May assist in identifying anomalous or malicious user behaviour indicating an exploitation attempt or successful compromise.
- **User applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Web applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Web proxies:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.

Security monitoring policy

By developing a security monitoring policy, taking into consideration any shared responsibilities between service providers and their customers, an organisation can improve their ability to detect malicious behaviour on their systems. In doing so, the security monitoring policy should cover the types of events to be logged, the event logging facilities to be used, how event logs will be monitored and how long event logs will be retained.

Control: ISM-0580; Revision: 8; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A security monitoring policy is developed, implemented and maintained.

Centralised event logging facility

A centralised event logging facility can be used to capture, protect and manage event logs from multiple sources in a coordinated manner. This may be achieved by using a Security Information and Event Management (SIEM) platform, a Security Orchestration, Automation and Response (SOAR) platform, or both. Furthermore, in support of a centralised event logging facility, it is important that an accurate and consistent time source is used to assist with identifying connections between events.

Control: ISM-1405; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A centralised event logging facility is implemented.

Control: ISM-1983; Revision: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs sent to a centralised event logging facility are sent as soon as possible after they occur.

Control: ISM-1984; Revision: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs sent to a centralised event logging facility are encrypted in transit using Australian Signals Directorate (ASD)-approved cryptography.

Control: ISM-1985; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are protected from unauthorised access.

Control: ISM-1815; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Event logs are protected from unauthorised modification and deletion.

Control: ISM-0988; Revision: 7; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An accurate and consistent time source is used for event logging.

Event log details

For each event logged, sufficient detail needs to be captured for event logs to be useful. In doing so, event logs should be captured and stored in a consistent and structured format.

Control: ISM-0585; Revision: 7; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
For each event logged, the date and time of the event, the relevant user or process, the relevant filename, the event description, and the information technology equipment involved are captured.

Control: ISM-1959; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
To the extent possible, event logs are captured and stored in a consistent and structured format.

Event log monitoring

Event log monitoring is critical to maintaining the security posture of systems. It involves the timely analysis of event logs to detect cyber security events and identify potential cyber security incidents. In doing so, successful detection of cyber security events, and identification of cyber security incidents, requires trained cyber security personnel with access to sufficient tools that support manual and automated analysis of system behaviour.

Control: ISM-0120; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cyber security personnel have access to sufficient tools to facilitate the detection of cyber security events and the identification of cyber security incidents.

Control: ISM-2116; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cyber threat intelligence services are used to support the detection of cyber security events and the identification of cyber security incidents.

Control: ISM-2117; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Suitable AI models are used to augment the detection of cyber security events and the identification of cyber security incidents.

Control: ISM-1986; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from critical servers are analysed in a timely manner to detect cyber security events.

Control: ISM-1906; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

Control: ISM-1907; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.

Control: ISM-0109; Revision: 9; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Event logs from workstations are analysed in a timely manner to detect cyber security events.

Control: ISM-1987; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from security products are analysed in a timely manner to detect cyber security events.

Control: ISM-1960; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from internet-facing network devices are analysed in a timely manner to detect cyber security events.

Control: ISM-1961; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from non-internet-facing network devices are analysed in a timely manner to detect cyber security events.

Control: ISM-1228; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cyber security events are analysed in a timely manner to identify cyber security incidents.

Event log retention

The retention of event logs is integral to security monitoring, threat hunting and cyber security incident response activities. As such, event logs should be retained for a suitable period to facilitate these activities.

Control: ISM-1988; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are retained in a searchable manner for at least 12 months.

Control: ISM-1989; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are retained as per minimum retention requirements for various classes of records as set out by the National Archives of Australia's Administrative Functions Disposal Authority Express (AFDA Express) Version 2 publication.

Further information

Further information on logging intrusion activity can be found in the 'Managing cyber security incidents' section of the *Guidelines for cyber security incidents*.

Further information on event logging for application-based security products can be found in the 'Operating system hardening' section of the *Guidelines for system hardening*.

Further information on event logging for AI applications can be found in the 'Software development fundamentals' section of the *Guidelines for software development*.

Further information on event logging for Cross Domain Solutions can be found in the 'Cross Domain Solutions' section of the *Guidelines for gateways*.

Further information on event logging for databases can be found in the 'Databases' section of the *Guidelines for database systems*.

Further information on event logging for gateways can be found in the 'Gateways' section of the *Guidelines for gateways*.

Further information on event logging for mobile applications can be found in the 'Software development fundamentals' section of the *Guidelines for software development*.

Further information on event logging for multifunction devices can be found in the 'Multifunction devices' section of the *Guidelines for communications systems*.

Further information on event logging for network-based security products can be found in the 'Network design and configuration' section of the *Guidelines for networking*.

Further information on event logging for operating systems can be found in the 'Operating system hardening' and 'Authentication hardening' sections of the *Guidelines for system hardening*.

Further information on event logging for server applications can be found in the 'Server application hardening' section of the *Guidelines for system hardening*.

Further information on event logging for system access can be found in the 'Access to systems and their resources' section of the *Guidelines for personnel security*.

Further information on event logging for user applications can be found in the 'User application hardening' section of the *Guidelines for system hardening*.

Further information on event logging for web applications can be found in the 'Software development' section of the *Guidelines for software development*.

Further information on event logging for web proxies can be found in the 'Web proxies' section of the *Guidelines for gateways*.

Further information on event logging can be found in the following ASD publications:

- *Best practices for event logging and threat detection*
- *Detecting and mitigating Active Directory compromises*
- *Hardening Microsoft Windows 10 workstations*
- *Hardening Microsoft Windows 11 workstations*
- *Priority logs for SIEM ingestion: Practitioner guidance*
- *Windows event logging and forwarding*.

Further information on ASD's cyber threat intelligence service, that is available to ASD Cyber Security Network Partners, can be found on ASD's Cyber Threat Intelligence Sharing service webpage.

Further information on using AI models for security monitoring activities can be found in ASD's *Opportunities for AI in cyber defence* publication.

Further information on SIEM and SOAR platforms can be found in ASD's *Implementing SIEM and SOAR platforms: Executive guidance* and *Implementing SIEM and SOAR platforms: Practitioner guidance* publications.

Further information on prioritising the collection and storage of event logs can be found in the United States' Cybersecurity & Infrastructure Security Agency's *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities* publication.

Further information on the National Archives of Australia's requirements for event log retention can be found in their *AFDA Express Version 2 – Technology & Information Management* publication.

Security assessments

Vulnerability scanning

To ensure that patches or updates are being applied to applications, operating systems, drivers and firmware, it is essential that an organisation regularly identify all assets within their environment using an

automated method of asset discovery, such as an asset discovery tool or a vulnerability scanner with equivalent functionality. Following asset discovery, identified assets can be scanned for missing patches or updates using a vulnerability scanner with an up-to-date vulnerability database. Ideally, vulnerability scanning should be conducted in an automated manner and take place at twice the frequency at which patches or updates need to be applied. For example, if patches or updates are to be applied within two weeks of release then vulnerability scanning should be undertaken at least weekly.

Control: ISM-1807; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

Control: ISM-1808; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

Control: ISM-1698; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.

Control: ISM-1699; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products.

Control: ISM-1700; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products.

Control: ISM-1701; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.

Control: ISM-1702; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.

Control: ISM-1752; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices.

Control: ISM-1703; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.

Control: ISM-1900; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.

Control: ISM-1921; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The likelihood of system compromise is frequently assessed when working exploits exist for unmitigated vulnerabilities.

Vulnerability assessments and penetration tests

Measures to monitor and manage vulnerabilities in systems can provide an organisation 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. Regardless of the security assessment activity performed, they should be conducted by suitably skilled personnel augmented by AI models. In doing so, personnel can be internal to an organisation or from a third party, however, such personnel should be independent of the system being assessed. This ensures that there is no conflict of interest, perceived or otherwise, and that the activities are undertaken in an objective manner.

Control: ISM-2118; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vulnerability assessments and penetration tests are conducted for systems prior to their deployment, including prior to the deployment of significant changes, and at least annually thereafter.

Control: ISM-2119; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Suitable AI models are used to augment vulnerability assessments and penetration tests.

Further information

Further information on responsibilities for security assessment activities as part of continuously monitoring the security of systems can be found in the 'System owners' section of the *Guidelines for cyber security roles*.

Further information on using AI models for security assessment activities can be found in ASD's *Opportunities for AI in cyber defence* publication.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre