Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for System Management

System administration

What is secure system administration

Secure system administration allows organisations to be resilient in the face of targeted cyber intrusions by protecting administrator workstations and accounts from compromise, as well as making adversary movement throughout a network more difficult. If a secure system administration environment withstands a targeted cyber intrusion, incident response will be far more agile, the damage will be limited and remediation work will be completed faster.

Secure system administration of cloud services

Secure system administration of cloud services brings unique challenges when compared to the secure administration of on-premise assets. Notably, responsibility for system administration of cloud services is often shared between service providers and organisations. As the technology stack and secure administration processes implemented by service providers are often opaque to organisations, organisations should consider a service provider's control plane to operate within a different security domain. As such, the security controls below may require adjustment.

Administrative accounts

The use of the same credentials on both an administrator workstation and a user workstation puts the administrator workstation at risk of compromise if the user workstation is compromised. The table below provides clarification on the use of different accounts.

Regular User Account	Unprivileged Administration Account	Privileged Administration Account
Unprivileged account	Unprivileged account	Privileged account
Used for web and email access Used for day-to-day non-administrative tasks	Used for authentication to dedicated administrator workstation Used for authentication to jump server(s)	Used for performance of administration tasks

Different username and passphrase to regular user account	Different username and passphrase to regular user account

System administration process and procedures

A key component of secure system administration is ensuring that privileged actions are performed using an approved system administration process supported by system administration procedures. This will ensure that privileged actions are undertaken in a repeatable and accountable manner.

Security Control: 0042; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
A system administration process, with supporting system administration procedures, is developed and implemented.

Separate administrator workstations

One of the greatest threats to the security of a network as a whole is the compromise of a workstation used for administration activities. Providing a physically separate hardened administrator workstation to privileged users, in addition to their workstation used for unprivileged user access, provides greater assurance that privileged activities and credentials will not be compromised.

Using different physical machines is considered the most secure solution to separate workstations; however, a risk-based approach may determine that a virtualisation-based solution is sufficient. In such cases, the unprivileged user environment should be the 'guest' and the administrative environment should be the 'host'.

Security Control: 1380; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Privileged users use a dedicated administrator workstation when performing privileged tasks.

Security Control: 1382; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Privileged users are assigned an unprivileged administration account for authenticating to their dedicated administrator workstations.

Security Control: 1381; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Dedicated administrator workstations used for privileged tasks are prevented from communicating to assets not related to administrative activities.

Security Control: 1383; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All administrative infrastructure including, but not limited to, administrator workstations and jump servers are hardened.

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.

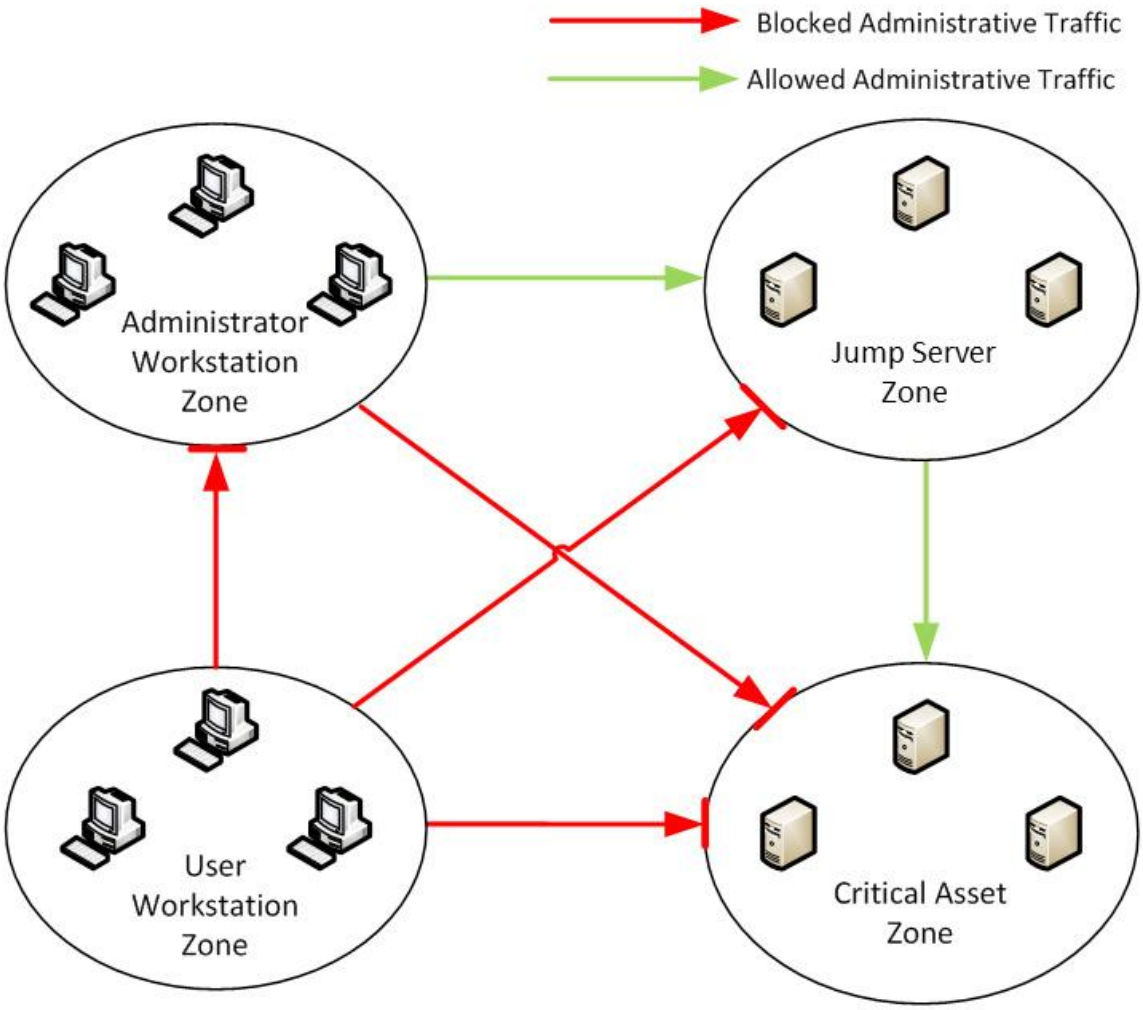
Security Control: 1385; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Administrator workstations are placed into a separate network zone to user workstations.

Restriction of management traffic flows

Limiting the flow of management traffic to only those network elements and segments 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.

Although user workstations will have a need to communicate with critical assets such as web servers or domain controllers in order to function, it is highly unlikely that they will need to send or receive management traffic (such as Remote Desktop Protocol [RDP], Secure Shell [SSH] and similar protocols) to these assets.

The following diagram outlines how management traffic filtering could be implemented between a network comprising different network zones. The only flows of management traffic allowed are those between the 'Administrator Workstation Zone' and the 'Jump Server Zone' as well as the 'Jump Server Zone' and the 'Critical Asset Zone'. All other traffic is blocked as there is no reason for management traffic to flow between the other network zones.



Security Control: 1386; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Management traffic is only allowed to originate from network zones that are used to administer systems and applications.

Jump servers

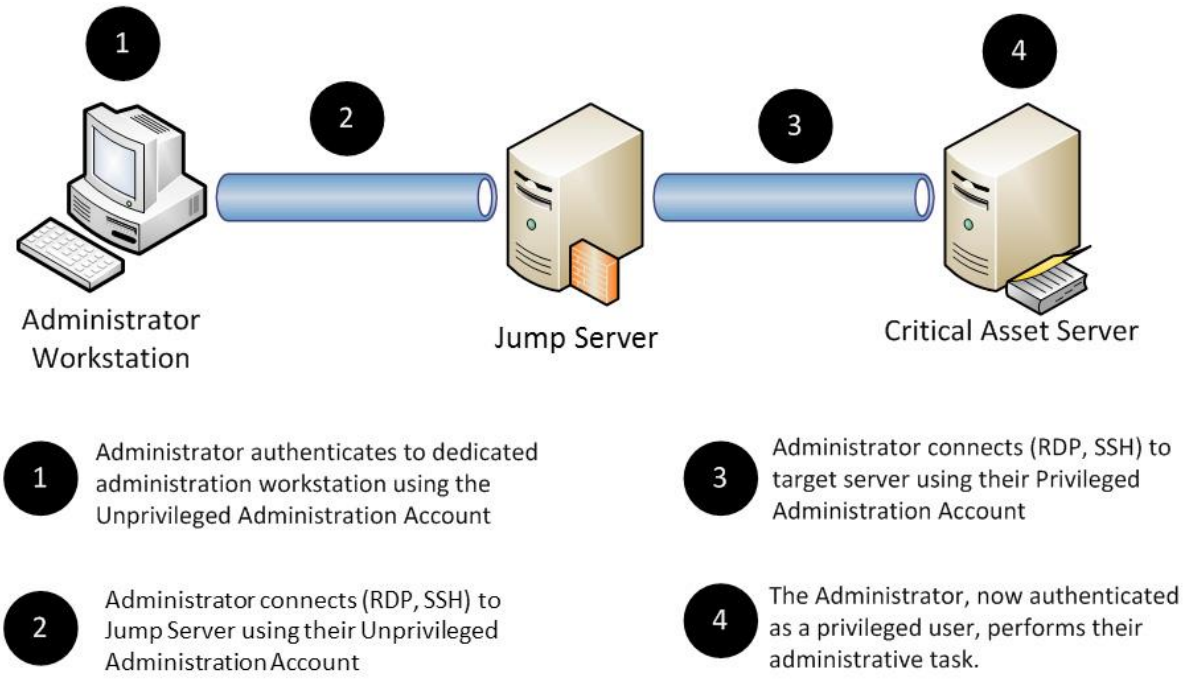
A jump server (also known as a jump host or jump box) is used to manage important or critical resources in a separate security domain. The use of jump servers as a form of 'management proxy' can be an effective way of simplifying and securing privileged activities. Implementing a jump server can yield the following benefits:

- an efficient and effective focal point to perform multi-factor authentication

- a single place to store and patch management tools
- simplified implementation of management traffic filtering
- a focal point for logging, monitoring and alerting.

In a typical scenario, if a privileged user wanted to perform administrative activities they would connect directly to the target server using RDP or SSH. However, in a jump server setup the privileged user would first connect and authenticate to the jump server, then RDP, SSH, or use remote administration tools to access the target server.

When implementing a jump server, it is recommended that organisations implement multi-factor authentication, enforce strict device communication restrictions, and harden administrative infrastructure, otherwise a jump server will yield little security benefit.



Security Control: 1387; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All administrative actions are conducted through a jump server.

Security Control: 1388; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Jump servers are prevented from communicating to assets and sending and receiving traffic not related to administrative activities.

Further information

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

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

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

Further information on secure system administration can be found in the Australian Cyber Security Centre (ACSC)'s ***Secure Administration*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/secure-administration.

Further information on mitigating the use of stolen credentials can be found in the ACSC's ***Mitigating the Use of Stolen Credentials*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/mitigating-the-use-of-stolen-credentials.

Further information can also be found in Microsoft's ***Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, Version 1 and 2*** publication at https://www.microsoft.com/en-au/download/confirmation.aspx?id=36036.

System patching

Patching approaches

Patches for security vulnerabilities are provided by vendors in many forms, such as:

- fixes that can be applied to pre-existing application versions
- fixes incorporated into new applications or drivers that require pre-existing versions to be replaced
- fixes that require the overwriting of firmware on ICT equipment.

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 sanitisation
- 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.

Patch management process and procedures

Applying patches or updates is critical to ensuring the security of applications, drivers, operating systems and firmware in workstations, servers, mobile devices, network devices and all other ICT equipment. To assist in this, suitable sources of information should be monitored for information about new patches or updates.

Security Control: 1143; Revision: 7; Updated: Aug-19; Applicability: O, P, S, TS
A patch management process, and supporting patch management procedures, is developed and implemented.

Security Control: 1493; Revision: 2; Updated: Jun-21; Applicability: O, P, S, TS
Software registers are maintained and regularly audited for workstations, servers, mobile devices, network devices and all other ICT equipment.

Security Control: 1643; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.

When to patch security vulnerabilities

There are multiple sources of information that organisations can use to assess the applicability and impact of security vulnerabilities in the context of their environment. This can include information published in vendor security bulletins or in severity ratings assigned to security vulnerabilities using standards such as the Common Vulnerability Scoring System.

Once a patch is released by a vendor, and the associated security vulnerability has been assessed for its applicability and importance, the patch should be deployed in a timeframe that is commensurate with the security risk. Doing so ensures that resources are spent in an effective and efficient manner by focusing effort on the most significant security risks first.

If a patch is released for high assurance ICT equipment, the ACSC will conduct an assessment of the patch and may revise the ICT equipment's usage guidance. If a patch for high assurance ICT equipment is approved for deployment, the ACSC will inform organisations of the timeframe in which the patch is to be deployed.

If no patches are immediately available for security vulnerabilities, temporary workarounds may provide the only effective protection until patches become available. These workarounds may be published in conjunction with, or soon after, security vulnerability announcements. Temporary workarounds may include disabling the vulnerable functionality within the operating system, application or device, or restricting or blocking access to the vulnerable service using firewalls or other access controls. The decision as to whether a temporary workaround is implemented should be risk-based, as with patching.

Security Control: 1144; Revision: 9; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

Security Control: 0940; Revision: 8; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 1472; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 1494; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

Security Control: 1495; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 1496; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 0300; Revision: 6; Updated: Sep-18; Applicability: S, TS
High assurance ICT equipment is only patched with patches approved by the ACSC using methods and timeframes prescribed by the ACSC.

How to patch security vulnerabilities

To ensure that patches are applied consistently across an organisation's workstation and server fleet, it is essential that organisations use a centralised and managed approach. This will assist in ensuring the integrity and authenticity of patches being applied to workstations and servers.

Security Control: 0298; Revision: 7; Updated: Oct-19; Applicability: O, P, S, TS
A centralised and managed approach is used to patch or update applications and drivers.

Security Control: 0303; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
An approach for patching or updating applications and drivers that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

Security Control: 1497; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.

Security Control: 1498; Revision: 1; Updated: Oct-19; Applicability: O, P, S, TS
A centralised and managed approach is used to patch or update operating systems and firmware.

Security Control: 1499; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An approach for patching or updating operating systems and firmware that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

Security Control: 1500; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.

Cessation of support

When applications, operating systems and ICT equipment reach their cessation date for support, organisations will find it increasingly difficult to protect against security vulnerabilities as patches, or other forms of support, will not be made available by vendors. While the cessation date for support for operating systems is generally advised many years in advance by vendors, other applications and ICT equipment may cease to receive support immediately after a newer version is released by a vendor.

Security Control: 0304; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Security Control: 1501; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Further information

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

Further information on what constitutes different levels of security risk for security vulnerabilities can be found in the ACSC's ***Assessing Security Vulnerabilities and Applying Patches*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches.

Further information on patching during change freezes can be found in the ACSC's ***Patching During Change Freezes*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/patching-during-change-freezes.

Change management

Identifying the need for change

The need for change can be identified in various ways, including:

- identification of security vulnerabilities or cyber threats
- users identifying problems or a need for system enhancements
- upgrades or patches for software or ICT equipment
- vendors notifying the end of life for software or ICT equipment
- the implementation of new software or ICT equipment
- organisational or business process changes
- other continuous improvement activities.

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: 1211; Revision: 3; Updated: Jul-20; Applicability: O, P, S, TS
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.*

Data backup and restoration

Digital preservation policy

Developing and implementing 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 media, hardware and software obsolesce.

Security Control: 1510; Revision: 1; Updated: Aug-19; Applicability: O, P, S, TS
A digital preservation policy is developed and implemented.

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.

Security Control: 1547; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
A data backup process, and supporting data backup procedures, is developed and implemented.

Security Control: 1548; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
A data restoration process, and supporting data restoration procedures, is developed and implemented.

Performing backups

When performing backups, all important data, software and configuration settings for software, network devices and other ICT equipment should be captured on a daily basis. This will ensure that should a system fall victim to a ransomware attack, important data will not be lost and that business operations will have reduced downtime.

Security Control: 1511; Revision: 1; Updated: Jun-21; Applicability: O, P, S, TS
Backups of important data, software and configuration settings are performed at least daily.

Backup storage

To mitigate the likelihood of data becoming unavailable due to accidental or malicious deletion of backups, organisations should ensure that backups are protected from unauthorised modification, corruption and deletion. This can be achieved by storing backups offline, ideally at multiple geographically-dispersed locations, or online but in a non-rewritable and non-erasable manner, such as through the use of write once, read many technologies.

Security Control: 1512; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored offline, or online but in a non-rewritable and non-erasable manner.

Security Control: 1513; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored at a multiple geographically-dispersed locations.

Retention periods for backups

To prevent backups from being retained for an insufficient amount of time to allow for the recovery of data, organisations are strongly encouraged to store backups for three months or greater.

Security Control: 1514; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored for three months or greater.

Testing restoration of backups

To ensure that backups can be restored when the need arises, and that any dependencies can be identified and managed, it is important that full restoration of backups has been tested at least once following the implementation of

backup technologies and processes. Furthermore, full restoration of backups should be tested each time fundamental information technology changes occur, such as when deploying new backup technologies. In the intervening time, it is important that regular testing in the form of partial restoration of backups is undertaken.

Security Control: 1515; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS
Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Security Control: 1516; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS
Partial restoration of backups is tested on a quarterly or more frequent basis.

Further information

Further information on business continuity can be found in the service continuity for online services section of the ***Guidelines for Networking***.

Further information on preserving digital information can be found on the National Archives of Australia's website at: https://www.naa.gov.au/information-management/store-and-preserve-information/preserving-information/preserving-digital-information/digital-preservation-planning.