Hybrid system security plan

2022-07-26

Introduction

System name

HybridSystem.

System overview

The HybridSystem leverages the Information Security Registered Assessors Program (IRAP) assessed Microsoft Azure, Office 365 platforms and their associated services. As well as leveraging an Agency's existing on-premises environment. The blueprint includes the following components to improve the security posture of a target Agency:

- Cloud identity – Synchronising identities from Active Directory (AD) to Azure Active Directory (Azure AD) for authentication. Azure AD configuration including Conditional Access policies allowing log in from anywhere and appropriate security policies to be applied.
- Office 365 – Configuration of Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, Microsoft Forms, Microsoft Whiteboard, and Microsoft Planner allowing cloud-based file storage and collaboration.
- Hybrid – Configuration between on-premises Exchange and Exchange Online, on-premises SharePoint and SharePoint Online to provide a seamless transition and extend cloud security capabilities.
- Device management – Management of security and configuration profiles for enrolled devices including the testing against security baselines and confirmation of security compliance.
- Applications – Delivery and configuration of applications appropriate to the user.
- Security stack – Security configuration of Office 365 and endpoint devices to maximise compliance and minimise risk.
- Autopilot deployment – Configuration of Autopilot to allow for automated deployment (and redeployment when required) of devices with no user interaction.
- Support – A flexible support model where system administration and Role-Based Access Control (RBAC) is provided regardless of whether the support is carried out by in house staff, third party contractors or a managed service provider.

System classification

The HybridSystem is designed to be able to achieve and maintain security accreditation up to PROTECTED.

System purpose and scope

The HybridSystem is intended to achieve a PROTECTED standard and raise Australian Government Agencies' cyber security posture. The HybridSystem details technology and configuration settings to deploy a hybrid Microsoft 365 solution for Agencies wanting to integrate with their existing on-premises environment.

Note: The Microsoft 365 suite includes multiple products including Windows 10, Office 365 and Enterprise Mobility + Security (EM+S).

System boundary

The system boundary is the subscription level of the Microsoft 365 implementation and the Agency's on-premises servers (Exchange, SharePoint, Configuration Manager and Active Directory) the HybridSystem leverages. The Azure AD tenant and all Microsoft 365 components (including both Azure and Office 365 hosted services), the transport of data between the endpoint devices and cloud services, along with the endpoint devices themselves, are included within the system. Network components are not considered to be part of the system.

As shown in the following figure, the system boundary includes:

- Microsoft 365 (including Azure and Office 365)
- Multi-Factor Authentication (MFA)
- Subscription and its management
- Azure AD tenant and its management
- On-premises and its management
- Endpoints including the hardware, firmware, and the management of the endpoints
- Transport of data between the endpoints and the cloud components

Note: This means that Transport Layer Security (TLS) would be included within the system boundary, but the network devices and mail gateway would not be included in the system boundary from a security perspective. Those items outside of the system boundary will be consumed and the existing security documentation will be utilised.

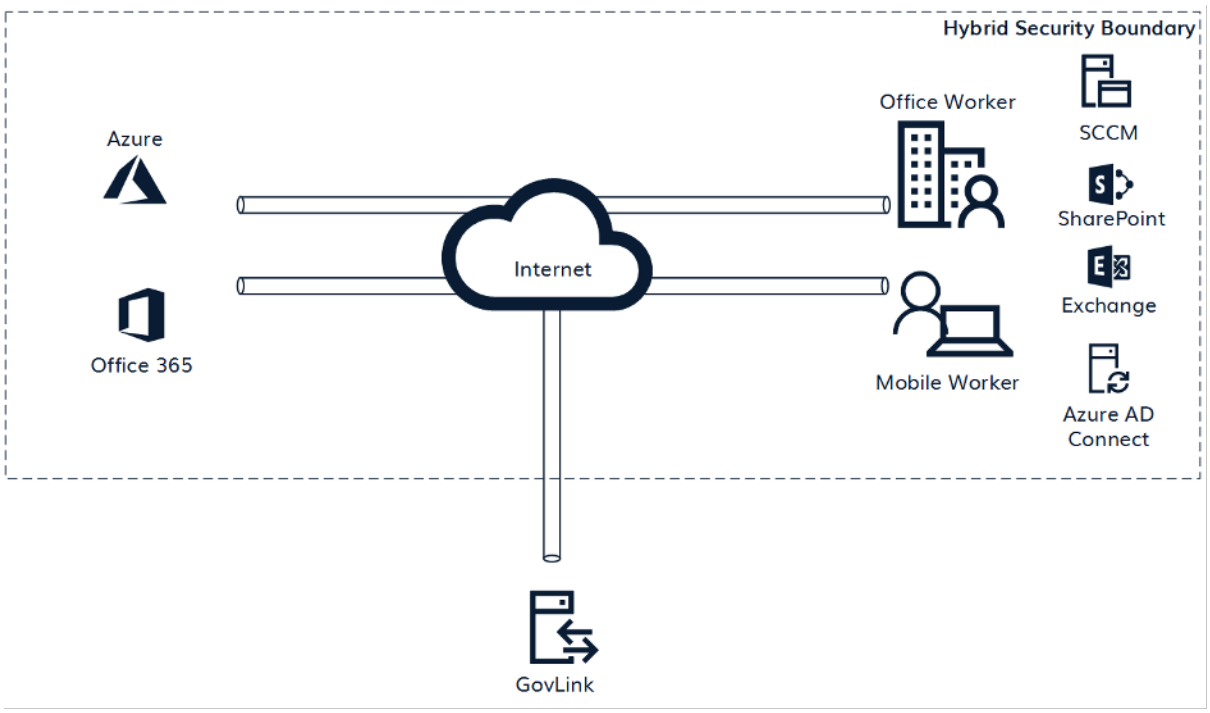

Figure 1: Hybrid Security Boundary

Document purpose and scope

The purpose of this System Security Plan (SSP) is to describe the security implementation of the HybridSystem, including the underlying Azure and Office 365 components that are leveraged in its deployment. This document is designed to comply with the Australian Government Information Security Manual (ISM) documentation requirements for system authorisation.

This document is deliberately written using descriptive and explanatory language to assist an Agency to understand how the HybridSystem operates securely, the security controls it provides, and the residual controls that must be addressed by an Agency.

For detailed information on how the HybridSystem addresses specific controls in the ISM (June 2022 update), refer to the 'DTA - Hybrid Blueprint - System Security Plan Annex (June 2022)'.

Overarching security policies

The security policies that the HybridSystem has been designed to comply with are listed below:

- The Australian Government ISM (June 2022) controls.
- The Australian Cyber Security Centre (ACSC) Strategies to Mitigate Cyber Security Incidents, including the Essential Eight Maturity Model.
- The ACSC Security Configuration Guide - Apple iOS 14 Devices (October 2021).
- The Protective Security Policy Framework (PSPF).
- Hardening Microsoft Windows 10 version 21H1 Workstation (October 2021).

Related security documentation

In accordance with the requirements of the ISM, the following security documentation has been developed for the HybridSystem:

- DTA – Blueprint – Solution Overview
- DTA – Blueprint – Client Devices Design
- DTA – Blueprint – Platform Design
- DTA – Blueprint – Office 365 Design
- DTA – Hybrid Blueprint – System Security Plan (this document)
- DTA – Hybrid Blueprint – System Security Plan Annex (June 2022)
- DTA – Hybrid Blueprint – Security Risk Management Plan
- DTA – Hybrid Blueprint – Standard Operating Procedures
- DTA – Hybrid Blueprint – Incident Response Plan

The IRAP reports for the assessment of Azure and Office 365 at PROTECTED have also been leveraged in the development of the HybridSystem, and includes the following:

- Azure Security Fundamentals and Cloud Services IRAP Assessment Report 2021
- Office 365 Security Fundamentals and Cloud Services IRAP Assessment Report 2021

These documents are available from the Microsoft Service Trust Portal.

Risk assessment

The results of the threat and risk assessment undertaken on the HybridSystem are documented in the 'DTA – Hybrid Blueprint – Security Risk Management Plan' (SRMP). This document describes the reduction in risk to the confidentiality, integrity and availability of system components and information processed and stored by the HybridSystem by the implementation of security controls and mitigations.

Assessment of services

This section provides details of the security assessment status of each Azure and Office 365 service used by the HybridSystem as listed in their respective IRAP reports. The assessment status of each of the utilised services and any associated mitigations is shown in Table 1.

Table 1 Assessment of Services

Category	Service	Assessment Status	Mitigation
General	Azure Portal	PROTECTED	N/A
Identity Services	Azure AD	PROTECTED	N/A

Category	Service	Assessment Status	Mitigation
Identity Services	Conditional Access	Not Assessed	Conditional Access is an Azure AD Premium P1 licenced feature of Azure AD (included in Microsoft 365 E3) that restricts access to cloud resources and management tools beyond just a successful authentication. It includes customisable policies based on location, user, device and more. Conditional Access is an additional security capability that is part of Azure AD, which is PROTECTED certified.
Identity Services	Azure MFA	PROTECTED	N/A
Identity Services	Azure AD Identity Protection	Not Assessed	Azure AD Identity Protection is an Azure AD Premium P2 licenced feature of Azure AD (included in Microsoft 365 E5) that allows organisations to accomplish three key tasks:* Automate the detection and remediation of identity-based risks.* Investigate risks using data in the portal.* Export risk detection data to third-party utilities for further analysis.
Office 365	Exchange Online, SharePoint Online, Microsoft Teams, Microsoft Forms, Microsoft Whiteboard, Microsoft Planner	PROTECTED	N/A
Monitoring and Compliance	Intune Policies	PROTECTED	Microsoft Endpoint Manager - Intune (Intune) is configured to allow policies to be created and deployed to devices that configure, check for compliance and assess against a security baseline. These policies are applied and reported against in the Intune web console.

Section definitions

The remaining sections of this document relate specifically to the chapters of the ISM. For each chapter of the ISM there is a corresponding section in this document, which is divided into four sections as detailed below in Table 2.

Table 2 Section Definitions

Section	Description
Applicability to HybridSystem	For each chapter, the applicability relates to whether the HybridSystem provides any technical, process or documentation that need to be assessed.The HybridSystem inherits many controls from the underlying Azure and Office 365 platforms, so if a chapter is listed as Not Applicable then the Agency may or may not be required to address the control. The reason the chapter is not applicable is stated in this section and if the Agency is required to address the controls then this is listed in the Residual controls to be addressed by the Agency section.
HybridSystem compliance approach	The compliance approach for the HybridSystem is described in this section to provide:* The background and context for how the HybridSystem addresses the controls in the chapter* To provide the Agency with information to assist in the assessment of the HybridSystem
Security controls provided by the HybridSystem	The specific technical implementation, process or documentation that the HybridSystem provides to address the controls are listed in this section.
Residual controls to be addressed by the Agency	If there are any residual controls that the Agency must address in relation to the operation of the HybridSystem, then they are listed in this section.

Summary of applicability

A summary of the applicability and responsibility for the controls presented in each chapter of the HybridSystem is listed below in Table 3. Each of these chapters are discussed in further details in this document, and the implementation status of each control is listed in the SSP Annex.

Table 3 Summary of Applicability

ISM Chapter	Applicability	Rationale
Guidelines for Cyber Security Roles	Not Applicable	Fulfilling these roles is an Agency responsibility.
Guidelines for Cyber Security Incidents	Not Applicable	The Agency is responsible for identifying, managing and reporting cyber security incidents.
Guidelines for Outsourcing	Applicable	Shared responsibility between the HybridSystem and the Agency consuming it.
Guidelines for Security Documentation	Applicable	The HybridSystem provides system-specific documentation to be read in conjunction with the Agency's cyber security strategy.

ISM Chapter	Applicability	Rationale
Guidelines for Physical Security	Not Applicable	The HybridSystem inherits the physical security controls which are implemented by Microsoft for Azure and Office 365 components.
Guidelines for Personnel Security	Applicable	The HybridSystem implements technical controls to assist the Agency with managing personnel security.
Guidelines for Communications Infrastructure	Not Applicable	The Agency is responsible for communications infrastructure leveraged by the HybridSystem.
Guidelines for Communications Systems	Applicable	The HybridSystem includes Microsoft Teams which provides video conferencing functionality.
Guidelines for Enterprise Mobility	Applicable	The HybridSystem includes the management and use of mobile devices.
Guidelines for Evaluated Products	Applicable	The HybridSystem includes Windows 10 which has been evaluated. Additionally, the HybridSystem leverages Office 365 services which include evaluated products.
Guidelines for ICT Equipment Management	Not Applicable	The security of the Azure and Office 365 hosting equipment is the responsibility of Microsoft.
Guidelines for Media	Applicable	The HybridSystem is responsible for encrypting removeable media.
Guidelines for System Hardening	Applicable	Hardening of operating systems and applications included in the HybridSystem is applicable.
Guidelines for System Management	Applicable	Management of HybridSystem system components is applicable.
Guidelines for System Monitoring	Applicable	Monitoring of HybridSystem system components is applicable.
Guidelines for Software Development	Not Applicable	The HybridSystem is not designed to support software development activities.
Guidelines for Database Systems	Not Applicable	The Agency is responsible for database systems leveraged by the HybridSystem.
Guidelines for Email	Applicable	The HybridSystem leverages Office 365 to provide email functionality.
Guidelines for Networking	Applicable	The HybridSystem is designed to run using the public internet and implements controls on the endpoint devices and the Office 365 component.
Guidelines for Cryptography	Applicable	The HybridSystem makes use of cryptography to protect both data at rest and data in transit.

ISM Chapter	Applicability	Rationale
Guidelines for Gateways	Applicable	The HybridSystem leverages Exchange Online Protection and Defender for Office 365 for email content filtering and Defender for Endpoint for web content filtering.
Guidelines for Data Transfers	Applicable	The HybridSystem is responsible for implementing technical controls relating to data transfer.

Cyber security roles

Chief Information Security Officer

Applicability to HybridSystem Not applicable as appointing a Chief Information Security Officer (CISO) is an Agency's responsibility.

HybridSystem compliance approach The HybridSystem is deployed into the Agency's environment and is under the scope of the Agency's CISO.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency must appoint a CISO to provide cyber security leadership and guidance.
- The Agency's CISO is responsible for all duties outlined in the Annex.

System owners

Applicability to HybridSystem Not applicable as the HybridSystem does not designate a system owner.

HybridSystem compliance approach The deployment of the HybridSystem into an Agency's environment can be designated as a specific system, or it can form part of a broader system.

By default, the HybridSystem is defined as a system and all documentation, including this SSP, is written in that context.

Security controls provided by the HybridSystem Not Applicable.

Residual controls to be addressed by the Agency

- The Agency must designate a System Owner for the HybridSystem.
- The System Owner must perform the relevant duties outlined in the Annex.

Cyber security incidents

Detecting cyber security incidents

Applicability to HybridSystem Not applicable to the HybridSystem as the detection of cyber security incidents is the responsibility of the Agency.

HybridSystem compliance approach The HybridSystem implements technical controls and processes to assist the Agency with detecting cyber security incidents related to the system.

Security controls provided by the HybridSystem The HybridSystem utilises Microsoft Defender for Endpoint and Defender for Office 365 to assist in the detection of cyber security incidents. These products are centralised into the Microsoft 365 Defender portal, which includes: * Incidents & alerts * Hunting (including advanced hunting and custom detection rules) * Action center * Threat analytics * Secure score

The HybridSystem also utilises Defender for Identity to assist in the detection of cyber security incidents relating to authentication. The Defender for Identity portal shows: * Suspicious activities * Health alerts

Defender for Identity alerts are also available via the Microsoft 365 Defender portal.

Residual controls to be addressed by the Agency The Agency must develop and implement an Intrusion Detection and Prevention Policy, which can leverage the security controls implemented by the HybridSystem and meets requirements outlined in the Annex.

Managing cyber security incidents

Applicability to HybridSystem Not applicable to the HybridSystem as the management of cyber security incidents is the responsibility of the Agency.

HybridSystem compliance approach The HybridSystem implements technical controls and processes to assist the Agency with managing cyber security incidents related to the system.

Security controls provided by the HybridSystem

- The HybridSystem utilises the Microsoft 365 Defender portal to assist in the management of cyber security incidents. Specific capabilities include the Incident queue and Incident management pane views.

Residual controls to be addressed by the Agency

- The Agency should establish a cyber security incident register, cyber security incident communication and response strategy and associated procedures that meet requirements outlined in the Annex.

Reporting cyber security incidents

Applicability to HybridSystem Not applicable to the HybridSystem as the reporting of cyber security incidents is the responsibility of the Agency.

HybridSystem compliance approach The reporting requirements for cyber security incidents are the Agency's responsibility.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency should establish a process and standard operating procedures for reporting cyber security incidents that meet requirements outlined in the Annex.

Outsourcing

Information technology and cloud services

Applicability to HybridSystem Outsourcing is applicable to the HybridSystem as it leverages both Azure and Office 365, which are cloud services.

HybridSystem compliance approach The HybridSystem leverages Microsoft Azure and Office 365, which have been IRAP assessed at PROTECTED by CyberCX. All HybridSystem services have been IRAP assessed.

Azure AD is defined as a non-regional service, but hosts identity data in Australian datacentres for customers that provide an Australian or New Zealand address . This includes Azure AD Directory Management and Authentication functions. Other Azure AD functions, including Azure MFA, store data in global datacentres.

Where possible the HybridSystem leverages services located in Australia, otherwise the United States is selected. Microsoft Defender for Cloud Apps is available in the United Kingdo,. Europe or United States regions. If the Azure AD tenant is in Australia, United States is automatically selected. Microsoft Defender for Endpoint is available in the Europe, United Kingdom, or in the United States. The United States is selected as part of the service creation for the HybridSystem. Defender for Identity is available in Europe, North America/Central America/Caribbean and Asia. The United States is automatically selected based on the geographical location of the Azure AD tenant.

Security controls provide by the HybridSystem

- Australian data locations have been selected where supported by Azure and Office 365 services leveraged by the HybridSystem.
- Microsoft provides a shared responsibility model which outlines how security responsibilities are shared between itself and the Agency.

Residual controls to be addressed by the Agency

- The Agency must assess, establish, manage and maintain the commercial and contractual relationship with Microsoft as the provider of the cloud services and review changes to the Microsoft IRAP assessments as they occur.

Shared responsibility When consuming a cloud service, management of some security controls is transferred from the Agency to the Cloud Service Provider (CSP), in this case Microsoft. The level of control transferred ultimately depends on the type of services being consumed i.e. cloud native or hybrid deployment and the agreement made with Microsoft.

Whilst responsibility for controls may be shared, Agencies must be conscious that security risk is not transferred to the service provider. It is therefore critical that Agencies understand how the sharing of responsibilities impacts system risk and what impact it may have on Assessing and Authorising the system within their environment.

In general, Microsoft defines themselves as being responsible for:

- Ensuring the physical systems and infrastructure required for the operation of a cloud service is secured appropriately.
- Accountable in the event of an incident relating to the physical systems and infrastructure they manage as required for the operation of a cloud service.
- Assess, managing and where possible mitigating risks inherent with the physical systems and infrastructure required for the operation of a cloud service.

In the context of Software as a Service (SaaS) Protected Utility platforms, Microsoft is responsible for:

- Incident response
- Backups
- Physical security
- System hardening
- Vulnerability and patch management
- Software development

When deploying a hybrid model, in the context of SaaS Protected Utility platforms, the Agency is responsible for:

- Access management
- System monitoring

- Non-Microsoft product vendors
- Client devices

Overall, the Agency is deemed accountable for any technology platform when in use with Microsoft or external product vendors responsible for parts of the platform operational management.

A suggested high-level shared responsibility matrix for the technology stack across the platform, Microsoft Office 365 and client devices has been tabled below. There are three defined stakeholders who share the responsibility to maintain the Agency's security capabilities.

- **Agency**: Australian government Agency adapting and implementing the DTA hybrid blueprint.
- **Microsoft**: CSP who provide and/or manage the defined technology platforms.
- **Product Vendor**: external product vendors (such as Apple for iOS) that provide or manage platforms within the Agency's ecosystem that are not performed by Microsoft.

Platform

CATEGORY	SYSTEM	INCIDENT RESPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
IDENTITY & ACCESS MANAGEMENT	AZURE ACTIVE DIRECTORY	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
IDENTITY & ACCESS MANAGEMENT	ON-PREM ACTIVE DIRECTORY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
SECURITY	MICROSOFT CLOUD APP SECURITY	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
SECURITY	AZURE ADVANCED THREAT PROTECTION	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
SECURITY	MICROSOFT DEFENDER ADVANCED THREAT PROTECTION	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT

CATEGORY	SYSTEM	INCIDENT RESPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
SECURITY	LOG ANALYTICS	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
SECURITY	SECURITY INFORMATION & EVENT MANAGEMENT	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY
CLIENT CONFIGURATION	MICROSOFT ENDPOINT MANAGER - INTUNE	AGENCY	AGENCY	MICROSOFT	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
CLIENT CONFIGURATION	MICROSOFT ENDPOINT CONFIGURATION MANAGER	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
CLIENT CONFIGURATION	PRINTING	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY
BACKUP & OPERATIONAL MANAGEMENT	BACKUP PLATFORM	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY
SYSTEM ADMINISTRATION	ADMINISTRATIVE CONSOLES	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT

CATEGORY	ITEM	INCIDENT RESPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
SYSTEM ADMINISTRATION	PRIVILEGED IDENTITY MANAGEMENT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT

Office 365

ITEM	INCIDENT RESPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
EXCHANGE ONLINE	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
SHAREPOINT ONLINE	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
ONEDRIVE FOR BUSINESS	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
MICROSOFT TEAMS	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
POWER BI	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
SECURITY & COMPLIANCE PLATFORMS	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
EXCHANGE ONLINE PROTECTION	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
OFFICE 365 ADVANCED THREAT PROTECTION	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
MICROSOFT FORMS	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
MICROSOFT WHITEBOARD	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT

ITEM	INCIDENT RESPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
MICROSOFT PLANNER	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT

Client devices

ITEM	INCIDENT RESPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
WINDOWS 10 – INTUNE MANAGED	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
WINDOWS 10 – MECM MANAGED	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
IOS – INTUNE MANAGED	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	APPLE

Security documentation

Development and maintenance of security documentation

Applicability to HybridSystem Development and maintenance of security documentation is applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem provides security documentation that an Agency can review, approve and incorporate into the broader Agency-level security documentation.

Security controls provided by the HybridSystem

- All security documentation produced by DTA for the HybridSystem has been updated within the last year and include the 'last updated' date.
- DTA provide updates to documentation via the Protected Utility website at desktop.gov.au. Release logs and change sets between versions can be obtained at GitHub.

Residual controls to be addressed by the Agency

- The Agency must develop a cyber security strategy.
- The Agency CISO or equivalent should approve all security documentation and ensure the documentation is reviewed annually.
- The Agency should communicate their security documentation to stakeholders of the HybridSystem and ensure stakeholders are notified of subsequent changes.

System-specific security documentation

Applicability to HybridSystem System-specific security documentation is applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem includes a suite of security and operational documentation that are logically connected and consistent.

The HybridSystem provides an SSP (this document), SSP Annex (formerly the Statement of Applicability (SoA)), SRMP, Incident Response Plan (IRP), Standard Operating Procedures (SOPs) and other operational documentation to assist in the understanding of the HybridSystem system and the security controls included.

Continuous Monitoring Plan (CMP) has also been developed for the blueprint to assist Agencies with the development of their own Agency-specific CMPs.

Security controls provided by the HybridSystem

- An SSP has been drafted for the HybridSystem (this document).
- A system-specific IRP has been drafted for the HybridSystem which integrates with the Agency-level IRP.
- The blueprint includes guidance to assist Agencies in developing a CMP.

Residual controls to be addressed by the Agency

- The Agency is responsible for developing an Agency-specific CMP.
- The Agency is responsible for developing a security assessment report including a plan of action post security assessment.

Physical security

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

Not applicable as the HybridSystem does not contain any physical hosting components, and the security of the Azure and Office 365 hosting equipment is the responsibility of Microsoft and is addressed in the respective IRAP reports for each service. For HybridSystem components hosted on-premises, such as the Azure AD Connect and Exchange servers, the Agency is responsible for their physical security controls.

HybridSystem compliance approach

The HybridSystem inherits physical security controls from the underlying Azure and Office 365 platforms, and from the Agency itself.

Security controls provided by the HybridSystem

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the physical security of all Agency-owned equipment, such as network devices and endpoint devices, that are utilised to connect to Azure and Office 365.
- The Agency is responsible for the physical security controls for all on-premises servers leveraged by the HybridSystem.

Personnel security

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

Technical controls relating to personnel security are applicable to the HybridSystem. An Agency's implementation of personnel security controls should include the HybridSystem.

HybridSystem compliance approach

The HybridSystem provides a role-based access control implementation and associated operations guide to enable an Agency to easily and securely control access, including privileged and emergency access, to Azure and Office 365 services. The HybridSystem leverages in-built authentication logging provided by the platform, and centralises logs to prevent unauthorised modification and deletion.

The controls provided by the HybridSystem are specific to Azure AD only and the Agency is responsible for implementing equivalent controls for Active Directory on-premises.

Security controls provided by the HybridSystem

- All unprivileged access attempts are logged in Azure AD Sign-ins. Azure AD logs are forwarded to a Log Analytics workspace for long-term secure retention.
- Intune configures an AppLocker blocklist to prevent administrators from launching web browsers and email clients.
- The HybridSystem leverages Azure AD Privileged Identity Management (PIM) to provide Just-in-time administration.
- Changes to privileged accounts and groups are logged in the Azure AD Audit Log.
- Azure AD logs are forwarded to a Log Analytics workspace for long-term secure retention.
- The HybridSystem includes automation to disable inactive Azure AD accounts after 45 days.
- Microsoft Defender for Cloud Apps policy monitoring is implemented to monitor activity of break glass accounts. The use of break glass accounts are also logged in Azure AD Sign-ins.

Residual controls to be addressed by the Agency

- The Agency is responsible for ensuring that personnel undergo pre-employment checks and hold the appropriate level of security clearance, as well as providing cyber security awareness training to staff and contractors.
- The Agency is responsible establishing processes for the creation, maintenance and decommissioning of accounts created within the system in accordance with the controls within the annex.
- The Agency is responsible for documenting and testing emergency access procedures.
- The Agency is responsible for monitoring and actioning cyber security events that are centralised to Log Analytics.

Communications infrastructure

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

Not applicable as the HybridSystem does not contain any communications infrastructure, and the security of the Azure and Office 365 hosting equipment is the responsibility of Microsoft and is addressed in the respective IRAP reports for Azure and Office 365.

HybridSystem compliance approach

The HybridSystem inherits communications infrastructure controls from the underlying Azure and Office 365 platforms.

Security controls provided by the HybridSystem

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the Agency-owned communication infrastructure utilised to connect to Azure and Office 365.

Communications systems

Telephone systems

Applicability to HybridSystem This section is not applicable as the HybridSystem does not include telephone systems.

HybridSystem compliance approach Not Applicable.

Security controls provided by the HybridSystem Not Applicable.

Residual controls to be addressed by the Agency Not applicable.

Video conferencing and IP telephony

Applicability to HybridSystem This section is applicable as the HybridSystem contains Microsoft Teams which provides video conferencing functionality.

HybridSystem compliance approach The HybridSystem inherits the security controls Microsoft have implemented for Microsoft Teams as assessed in the Office 365 IRAP report.

The Annex specifies the controls associated with the self-contained use of Microsoft Teams up to the level of PROTECTED. As per the Office 365 design, Agencies have the ability to connect Teams to the Telstra Calling for Office 365 service to allow calling between Teams and traditional telephones. Agencies wishing to use Telstra Calling for Office 365 or another similar services should undertake a security assessment to ensure that the product addresses their security requirements.

Security controls provided by the HybridSystem

- Microsoft Teams signalling data is encrypted.
- Secure signalling and data protocols are used by Microsoft Teams including Session Initiation Protocol (SIP) and Secure Real Time Protocol (SRTP).
- Microsoft Teams leverages Azure AD for authentication.
- Microsoft Teams has a dedicated Virtual Local Area Network (VLAN) within the Microsoft cloud.
- Microsoft Teams leverages Azure's Distributed Denial of Service (DDoS) protection capabilities.

Residual controls to be addressed by the Agency

- The Agency is responsible for all gateway configurations.

Fax machines and multifunction devices

Applicability to HybridSystem This section is not applicable as the HybridSystem does not include fax machines or multifunction devices.

HybridSystem compliance approach Not Applicable.

Security controls provided by the HybridSystem Not Applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the use and management of any fax machines and Multifunction Devices (MFDs) that are used with the HybridSystem.

Enterprise mobility

Mobile device management

Applicability to HybridSystem This section is applicable as the HybridSystem includes mobile devices.

HybridSystem compliance approach The HybridSystem leverages Microsoft Endpoint Manager - Intune (Intune) to provide both Mobile Device Management (MDM) and Mobile Application Management (MAM) controls to protect mobile devices and data stored on them. Both Windows laptops and iOS devices will be enrolled within Intune and tagged as Corporate devices, allowing policies to be centrally managed and deployed. This includes configuring storage encryption, disabling unneeded features and controlling application behaviour.

The HybridSystem does not include the use of privately-owned mobile devices. Only Agency-owned devices are enrolled and allowed to access data.

iOS devices are hardened in accordance with the ACSC 'Security Configuration Guide - Apple iOS 14 Devices' and Information Security Manual (ISM) with specific deviations to maximise usability for the target users as described below. Note: Agencies should do a risk assessment before deciding to change settings relating to mobile devices.

Bluetooth is enabled as it allows users to pair devices they may require to perform their duties (e.g. conference calls or online meetings).

Users can reset certain security settings in Personal Hotspot and Passcode for situations where the passcode/password may have been compromised.

The HybridSystem does not include the use of a full VPN on mobile devices, and therefore a direct connection to the internet is used. It is recommended Agencies consider implementing a VPN for mobile devices in accordance with the ACSC's recommendation for iOS devices. The blueprint includes suggested per app VPN configuration, however the selection and configuration of a VPN server is the responsibility of the Agency.

Applications are installed from the App Store using the Volume Purchasing Program (VPP) tokens through Apple Business Manager Enrollment. This provides application control for iOS mobile devices, and removes the need for users having to install applications from the App Store through an Apple ID.

The risk of non-compliance with controls relating to iOS devices is addressed in the 'DTA - Hybrid Blueprint - Security Risk Management Plan' at R17.

Security controls provided by the HybridSystem

- Microsoft Intune provides MDM and MAM capability.
- The HybridSystem provides Windows 10 for laptops which is hardened in accordance with ACSC guidance. The HybridSystem also provides MDM for iOS but does not fully implement ACSC's guidance for PROTECTED.
- Microsoft BitLocker provides full disk encryption of the HybridSystem mobile devices, implementing Advanced Encryption Standard (AES)-256. Additionally, iOS devices implement AES-256 encryption by default.
- All information transmitted to and from mobile devices and Office 365 is encrypted.
- Bluetooth device type allow lists are configured on Windows 10 devices. Bluetooth is not managed for iOS devices.
- The HybridSystem standard users do not have sufficient permissions to install or uninstall applications on Windows 10 devices. Standard users can install and uninstall applications on iOS devices via the App Store.
- Intune will monitor and report installed iOS applications on any company-owned device.
- The HybridSystem standard users do not have sufficient permissions to modify security functions on Windows 10 devices. Standard users can modify security functions on iOS devices.
- Apple provides timely security updates for iOS devices.

Residual controls to be addressed by the Agency

- The Agency is responsible for developing a mobile device management policy in relation to the HybridSystem that meets requirements outlined in the Annex.

Mobile device usage

Applicability to HybridSystem This section is applicable as the HybridSystem may contain mobile devices.

HybridSystem compliance approach The HybridSystem is reliant on the Agency to development and enforce a mobile device usage policy which include mobile devices that are enrolled into the HybridSystem.

Security controls provided by the HybridSystem Not Applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the HybridSystem that meets requirements outlined in the Annex.

Evaluated products

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

The HybridSystem includes Windows 10 which has been evaluated and therefore the controls relating to evaluated products are applicable to the HybridSystem. No high assurance products are used by the HybridSystem, Azure or Office 365.

HybridSystem compliance approach

A Protection Profile (PP) evaluation has been performed on Windows 10 and Microsoft publish deployment and administration guides for each evaluated operating system. The HybridSystem implements the recommendations for the latest evaluated version of Windows 10 (2004). This includes sourcing installation media directly from Microsoft and implementing configuration hardening.

Security controls provided by the HybridSystem

- The HybridSystem includes Windows 10 which has been evaluated against the relevant Protection Profile.
- Windows 10 installation media is sourced directly from Microsoft in accordance with the evaluated delivery procedures.
- Windows 10 is managed by Microsoft Endpoint Manager (Intune) in accordance with the published guidance from Microsoft as well the ACSC's hardening guide for Windows 10.

Residual controls to be addressed by the Agency

- The Agency is responsible for any evaluated products if they are implemented as part of network connectivity to Azure and Office 365.

ICT equipment management

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

The security of the Azure and Office 365 hosting equipment is the responsibility of Microsoft and is addressed in the respective IRAP reports for Azure and Office 365.

HybridSystem compliance approach

The HybridSystem inherits ICT equipment controls from the underlying Azure and Office 365 platforms.

Security controls provided by the HybridSystem

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the implementation of controls relating to ICT equipment management based on their deployment of the HybridSystem.

Media management

Media usage

Applicability to HybridSystem This section is applicable as removable media may be connected to the HybridSystem endpoints.

HybridSystem compliance approach The HybridSystem implements technical controls to protect the confidentiality and integrity of data written to removeable media devices that may be connected to HybridSystem endpoints.

Security controls provided by the HybridSystem

- Removable media is encrypted via BitLocker using AES-256.

Residual controls to be addressed by the Agency The Agency is responsible for implementing controls relating to media management if media is connected to the HybridSystem.

Media sanitisation

Applicability to HybridSystem The controls relating to the sanitisation of media are not applicable to the HybridSystem and are instead the responsibility of the Agency.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the management, including sanitisation, of media connected to the HybridSystem endpoints.

Media destruction

Applicability to HybridSystem The controls relating to the destruction of media are not applicable to the HybridSystem and are instead the responsibility of the Agency.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the management, including destruction, of media connected to the HybridSystem endpoints.

Media disposal

Applicability to HybridSystem The controls relating to the disposal of media are not applicable to the HybridSystem and are instead the responsibility of the Agency.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the management, including disposal, of media connected to the HybridSystem endpoints.

System hardening

Operating system hardening

Applicability to HybridSystem Operating system hardening is applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem will utilise Windows 10 as the endpoint operating system, provided by the Original Equipment Manufacturer (OEM), and then use the Software Updates component of Microsoft Endpoint Manager or Microsoft Endpoint Configuration Manager (MECM) to maintain the latest version of the operating system.

The HybridSystem will harden the operating system configuration using a combination of Intune and MECM policies to implement ACSC and vendor guidance. These policies achieve the results that would traditionally be performed by Group Policy alone. Local administrator accounts and guest accounts will be disabled and renamed via Intune policy.

The potential attack surface will be minimised by only including required components and apps, removing and disabling the components that aren't needed. Standard users will be prevented from running all script execution engines. The HybridSystem will install applications via Intune or MECM and not allow standard users the ability to install applications.

Available firmware security controls are configured to protect Windows 10 devices from boot time threats. This includes Early Launch Antimalware (ELAM), Secure Boot and Trusted Boot. Measured boot is not configured as it requires an attestation server that is not in scope of the blueprint.

The HybridSystem will use Windows Defender Application Control (WDAC) to perform application control. WDAC is the latest capability from Microsoft for application control and works in a very similar manner to AppLocker. In addition to the enforceable file types available from AppLocker, WDAC also supports driver files (.sys), and kernel mode policies as well as user mode enforcement.

Enhanced Mitigation Experience Toolkit (EMET) is not supported by the latest release of Windows 10 and all functionality of EMET has been incorporated into Windows Defender Exploit Guard which is fully configured.

PowerShell hardening and logging is configured via Intune for the Windows 10 SOE. As the blueprint does not include Public Key Infrastructure (PKI) the Protected Event Logging feature for PowerShell is not included.

Windows Defender Firewall is enabled as part of the HybridSystem Windows 10 Standard Operating Environment (SOE) and configured by Intune policies. Windows Defender Antivirus and Microsoft Defender for Endpoint provide antivirus including signature, reputation and heuristic-based detection. Controlled folder access is also enabled to provide additional ransomware protection.

Scanning frequency for both quick scans and full scans is determined by the policies and occurs for fixed and removable drives.

Endpoint Device Control will be configured by Intune policies restricting usage to only permitted devices. This includes disabling Direct Memory Access (DMA).

Security controls provided by the HybridSystem

- Microsoft have made a commit to support Windows 10 and provide security updates in accordance with the document lifecycle for the operating system.
- Windows 10 Semi-Annual Channel (SAC) is used as the SOE for the HybridSystem.
- The 64-bit version of Windows 10 is used as the SOE for the HybridSystem.
- The Windows 10 SOE has been hardened in accordance with ACSC 'Hardening Microsoft Windows 10 version 21H1 Workstations' guidance.
- Only required software and components are included in the SOE. Default accounts are disabled.
- The default administrator and guest accounts have been disabled and renamed.
- Autorun is disabled for removable media via Intune policies.
- Internet Explorer 11 is disabled as part of the Windows 10 SOE.
- .NET Framework 3.5 and any previous versions are disabled as part of the Windows 10 SOE.
- The 'Exploit protection' feature is enabled as part of the HybridSystem Windows 10 SOE.
- ELAM, Secure Boot and Trusted Boot are enabled as part of the Windows 10 SOE.
- HybridSystem standard users do not have sufficient permissions to modify security functions on Windows 10 devices.
- A combination of WDAC and AppLocker policies prevent the use of script execution engines.
- Standard (unprivileged) users do not have sufficient permissions to install or uninstall applications on Windows 10 devices.
- WDAC provides application control functionality. A combination of hash, publisher certificate and path rules will be used by WDAC for control of applications. Both publisher and product names are used by WDAC for control of applications. WDAC writes to the local event log. Standard users cannot disable application control.
- File permissions prevent standard users from writing to locations that are whitelisted using path rules.
- Microsoft recommended block rules and Microsoft recommended driver block rules to prevent known WDAC bypasses are implemented.
- PowerShell v2 is disabled in the Windows 10 SOE.
- PowerShell is configured to run in Constrained Language Mode (CLM).
- PowerShell logging is enabled as per the ACSC Windows 10 hardening guide.
- Microsoft Defender Exploit Guard and Defender for Endpoint provide HIPS functionality as part of the HybridSystem Windows 10 SOE.
- Windows Defender Firewall is enabled as part of the HybridSystem Windows 10 SOE.
- Microsoft Defender Antivirus and Defender for Endpoint provide antivirus including signature and heuristic-based detection. Virus definitions are set to automatically update. Controlled folder access (ransomware protection) is also configured.

- Intune provides device access control by DeviceID or Device Class.
- Only authorised devices in Intune policies can be connected. Unauthorised devices will not be mounted to the operating system.
- External connections relying on DMA will be disabled via Intune policies.
- Defender for Endpoint centrally stores Endpoint Detection and Response (EDR) logs for all Windows 10 blueprint devices.

Residual controls to be addressed by the Agency

- Where Agencies utilise a SOE developed by third parties, the Agency must ensure that the SOE is scanned for malicious content and configurations before being used and that the design is reviewed and updated at least annually.
- The Agency must validate cryptographic hash rules, publisher certificate rules and path rules used for application control at least annually.
- The Agency is responsible for collecting and storing WDAC and PowerShell logs in a centralised logging facility/SIEM as this capability is not included in the blueprint.
- The Agency is responsible for configuration of Protected Event Logging functionality if required.
- The Agency is responsible for monitoring and actioning cyber security events from the EDR logs.

Application hardening

Applicability to HybridSystem Application hardening is applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem compliance approach is to select native cloud capabilities that are hardened and maintained as part of the service.

The HybridSystem utilises the Monthly Enterprise Channel of Office to ensure the latest versions of software are used. Where third party applications are used these are also targeted at the most recent versions. Software update policies are configured to update plugins, browsers and applications regularly ensuring endpoints are using most recent versions.

ACSC guidance has been incorporated into the applications to harden the configuration and remove unneeded features, including the hardening guide for Office 365.

Web browsers are configured to block Flash content and Java content by the Intune policies. Neither Flash nor Java is included in the Windows 10 SOE. Native Microsoft Edge advertisement blocking is enabled. The blueprint recommends Agencies deploy a third-party add-on to provide further advertisement blocking.

Office macros sourced from the internet are blocked and only signed macros will be allowed to execute. Additional macro controls are configured in the Attack Surface Rules configuration controlled by Intune. Users are not able to change macro settings.

Security controls provided by the HybridSystem

- All applications are supplied by Microsoft which has made a commitment to secure development. The HybridSystem does not include any third-party applications.
- The latest version of Microsoft Office 365 and Microsoft Edge are installed. No third-party applications are installed.
- ACSC guidance has been implemented to harden Office and built-in web browsers.
- Unrequired functionality, such as Microsoft Access, has been removed.
- The Windows 10 SOE restricts the use of add-ons to only those deployed via Intune.
- The Windows 10 SOE does not include Java.
- Native Microsoft Edge advertisement blocking is enabled.
- Internet Explorer 11 is disabled as part of the Windows 10 SOE.
- Attack Surface Reduction rules are configured for Microsoft Office in accordance with the ACSC hardening guides for Windows 10 and Office 365.
- Object Linking and Embedding (OLE) is blocked for Microsoft Office.
- Only Office macros that have been digitally signed by a trusted publisher can execute.
- All macros downloaded from the internet are disabled.
- Antivirus scanning is enabled for Office macros.
- Users cannot change macro settings.
- Defender for Endpoint centrally stores EDR logs for all Windows 10 blueprint devices.

Residual controls to be addressed by the Agency

- The Agency is responsible for hardening any third-party browsers (e.g. Google Chrome) that are deployed to HybridSystem endpoints. The United Kingdom Government provides guidance on hardening Chrome specifically which Agencies may choose to follow.
- The Agency is responsible for reviewing EDR logs in relation to macro executions.

Authentication hardening

Applicability to HybridSystem The authentication hardening section is applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverages Azure AD for controlling system access. All technical capabilities that the HybridSystem performs are completed through Application and Service Principal objects in Azure AD, which utilise certificate-based authentication.

The HybridSystem utilises RBAC, automation and policy controls to restrict access to modify any of the functional capabilities provided by the HybridSystem. The HybridSystem also provides auditing and alerting on attempted or successful modifications of the HybridSystem capabilities.

The HybridSystem provides security controls and an identity management framework that can be utilised to manage system access for systems deployed within the HybridSystem. The HybridSystem enforces multi-factor authentication through Conditional Access policies, creates recovery (emergency access) accounts for maintaining access to resources and enforces password policies for accounts created directly in Azure AD. The HybridSystem uses a soft-token - the Microsoft Authenticator app - to reduce the need for purchase, distribution and management of hard-tokens.

The Microsoft Authenticator app cannot be centrally managed to require the enforcement of a PIN or biometric unlock. It is also not currently considered verifier impersonation resistant.

The Protected User security group is not available in Azure AD and is the Agency's responsibility to populate for on-premises AD used by the HybridSystem.

The HybridSystem utilises Azure AD to store groups utilised for RBAC and provides process and administration documentation for managing access to Azure resources.

To minimise potential user impact, Windows 10 laptops are not rebooted daily. Instead, automatic reboots are only performed as part of automated patching.

Security controls provided by the HybridSystem

- Azure AD is configured to require all users to be authenticated before granting access.
- Azure MFA is enforced for all standard and privileged users accessing M365 services.
- MFA requires Azure AD password and Microsoft Authenticator app (either acceptance of push notification or entry of OTP).
- Azure AD password complexity enforces a minimum character length of 8 characters.
- All authentication attempts are logged in Azure AD Sign-ins.
- Azure AD logs are forwarded to a Log Analytics workspace for long-term secure retention.
- Legacy authentication methods are disabled in the Windows 10 SOE following the ACSC hardening guide.
- Credentials are stored within Azure AD and the on-premises AD.
- Standard Windows & iOS functionality is to obscure passwords during logon.
- Windows Defender Credential Guard is enabled for the Windows 10 SOE.
- Only one previous logon is cached for the Windows 10 SOE.
- The HybridSystem Windows 10 SOE is configured with a screen saver after 15 minutes which requires users to re-authenticate.
- The HybridSystem Windows 10 SOE is configured with a logon banner provided by the Agency.

Residual controls to be addressed by the Agency

- The Agency is responsible for investigating repeated account lockouts.
- The Agency is responsible for managing passwords/passphrases.
- The Agency is responsible for procedures involving provisioning user passwords.
- The Agency is responsible for populating the Protected Users security group for on-premises AD.
- The Agency is responsible for configuring Credential Guard and Remote Credential Guard on servers.
- The Agency is responsible for terminating user sessions and rebooting workstations outside of business hours.
- The Agency is responsible for the wording of the logon banner.

Virtualisation hardening

Applicability to HybridSystem This section is applicable as the HybridSystem includes the Agency's on-premises servers which integrate with M365 components (e.g. Azure AD Connect).

HybridSystem compliance approach The HybridSystem does not provide guidance on the hardening of on-premises servers, which instead are inherited from the Agency.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for implementing virtualisation hardening for servers used as part of the HybridSystem.

System management

System administration

Applicability to HybridSystem The system administration section is applicable to the HybridSystem in the context of the operations and management of the controls that the HybridSystem provides.

HybridSystem compliance approach Privileged Access Workstations (PAWs) and admin jump servers are not used in the HybridSystem due to the limited size of the expected Agencies and all administrative access to the Microsoft 365 portals is with Azure AD accounts using MFA. The risk of not implementing these controls is addressed in the HybridSystem SRMP.

Administration of the HybridSystem is performed through a web browser to a number of Microsoft 365 portals as listed below.

Portal	URL
Defender for Cloud Apps portal	https://portal.cloudappsecurity.com
Azure portal (including Azure AD)	https://portal.azure.com
Microsoft 365 Compliance Center	https://compliance.microsoft.com
Microsoft 365 Defender	https://security.microsoft.com
Office 365 homepage	https://portal.office.com
Defender for Identity portal	https://portal.atp.azure.com
Microsoft 365 admin center	https://admin.microsoft.com/

The HybridSystem protects access to these portals through authentication via Azure AD and enforcement of MFA and location-based policies through Conditional Access. Privileges within the HybridSystem are controlled through the RBAC model.

The Conditional Access policies and RBAC model also extend to the administration of endpoint devices that are deployed as part of the HybridSystem.

The administration of existing resources leveraged by the HybridSystem are listed below.

Resource	Location
Local user accounts and group management	On-premises Active Directory Server
Local mailboxes and contacts	On-premises Exchange Server
Local sites and data stores	On-premises SharePoint Server

Security controls provided by the HybridSystem

- The HybridSystem includes a system administration SOP.
- Azure MFA is required for all privileged user access.

Residual controls to be addressed by the Agency

- The Agency is responsible for provisioning, managing and decommissioning administrative accounts to be used for the HybridSystem administration.

System patching

Applicability to HybridSystem System patching of Office 365 and Azure AD are not applicable as these cloud components are a Microsoft responsibility.

System patching of endpoint devices is required, and this is accomplished via Intune or MECM policies setting the frequency, installation options and reporting values. Microsoft Defender for Endpoint provide a vulnerability management capability to aid Agencies in detecting missing patches and insecure configurations.

HybridSystem compliance approach The HybridSystem compliance approach is to primarily utilise native cloud capabilities that are patched as part of the service.

The HybridSystem uses Intune or MECM to automatically deploy operating system, application, driver, and firmware (where supported) updates to Windows 10 SOE devices.

The blueprint does not include third-party applications or any unsupported software.

Security controls provided by the HybridSystem

- The HybridSystem includes a system administration SOP which specifically references patching.
- Intune or MECM is configured to automatically install updates within 48 hours on all Windows 10 devices.
- Intune or MECM provides a centralised and managed approach to patching.
- Windows Update verifies the integrity of patches before installing them.
- Microsoft Defender for Endpoint provides a continuous vulnerability management capability for all Windows 10 devices.
- The blueprint does not include the use of unsupported software.

Residual controls to be addressed by the Agency

- The Agency is responsible for maintaining and auditing a software register.
- The Agency is responsible for patching any third-party applications deployed to Windows 10 devices.

Change management

Applicability to HybridSystem Change management is not applicable as the ongoing management and maintenance of the HybridSystem utilises the Agency's change management process.

HybridSystem compliance approach The HybridSystem integrates with an Agency's existing change management process.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for all change management processes.

Data backups

Applicability to HybridSystem Data backups are not applicable to the HybridSystem as they are the responsibility of the Agency to implement in accordance with their data preservation strategy.

HybridSystem compliance approach The Agency is responsible for backup and restoration of data and configurations stored in the HybridSystem.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for identifying what backup and restoration requirements they have and how these will be achieved within the HybridSystem.

System monitoring

Event logging and auditing

Applicability to HybridSystem The controls relating to the logging and auditing of events for components included in the HybridSystem are applicable. The HybridSystem does not include web applications, Domain Name System (DNS) or proxy services, and therefore the controls relating to these components are not applicable. The HybridSystem does not configure logging for the on-premises Azure AD Connect and SharePoint Server databases.

HybridSystem compliance approach The HybridSystem provides extensive event logging and auditing for Azure and Microsoft 365 resources that can be incorporated into an Agency's event logging strategy. Logs are stored in Log Analytics for two years which is the maximum available period for Log Analytics.

All logs relevant to the operation and integrity of the HybridSystem are stored in a centralised storage account. The HybridSystem protects the integrity of logs through policy enforcement, automation and RBAC.

Local event logs on Windows 10 devices will be lost when endpoints are rebuilt as the local event logs are not centralised.

Security controls provided by the HybridSystem

- Defender for Endpoint and Defender for Office 365 centralise logs relating to the security of devices and Office services.
- Windows 10 devices and Office 365 services leverage Microsoft's Window Time service.
- Azure AD logs authentication events to Log Analytics.
- The following events are logged to the local event log on each Windows 10 endpoint:
  - access to important data and processes
  - application crashes and any error messages
  - attempts to use special privileges
  - changes to accounts
  - changes to security policy
  - changes to system configurations
  - DNS and Hypertext Transfer Protocol requests
  - failed attempts to access data and system resources
  - service failures and restarts
  - system startup and shutdown
  - transfer of data to external media
  - user or group management
  - use of special privileges.
- Logs include the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded.
- Logs stored in Log Analytics are protected from unauthorised access, modification and deletion by the Azure AD RBAC model. Standard Windows 10 users do not have access to modify the local event logs.

Residual controls to be addressed by the Agency

- The Agency is responsible for developing and implementing an event logging policy.
- The Agency is responsible for establishing and maintaining logging facilities, including for the centralisation of Window 10 local event logs.
- The Agency is responsible for longer term log retention (greater than the two years offered by Log Analytics).
- The Agency is responsible for storing any DNS or proxy logs they generate as part of the system.

- The Agency is responsible for logging authentication requests to the on-premises AD.
- The Agency is responsible for logging for the on-premises Azure AD Connect database.
- The Agency is responsible for logging for the on-premises SharePoint Server database.

Software development

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

Not applicable as the HybridSystem is not designed to support software development activities.

HybridSystem compliance approach

Not applicable.

Security controls provided by the HybridSystem

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for all application development controls but can leverage the HybridSystem security controls detailed in this document.

Database systems management

This section does not include specific subsections as the information is the same for all subsections of this chapter.

Applicability to HybridSystem

Not applicable as the management of database servers, database management system software and databases leverage by the HybridSystem is the responsibility of the Agency.

HybridSystem compliance approach

Azure AD Connect and SharePoint Server leverage databases which are provided by the Agency. Neither of these databases are used to store any passwords/passphrases.

Security controls provided by the HybridSystem

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for managing the server used to host the Azure AD Connect database.
- The Agency is responsible for managing the server used to host the SharePoint Server database.
- The Agency is responsible for managing the database servers accessing the databases.
- The Agency is responsible for managing the database management system software used to manage the databases.
- The Agency is responsible the managing the Azure AD Connect database.
- The Agency is responsible the managing the SharePoint Server database.

Email management

Email usage

Applicability to HybridSystem The controls relating to email usage are applicable to the HybridSystem as it provides an email capability of its users.

HybridSystem compliance approach The HybridSystem provides the capability for users to apply protective markings to emails based on their classification. If required, users have the ability to lower the classification of an email, but are required to provide a text-based justification that is included in the audit log. This is due to a product limitation in Microsoft Information Protection (MIP).

The HybridSystem will leverage an Agency's Secure Internet Gateway (SIG) for proxy and mail services.

Security controls provided by the HybridSystem

- The HybridSystem applies protective markings based on the classification of the content of emails, including attachments.
- Users are required to select the classification of emails to apply protective markings.
- Only appropriate classification options will be presented to HybridSystem users.
- Defender for Office 365 will notify users and administrators of blocked emails.

Residual controls to be addressed by the Agency

- The Agency is responsible for developing and implementing an email usage policy.
- The Agency is responsible for preventing access to unapproved sites and services from within the network.
- The Agency is responsible for ensuring their email gateway blocks, logs and reports on emails with inappropriate protective markings.
- The Agency is responsible for conducting a risk assessment if the Agency chooses not to use a SIG.

Email gateways and servers

Applicability to HybridSystem The controls relating to email gateways and servers are applicable to the HybridSystem as it leverages Exchange Online.

HybridSystem compliance approach The HybridSystem leverages Exchange Online in conjunction with on-premises Exchange to leverage cloud security capabilities and expand email capability to the cloud. Native Exchange Online security capabilities are enabled to prevent against email-related threats such as spoofing and phishing. On-premises Exchange Server and Exchange Online are configured to route through the Agency's existing email gateway.

The advanced features of Defender for Office 365, including Safe Attachments and Safe Links which provide sandboxing of attachments and inspective of hyperlinks respectively, are enabled by the HybridSystem. This provides email content filtering and expands on the default protections offered by Exchange Online Protection (EOP).

Security controls provided by the HybridSystem

- Exchange Online is configured to route through the Agency's existing email gateway.
- Email traffic between external users and Exchange Online is encrypted with TLS 1.2. Exchange Online then forwards emails to the Agency's existing email gateway via an Exchange connector.
- Exchange Online is not configured to act as an open relay.
- Exchange Online implements TLS 1.2 for opportunistic TLS encryption where supported by the other mail server.
- Exchange Online implements Mail Transfer Agent - Strict Transport Security (MTA-STS) for outbound mail flow.
- Sender Policy Framework (SPF) is configured in Exchange Online using a hard fail record. SPF blocks are visible to the recipients.
- DomainKeys Identified Mail (DKIM) is configured in Exchange Online and DKIM signatures on received emails are verified.
- Domain-based Message Authentication, Reporting and Conformance (DMARC) records are configured in Exchange Online.
- Defender for Office 365 provides content filtering including sandboxing of attachments (Safe Attachments) and inspection of links (Safe Links).

Residual controls to be addressed by the Agency

- The Agency is responsible for controls implemented by their existing email gateway.
- The Agency's gateway is responsible for blocking incoming emails that use an internal domain name as the source address.
- The Agency's gateway is responsible for ensuring undeliverable notifications are only sent to sender that are verified by SPF or other trusted means.
- The Agency is responsible for any backup or alternative email gateways.

Network management

Network design and configuration

Applicability to HybridSystem The majority of the controls relating to network design and configuration are not directly applicable to the HybridSystem and are instead the responsibility of the Agency to implement. This is due to the HybridSystem not including network devices within its scope.

HybridSystem compliance approach The HybridSystem leverages the Microsoft backbone to provide networking for the Office 365 and Azure services. LAN design and configuration is the responsibility of the Agency and may reuse existing capabilities. The HybridSystem designs the interfaces between endpoints and services, including how data traverses public networks such as the internet.

The HybridSystem is designed to primarily run on-premises but also be able to use the public internet. All security controls are implemented on the endpoint devices and the Office 365 component.

Security controls provided by the HybridSystem

- The Office 365 design includes a high level network diagram showing the components that are considered in scope.
- The Office 365 design which includes the high level network design has a last updated date.
- All communication between HybridSystem Windows 10 endpoints and Office 365 components is encrypted by TLS.
- The blueprint uses Conditional Access policies to restrict access to only specified geographic regions within Australia. The blueprint also uses Azure AD Identity Protection to analyse sign-in logs to identify and notify administrators when users are identified as originating from anonymous proxy IP addresses.

Residual controls to be addressed by the Agency

- The Agency is responsible for the management of network devices used in relation to the HybridSystem.
- The Agency is responsible for implementing security controls within their email gateway.
- The Agency is responsible for managing servers used as part of the HybridSystem.
- The Agency is responsible for ensuring that they segregate their network from that of service providers.
- The Agency is responsible for reviewing alerts from Defender for Cloud Apps and Azure AD Identity Protection.
- The Agency is responsible for ensuring that outbound traffic to anonymity networks is blocked.
- The Agency is responsible for implementing a protective DNS service as part of their gateway.

Wireless networks

Applicability to HybridSystem The controls relating to wireless networks are not applicable as the HybridSystem does not include any wireless networks.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for securing any wireless networks that they provide to enable connectivity between HybridSystem endpoints and Azure/Office 365 services.

Service continuity for online services

Applicability to HybridSystem The controls relating to service continuity for online services are not applicable as the HybridSystem does not host online services.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the procurement and management of online services as applicable.

Using cryptography

Cryptographic fundamentals

Applicability to HybridSystem The controls relating to cryptographic fundamentals are applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverages cryptography provided by Microsoft to encrypt both data at rest and data in transit. This includes the use of Microsoft BitLocker to encrypt mobile devices using an Australian Signals Directorate (ASD) Approved Cryptographic Algorithm (AACA), namely AES. Note, that the HybridSystem does not use encryption for the purposes of reducing the handling requirements for endpoints.

Microsoft's implementation of cryptography, including TLS 1.2 which is an ASD Approved Cryptographic Protocol (AACP), has been assessed as part of the IRAP assessments for Azure and Office 365. However, an ASD Cryptographic Evaluation (ACE) has not been performed on Microsoft's cryptographic software.

At the time of writing Microsoft does not support the latest version of TLS – version 1.3. Microsoft have previously stated that versions 1.0 and 1.1 are not supported and were to become deprecated for Office 365 services from June 2020, however this has since been delayed due to world events. See Preparing for TLS 1.2 in Office 365 and Office 365 GCC.

Security controls provided by the HybridSystem

- The HybridSystem uses Microsoft BitLocker for encryption leveraging AES which is an AACA.
- Microsoft BitLocker provides full disk encryption of the HybridSystem mobile devices, implementing AES-256. BitLocker recovery keys are stored in Azure AD.
- TLS with AES is used to protect traffic to and from Azure and Office 365 servers over the internet.

Residual controls to be addressed by the Agency

- The Agency is responsible for the management of cryptographic keys used in relation to the HybridSystem other than those managed by Microsoft as part of the Microsoft 365 cloud services.
- The Agency is responsible for informing users of their responsibilities in relation to the management encrypted devices.

ASD approved cryptographic algorithms

Applicability to HybridSystem The controls relating to AACAs are applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverage's Microsoft's implementation of AACAs in Azure and Office 365.

Security controls provided by the HybridSystem

- Microsoft Azure and Office 365 services implement AACAs where possible.
- Microsoft Azure and Office 365 services implement Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) as the preferred algorithm.
- Microsoft Azure and Office 365 services do not use Diffie-Hellman (DH).
- Microsoft Azure and Office 365 services do not use Digital Signature Algorithm (DSA).
- Microsoft Azure and Office 365 services implement National Institute of Standards and Technology (NIST) P-256 and P-384.
- Microsoft Azure and Office 365 services use a 256-bit key where possible for Elliptic Curve Diffie-Hellman (ECDH).
- Microsoft Azure and Office 365 services use a 2048-bit key for Rivest–Shamir–Adleman (RSA).
- Microsoft Azure and Office 365 services use separate RSA key pairs for these purposes.
- SHA-384 is the preferred hashing algorithm used as part of TLS for Office 365 components.
- AES-256 is used for BitLocker encryption.

Residual controls to be addressed by the Agency Not applicable.

ASD approved cryptographic protocols

Applicability to HybridSystem The controls relating to AACPs are applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverage's Microsoft's implementation of AACPs in Azure and Office 365.

Security controls provided by the HybridSystem

- Microsoft Azure and Office 365 services implement AACPs where possible.

Residual controls to be addressed by the Agency Not applicable.

Transport layer security

Applicability to HybridSystem The controls relating to TLS are applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverage's Microsoft's implementation of TLS in Azure and Office 365.

Security controls provided by the HybridSystem

- Microsoft Azure and Office 365 services implement TLS versions 1.2 and 1.3.
- Microsoft Azure and Office 365 services implement AES in Galois Counter Mode (GCM).
- Microsoft Azure and Office 365 services implement secure renegotiation.
- Microsoft Azure and Office 365 services implement ECDHE as the preferred algorithm.
- Microsoft Azure and Office 365 services use SHA-2-based certificates.
- Microsoft Azure and Office 365 services use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function.
- Microsoft Azure and Office 365 services disable TLS compression.
- Microsoft Azure and Office 365 services implement Perfect Forward Secrecy (PFS).

Residual controls to be addressed by the Agency Not applicable.

Secure shell

Applicability to HybridSystem The controls relating to the use of Secure Shell (SSH) are not applicable to the HybridSystem as it does not utilise SSH.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency Not applicable.

Secure/multipurpose internet mail extension

Applicability to HybridSystem The controls relating to the use of Secure/Multipurpose Internet Mail Extension (S/MIME) are not applicable to the HybridSystem as it does not utilise S/MIME.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency Not applicable.

Internet protocol security

Applicability to HybridSystem The controls relating to the use of Internet Protocol Security (IPsec) are not applicable to the HybridSystem as it does not utilise IPsec.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency Not applicable.

Cryptographic system management

Applicability to HybridSystem The controls relating to cryptographic system management is not applicable to the HybridSystem as the HybridSystem does not include the use of Commercial Grade Cryptographic Equipment (CGCE) equipment.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the management of any CGCE used in relation to the HybridSystem.

Gateway management

Gateways

Applicability to HybridSystem The controls relating to gateways are applicable to the HybridSystem as the solution is designed to integrate with a SIG provided by the Agency.

HybridSystem compliance approach The HybridSystem leverages the Agency's SIG capability where required.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the implementation of security controls relating to their internet and email gateway if integrated with the HybridSystem.

Cross domain solutions

Applicability to HybridSystem The controls relating to cross-domain solutions are not applicable as the HybridSystem does not include any cross-domain solutions.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency Not applicable.

Firewalls

Applicability to HybridSystem The controls relating to firewalls are not applicable to the HybridSystem as the HybridSystem does not include firewalls for the purpose of separating official/classified and public networks.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the implementation of security controls relating to their email gateway if integrated with the HybridSystem.

Diodes

Applicability to HybridSystem The controls relating to diodes are not applicable to the HybridSystem as the HybridSystem does not include any diodes or unidirectional gateways.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency Not applicable.

Web proxies

Applicability to HybridSystem The controls relating to web proxies are applicable to the HybridSystem as the solution leverages the Agency's SIG for proxy services.

HybridSystem compliance approach The HybridSystem does not include a web proxy service.

Web proxies, content filters, SIG and VPN connections between mobile devices and Agency networks are not currently included within the Protected Utility design.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for the development and implementation of a web usage policy.
- The Agency is responsible for the implementation of a web proxy for devices within their network.

Web content filters

Applicability to HybridSystem The controls relating to web content filters are applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverages Defender for Endpoint to provide web content filtering capabilities on Windows 10 devices.

Security controls provided by the HybridSystem

- Web content filtering is enabled for Windows 10 devices using Microsoft Defender for Endpoint.
- Client-side active content, including all Java and Flash content, is blocked on all Windows 10 devices.
- Microsoft Defender for Endpoint blocks specific web categories which are maintained by Microsoft.

Residual controls to be addressed by the Agency

- The Agency is responsible for all gateway configurations relating to web content filtering.

Content filtering

Applicability to HybridSystem The controls relating to content filtering are applicable to the HybridSystem.

HybridSystem compliance approach The HybridSystem leverages Office 365 capabilities including Defender for Office 365 and EOP to inspect and manage email traffic.

The blueprint does not include content validation, conversion, and sanitisation capabilities, and digital signatures/checksums are not validated when files are imported.

Security controls provided by the HybridSystem

- Exchange Online Protection and Defender for Office 365 are configured to prevent specific file types from entering the system via email.
- Defender for Office 365 provides content filtering including sandboxing of attachments (Safe Attachments) and inspection of links (Safe Links).
- Multiple scanning engines are provided by Exchange Online Protection, Defender for Office 365 and Defender for Endpoint.
- Archives are scanned for malware.
- Defender for Office 365 alerts are configured.
- Integrity of patches is verified before installation.

Residual controls to be addressed by the Agency

- The Agency is responsible for implementing content filtering for web traffic and other vectors.

Peripheral switches

Applicability to HybridSystem The control relating to peripheral switches are not applicable to the HybridSystem as the HybridSystem does not include any peripheral switches.

HybridSystem compliance approach Not applicable.

Security controls provided by the HybridSystem Not applicable.

Residual controls to be addressed by the Agency Not applicable.

Data transfers

Applicability to HybridSystem

The controls relating to data transfers are applicable to the HybridSystem as it is expected users will transfer data to and from the solution.

HybridSystem compliance approach

The HybridSystem includes Microsoft Defender for Endpoint to assist with the inspection and auditing of data transfer to and from HybridSystem endpoints. Event logs are generated when data is transferred to external media from a Windows 10 endpoint.

The HybridSystem does not provide configuration advice on protective marking checks for documents due to the reliance on existing platforms and the difference in existing architectures across Commonwealth entities.

Security controls provided by the HybridSystem

- Defender for Endpoint will scan all data copied onto HybridSystem Windows 10 devices.
- Event logs are generated when data is transferred to external media from a Windows 10 endpoint.

Residual controls to be addressed by the Agency

- The Agency is responsible for the development and implementation of a data transfer policy.
- The Agency is responsible for auditing data transfer logs.