Information Security Manual

Published: 22 June 2023

Guidelines for System Management

System administration

System administration of cloud services

System administration of cloud services brings unique challenges when compared to system administration of on-premises assets. Notably, responsibility for system administration of cloud services is often shared between service providers and their customers. As the system administration processes and procedures implemented by service providers are often opaque to their customers, customers should consider a service provider's control plane to operate within a different security domain.

System administration processes and procedures

A key component of system administration is ensuring that administrative activities are undertaken in a repeatable and accountable manner using system administration processes and procedures. In doing so, requirements for administrative activities may cover:

- configuring applications, operating systems, network devices or other ICT equipment

- applying patches, updates or vendor mitigations to applications, drivers, operating systems or firmware

- installing or removing applications, operating systems, network devices or other ICT equipment

- implementing system changes or enhancements

- resolving problems identified by users.

Furthermore, in support of change management processes and procedures, system administrators should document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation.

Control: ISM-0042; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: N/A
System administration processes, and supporting system administration procedures, are developed, implemented and maintained.

Control: ISM-1211; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
System administrators document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation.

Separate privileged operating environments

One of the greatest threats to the security of networks is the compromise of privileged accounts. Providing a separate privileged operating environment for system administrators, in addition to their unprivileged operating environment, makes it much harder for administrative activities and privileged accounts to be compromised by an adversary.

Using different physical workstations is the most secure approach to separating privileged and unprivileged operating environments for system administrators. However, a virtualisation-based solution may be sufficient for separating privileged and unprivileged operating environments. In such cases, privileged operating environments should not be virtualised within unprivileged operating environments.

Control: ISM-1380; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged users use separate privileged and unprivileged operating environments.

Control: ISM-1687; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged operating environments are not virtualised within unprivileged operating environments.

Control: ISM-1688; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Unprivileged accounts cannot logon to privileged operating environments.

Control: ISM-1689; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

Administrative infrastructure

The security of administrative activities can be improved by segregating administrative infrastructure from the wider network and the internet. In doing so, the use of a jump server (also known as a jump host or jump box) can be an effective way of simplifying and securing administrative activities. Specifically, a jump server can provide filtering of network management traffic while also acting as a focal point to perform multi-factor authentication; store and manage administrative tools; and perform logging, monitoring and alerting activities. Finally, using separate jump servers for the administration of critical servers, high-value servers and regular servers can further assist in protecting these assets.

Control: ISM-1385; Revision: 4; Updated: Jun-23; Applicability: All; Essential Eight: N/A
Administrative infrastructure is segregated from the wider network and the internet.

Control: ISM-1750; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.

Control: ISM-1386; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Network management traffic can only originate from administrative infrastructure.

Control: ISM-1387; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Administrative activities are conducted through jump servers.

Control: ISM-1381; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Only privileged operating environments can communicate with jump servers.

Control: ISM-1388; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Only jump servers can communicate with assets requiring administrative activities to be performed.

Further information

Further information on system administration can be found in the Australian Cyber Security Centre (ACSC)'s *Secure Administration* publication.

Further information on the use of privileged accounts for system administration activities can be found in the access to systems and their resources section of the *Guidelines for Personnel Security*.

Further information on multi-factor authentication can be found in the authentication hardening section of the *Guidelines for System Hardening*.

Further information on event logging can be found in the event logging and monitoring section of the *Guidelines for System Monitoring*.

Further information on network segmentation and segregation can be found in the network design and configuration section of the *Guidelines for Networking*.

System patching

Patch management processes and procedures

Applying patches or updates is critical to ensuring the ongoing security of applications, drivers, operating systems and firmware. In doing so, it is important that patches or updates are applied consistently and in a secure manner. For example, by using a centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully.

Control: ISM-1143; Revision: 9; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.

Control: ISM-0298; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.

Software register

To assist with monitoring information sources for details of relevant patches or updates, an organisation should develop, implement, maintain and regularly verify software registers for workstations, servers, network devices and other ICT equipment.

Control: ISM-1493; Revision: 4; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Software registers for workstations, servers, network devices and other ICT equipment are developed, implemented, maintained and verified on a regular basis.

Control: ISM-1643; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.

Scanning for missing patches or updates

To ensure that patches or updates are being applied to applications, operating systems, drivers and firmware, it is essential that an organisation regularly identifies 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 half the frequency in 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; Applicability: All; Essential Eight: 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; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

Control: ISM-1698; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

Control: ISM-1699; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Control: ISM-1700; Revision: 1; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Control: ISM-1701; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.

Control: ISM-1702; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.

Control: ISM-1752; Revision: 1; Updated: Jun-23; Applicability: All; Essential Eight: N/A
A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices.

Control: ISM-1703; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: N/A
A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in drivers and firmware.

When to patch security vulnerabilities

When patches or updates are released by vendors for security vulnerabilities, an organisation should apply them in a timeframe commensurate with the likelihood of attempted exploitation by an adversary. For example, by prioritising patches or updates for security vulnerabilities in internet-facing services and their operating systems, especially when exploitation code exists or active exploitation is occurring.

If no patches or updates are available for security vulnerabilities, mitigation advice from vendors, trusted authorities or security researchers may provide some protection until patches or updates are made available. Such mitigation advice may be published in conjunction with, or soon after, announcements made relating to security vulnerabilities. Mitigation advice may cover how to disable or block access to vulnerable functionality, how to reconfigure vulnerable functionality, or how to detect attempted or successful exploitation of vulnerable functionality.

If a patch or update is released for high assurance ICT equipment, the ACSC will conduct an assessment of the patch or update. Subsequently, if the patch or update is approved for deployment, the ACSC will provide guidance on the methods and timeframes in which it is to be applied.

Control: ISM-1690; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
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.

Control: ISM-1691; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
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.

Control: ISM-1692; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
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.

Control: ISM-1693; Revision: 1; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.

Control: ISM-1694; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

Control: ISM-1695; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.

Control: ISM-1696; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists.

Control: ISM-1751; Revision: 1; Updated: Jun-23; Applicability: All; Essential Eight: N/A
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists.

Control: ISM-1697; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Patches, updates or vendor mitigations for security vulnerabilities in drivers and firmware are applied within two weeks of release, or within 48 hours if an exploit exists.

Control: ISM-0300; Revision: 8; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Patches, updates or vendor mitigations for security vulnerabilities in high assurance ICT equipment are applied only when approved by the ACSC, and in doing so, using methods and timeframes prescribed by the ACSC.

Cessation of support

When applications, operating systems, network devices and other ICT equipment reach their cessation date for support, an organisation will find it increasingly difficult to protect them against security vulnerabilities as patches, updates and other forms of support will no longer be made available by vendors. As such, unsupported applications, operating systems, network devices and other ICT equipment should be removed or replaced.

In planning for cessation of support, it is important to note that while vendors generally advise the cessation date for support of operating systems well in advance, some applications, network devices and other ICT equipment may cease to receive support immediately after newer versions are released.

Finally, when the immediate removal or replacement of unsupported applications, operating systems, network devices or other ICT equipment is not possible, compensating controls should be implemented until such time that they can be removed or replaced.

Control: ISM-1704; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

Control: ISM-0304; Revision: 6; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Applications that are no longer supported by vendors are removed.

Control: ISM-1501; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Operating systems that are no longer supported by vendors are replaced.

Control: ISM-1753; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Network devices and other ICT equipment that are no longer supported by vendors are replaced.

Further information

Further information on system patching can be found in the ACSC's *Assessing Security Vulnerabilities and Applying Patches* publication.

Further information on patching evaluated products can be found in the evaluated product usage section of the *Guidelines for Evaluated Products*.

Further information on cessation of support for Microsoft Windows operating systems, including potential compensating controls for use beyond their cessation date for support, can be found in the ACSC's *End of Support for Microsoft Windows and Microsoft Windows Server* publication.

Further information on hardening user applications can be found in the user application hardening section of the *Guidelines for System Hardening*.

Further information on hardening server applications can be found in the server application hardening section of the *Guidelines for System Hardening*.

Data backup and restoration

Digital preservation policy

Developing, implementing and maintaining a digital preservation policy, as part of digital continuity planning, can assist in ensuring the long term integrity and availability of important data is maintained, especially when taking into account the potential for data degradation and removable media, hardware and software obsolesce.

Control: ISM-1510; Revision: 2; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A digital preservation policy is developed, implemented and maintained.

Data backup and restoration processes and procedures

Having data backup and restoration processes and procedures is an important part of business continuity and disaster recovery planning. Such activities will also form an integral part of an overarching digital preservation policy.

Control: ISM-1547; Revision: 2; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Data backup processes, and supporting data backup procedures, are developed, implemented and maintained.

Control: ISM-1548; Revision: 2; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.

Performing and retaining backups

To mitigate the security risk of losing system availability or important data as part of a ransomware attack, or other form of destructive attack, backups of important data, software and configuration settings should be performed and retained with a frequency and retention timeframe in accordance with an organisation's business continuity requirements. In doing so, backups of all important data, software and configuration settings should be synchronised to enable restoration to a common point in time. Furthermore, it is essential that all backups are retained in a secure and resilient manner. This will ensure that should a system fall victim to a ransomware attack, or other form of destructive attack, important data will not be lost and, if necessary, systems can be quickly restored.

Control: ISM-1511; Revision: 3; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3

Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.

Control: ISM-1810; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.

Control: ISM-1811; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Backups of important data, software and configuration settings are retained in a secure and resilient manner.

Backup access

To mitigate the security risk of unauthorised access to backups, an organisation should ensure that access to backups is controlled through the use of appropriate access controls.

Control: ISM-1812; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Unprivileged accounts cannot access backups belonging to other accounts.

Control: ISM-1813; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML3
Unprivileged accounts cannot access their own backups.

Control: ISM-1705; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.

Control: ISM-1706; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3
Privileged accounts (excluding backup administrator accounts) cannot access their own backups.

Backup modification and deletion

To mitigate the security risk of backups being accidentally or maliciously modified or deleted, an organisation should ensure that backups are sufficiently protected from unauthorised modification and deletion through the use of appropriate access controls during their retention period.

Control: ISM-1814; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Unprivileged accounts are prevented from modifying and deleting backups.

Control: ISM-1707; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

Control: ISM-1708; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3
Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.

Testing restoration of backups

To ensure that backups can be restored when the need arises, and that any dependencies can be identified and managed beforehand, it is important that the restoration of important data, software and configuration settings from backups to a common point in time is tested in a coordinated manner as part of disaster recovery exercises.

Control: ISM-1515; Revision: 3; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3
Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises.

Further information

Further information on digital preservation planning and data retention is available from the National Archives of Australia.

Further information on the collection and retention of personal information can be found in the Office of the Australian Information Commissioner's *Australian Privacy Principles* and the associated *Australian Privacy Principles guidelines*.

Further information on business continuity and disaster recovery planning can be found in the Chief Information Security Officer section of the *Guidelines for Cyber Security Roles*.