

# Hybrid system security plan

2021-02-08

## 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 Agencies 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 allowing log in from anywhere and appropriate security policies to be applied.
- Office 365 – Configuration of Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Team 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 boundary of the system 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 tenancy 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 Figure 1 the system therefore includes:

- Office 365 (including Azure AD)
- Multi-Factor Authentication (MFA)
- Subscription and its management
- Tenancy and its management
- On-premises and its management
- Endpoints including the hardware and Basic Input/Output System (BIOS) 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.

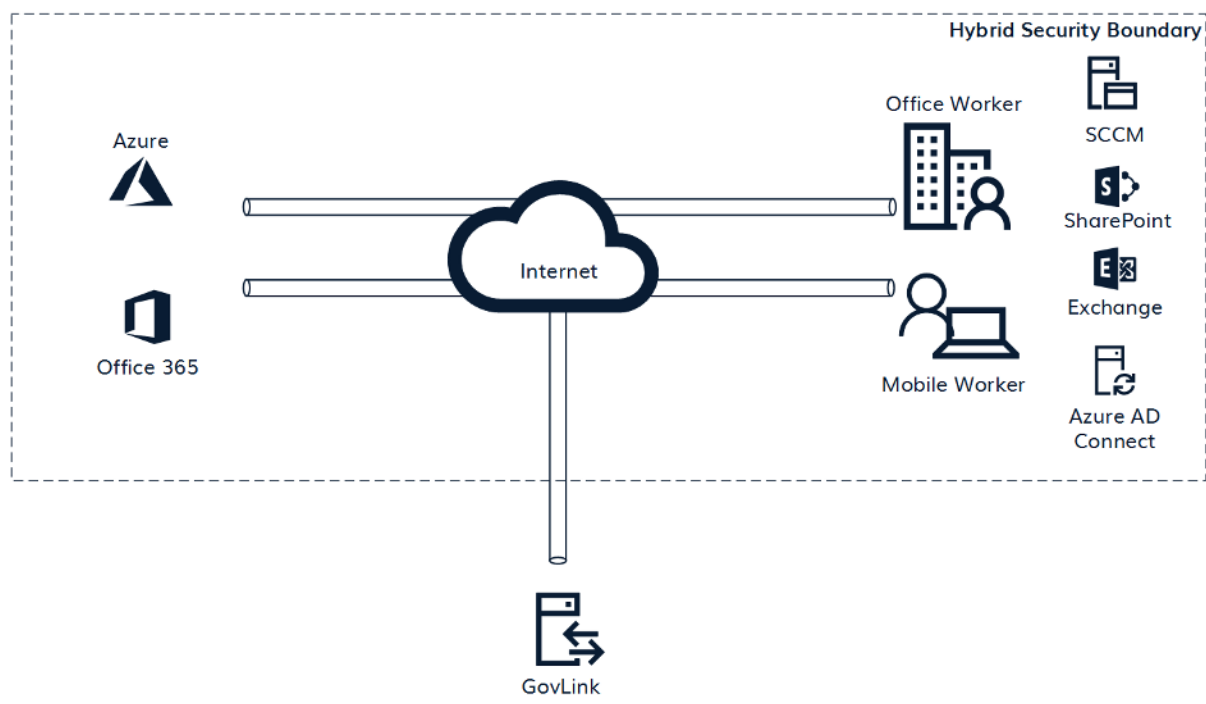


Figure 1: Figure 1 Hybrid Security Boundary

### 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 2020 update), refer to the 'DTA - Hybrid Blueprint - System Security Plan Annex (August 2020)'.

## Overarching security policies

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

- The Australian Government ISM (October 2020) 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 12 Devices (June 2020).
- The Protected Security Policy Framework.
- Hardening Microsoft Windows 10 version 1709 Workstation (April 2020).

## 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 (August 2020)
- DTA – Blueprint – Client Devices Design (August 2020)
- DTA – Blueprint – Platform Design (August 2020)
- DTA – Blueprint – Office 365 Design (August 2020)
- DTA – Hybrid Blueprint – System Security Plan (October 2020) (this document)
- DTA – Hybrid Blueprint – System Security Plan Annex (October 2020)
- DTA – Hybrid Blueprint – Security Risk Management Plan (October 2020)
- DTA – Hybrid Blueprint – Standard Operating Procedures (October 2020)
- DTA – Hybrid Blueprint – Incident Response Plan (October 2020)

The suite of documentation produced to support ACSC’s certification of Azure and Office 365 for PROTECTED have also been leveraged in the development of the HybridSystem, and includes the following :

- 2019 Microsoft Azure IRAP Assessment Report
- 2019 Microsoft Office 365 IRAP Assessment Report

Both 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 (August 2020)’ (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	PROTECTED	N/A
Monitoring and Compliance	Intune Policies	PROTECTED	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 address 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, 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.
Guidelines for Physical Security	Not Applicable	The HybridSystem inherits the physical security controls which are implemented by Microsoft for Azure and Office 365 components.

ISM Chapter	Applicability	Rationale
Guidelines for Personnel Security	Not Applicable	The Agency is responsible for the personnel security as it relates to users of the HybridSystem.
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 HybridSystem does not contain any Information and Communications Technology (ICT) Equipment, and the security of the Azure and Office 365 hosting equipment is the responsibility of Microsoft.
Guidelines for Media	Applicable	The HybridSystem is responsible for restricting the use of unapproved 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.

ISM Chapter	Applicability	Rationale
Guidelines for Networking	Applicable	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. The Office 365 design includes a high-level network diagram showing the components that are considered in scope.
Guidelines for Cryptography	Applicable	The HybridSystem makes use of cryptography to protect both data at rest and data in transit.
Guidelines for Gateways	Applicable	The HybridSystem leverages Exchange Online Protection and Office 365 Advanced Threat Protection (ATP) for content filtering.
Guidelines for Data Transfers	Applicable	The HybridSystem is responsible for implementing technical controls relating to data transfer and content filtering.

## 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 ATP to assist in the detection of cyber security incidents. The Defender ATP security operations dashboard shows:
  - Active alerts
  - Machines at risk
  - Sensor health
  - Service health
  - Daily machines reporting
  - Active automated investigations
  - Users at risk and
  - Suspicious activities
- The HybridSystem utilises Azure ATP to assist in the detection of cyber security incidents relating to authentication. The Azure ATP portal shows:
  - Suspicious activities
  - Health alerts

**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 Microsoft Defender ATP 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 Shearwater. With the exception of Microsoft Defender ATP, 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 Cloud App Security is available in the Europe or United States regions. If the Azure AD tenant is in Australia, United States is automatically selected. Microsoft Defender Advanced Threat Protection 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. Azure Advanced Threat Protection 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 Software as a Service (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 RE-SPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARDENING	ACCESS MANAGEMENT	VULNERABILITY & PATCH MANAGEMENT	SYSTEM MONITORING	SOFTWARE DEVELOPMENT
IDENTITY & ACCESS MANAGEMENT	AZURE AC-TIVE DIRECTORY	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
IDENTITY & ACCESS MANAGEMENT	ON-PREM AC-TIVE DIRECTORY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
SECURITY CLOUD APP SECURITY	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT

CATEGORY	ITEM	INCIDENT RE- SPONSE	BACKUP	PHYSICAL SECURITY	SYSTEM HARD- ENING	ACCESS MAN- AGE- MENT	VULNERA- & PATCH MAN- AGE- MENT	SYSTEM MONI- TOR- ING	SOFTWARE DE- VEL- OP- MENT
SECURITY	AZURE AD- VANCED THREAT PRO- TEC- TION	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
SECURITY	MICROSOFT DE- FENDER AD- VANCED THREAT PRO- TEC- TION	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
SECURITY	LOG ANA- LYT- ICS	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT
SECURITY	SECURITY INFOR- MA- TION & EVENT MAN- AGE- MENT	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY
CLIENT CON- FIGU- RA- TION	INTUNE	AGENCY	AGENCY	MICROSOFT	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
CLIENT CON- FIGU- RA- TION	SCCM	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
CLIENT CON- FIGU- RA- TION	PRINTING	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY
BACKUP & OP- ERA- TIONAL MAN- AGE- MENT	BACKUP PLAT- FORM	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY

CATEGORY	ITEM	INCIDENT RE- SPONSE	BACKUPS	PHYSICAL SECU- RITY	SYSTEM HARD- ENING	ACCESS MAN- AGE- MENT	VULNERA- & PATCH MAN- AGE- MENT	SYSTEM MONI- TOR- ING	SOFTWARE DE- VEL- OP- MENT
SYSTEM AD- MINIS- TRA- TION	ADMINIS- TRATION	THAT CON- SOLES	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT
SYSTEM AD- MINIS- TRA- TION	PRIVILEGE IDENTI- TITY MAN- AGE- MENT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	AGENCY	MICROSOFT	MICROSOFT	MICROSOFT

### Office 365

ITEM	INCIDENT RE- SPONSE	BACKUPS	PHYSICAL SECU- RITY	SYSTEM HARD- ENING	ACCESS MAN- AGE- MENT	VULNERA- & PATCH MAN- AGE- MENT	SYSTEM MONI- TOR- ING	SOFTWARE DEVEL- OP- MENT
EXCHANGE ON- LINE	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
SHAREPOINT ON- LINE	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
ONEDRIVE FOR BUSI- NESS	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 & COM- PLI- ANCE PLAT- FORMS	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT
EXCHANGE ON- LINE PRO- TEC- TION	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT

ITEM	INCIDENT RE-SPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARD-ENING	ACCESS MAN-AGE-MENT	VULNERAB& PATCH MAN-AGE-MENT	SYSTEM MONI-TOR-ING	SOFTWARE DEVEL-OP-MENT
OFFICE 365 AD-VANCED THREAT PRO-TEC-TION	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AGENCY	MICROSOFT	AGENCY	MICROSOFT

#### Client devices

ITEM	INCIDENT RE-SPONSE	BACKUPS	PHYSICAL SECURITY	SYSTEM HARD-ENING	ACCESS MAN-AGE-MENT	VULNERAB& PATCH MAN-AGE-MENT	SYSTEM MONI-TOR-ING	SOFTWARE DEVEL-OP-MENT
WINDOWS 10 – IN-TUNE MAN-AGED	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
WINDOWS 10 – SCCM MAN-AGED	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	AGENCY	MICROSOFT
IOS – IN-TUNE MAN-AGED	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.

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.

### Security controls provided by the HybridSystem

- The HybridSystem provides SOPs for administrators and support staff to understand, monitor and operate the HybridSystem provided security controls.

- The HybridSystem includes detailed design, configuration, operational and support documentation.
- The HybridSystem provides security documentation for input into an Agency's security processes.
- The HybridSystem's security documentation and notification of subsequent changes is communicated by DTA to Agencies who have implemented the HybridSystem.

#### **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, SRMP, IRP, SOPs and other operational documentation to assist in the understanding of the system and the security controls included.

#### **Security controls provided by the HybridSystem**

- The HybridSystem provides SOPs for administrators and support staff to understand, monitor and operate the HybridSystem provided security controls.
- The HybridSystem includes detailed design, configuration, operational and support documentation.
- The HybridSystem provides security documentation for input into an Agency's security processes.

#### **Residual controls to be addressed by the Agency**

- The Agency should incorporate the 'DTA – Hybrid Blueprint – Incident Response Plan (August 2020)' that applies to the HybridSystem into their Agency-wide IRP.
- The Agency is responsible for developing a continuous monitoring plan.
- 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 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 for 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**

Not applicable to the HybridSystem as this is an Agency's responsibility. An Agency's implementation of personnel security controls should cover the HybridSystem system.

#### **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.

#### **Security controls provided by the HybridSystem**

- The HybridSystem provides a framework for identity and access management for Azure and Office 365 resources.
- The HybridSystem provides emergency access or 'break-glass' accounts to be used in emergency situations to restore access to an environment or tenant.
- The HybridSystem provides Microsoft Cloud App Security (MCAS) policy monitoring to monitor the activity of the break-glass accounts.

### **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 for establishing processes for the creation, maintenance and remediation of accounts created within the system in accordance with the controls within the annex.

### **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 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 HybridSystem solution 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 this or a similar service should undertake a security assessment to ensure that the product addresses their security requirements.

### **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.

### **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 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.

iOS devices are lightly managed and partially comply with the ACSC 'Security Configuration Guide - Apple iOS 12 Devices' and Information Security Manual (ISM) to maximise usability for the target users. Note: Agencies should do a risk assessment before deciding to change settings relating mobile devices.

Bluetooth is enabled as it allows users to pair devices they may required 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.

To provide ease of use and maintain productivity users can download apps from the App Store. The agency can track, and monitor apps found on managed devices that have been enrolled in Intune. Details on how to view and report on discovered apps can be found in the 'DTA - Hybrid Blueprint - Security Standard Operating Procedures (August 2020)'.

The risk of lightly managed iOS devices is addressed in the 'DTA - Hybrid Blueprint - Security Risk Management Plan (August 2020)' at R17.

### Security controls provided by the HybridSystem

- Microsoft Intune provides MDM and MAM capability.
- The HybridSystem does not include the use of privately-owned mobile devices. Only Agency-owned devices are enrolled and allowed to access data.
- 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 is disabled 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.
- The HybridSystem does not use a VPN on iOS devices and therefore a direct connection to the internet is used.

### 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 develop and enforce a mobile device usage policy which includes 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 publishes deployment and administration guides for each evaluated operating system. The HybridSystem implements the recommendations for the latest evaluated version of Windows 10 (May 2019 Update). 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 Intune in accordance with the published guidance from Microsoft as well as 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 restrict access to removable media devices that may be connected to the HybridSystem endpoints.

### **Security controls provided by the HybridSystem**

- Autorun is disabled for removable media via Intune policies.
- Only authorised devices that are permitted in Intune policies can be connected to the HybridSystem endpoints. Unauthorised devices will not be mounted to the operating system.
- External connections relying on Direct Memory Access (DMA) will be disabled via Intune policies
- 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 Intune or SCCM to maintain the latest version of the operating system.

The HybridSystem will harden the operating system configuration using a combination of Intune and Microsoft System Center Configuration Manager (SCCM) policies to implement ACSC and vendor guidance. These policies achieve the results that would traditionally be performed by group policies 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 SCCM and not allow standard users the ability to install applications.

The HybridSystem will use Windows Defender Application Control (WDAC) to perform application control. WDAC is the latest system from Microsoft for application control and works in a very similar manner to AppLocker. In addition to performing all functions of AppLocker, WDAC is also able to control plug-ins, add-ins, modules and code at the kernel level as well as the user level.

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.

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 ATP provide antivirus including signature, reputation and heuristic-based detection.

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.

## Security controls provided by the HybridSystem

- 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 guidance where possible using Intune.
- The default administrator and guest accounts have been disabled and renamed.
- Intune and SCCM policies prevent standard users from running cmd.exe however can only restrict the PowerShell execution policy to RemoteSigned.
- RBAC policy defines separate domain and local administrator roles. Standard users do not have permissions to install or uninstall software.

- 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's recommended block rules to prevent known WDAC bypasses are implemented.
- The 'Exploit protection' feature is enabled as part of the HybridSystem Windows 10 SOE.
- Windows Defender Exploit Guard and Defender ATP provide Host Intrusion Prevention System (HIPS) functionality as part of the HybridSystem Windows 10 SOE.
- Windows Defender Firewall is enabled as part of the HybridSystem Windows 10 SOE.
- Defender Antivirus and Defender ATP provide antivirus including signature and heuristic-based detection. Reputation rating features are enabled.
- Intune and SCCM provides device access control by DeviceID or Device Class.

### **Residual controls to be addressed by the Agency**

- Where Agencies utilise 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.

### **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 Targeted 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.

Web browsers are configured to block Flash content and Java content by the Intune policies and Java can be selected by exception for non-internet sites. The HybridSystem does not include a web advertisements blocker to reduce the reliance on third party applications.

Office 365 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 is installed.
- ACSC guidance has been implemented to harden Office and built-in web browsers.
- Flash is blocked in both Edge and Internet Explorer.
- Flash and Java-based web advertisements are blocked in Edge and Internet Explorer.
- Java is blocked in both Edge and Internet Explorer.
- Support for Flash content is disabled by default.
- Object Linking and Embedding (OLE) is blocked for Microsoft Office.
- Unrequired functionality, such as Microsoft Access, has been removed.
- The use of add-ons is restricted to Microsoft-provided add-ons only.
- Microsoft's Attack Surface Reduction Rules are implemented in the configuration controlled by Intune.

- Only signed macros are enabled.
- All macros downloaded from the internet are disabled.
- Users cannot change macro settings.

#### **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 .

#### **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 accounts for maintaining access to resources and enforces password policies for accounts created directly in Azure AD. The HybridSystem uses a soft-token to reduce the need for purchase, distribution and management of hard-tokens.

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

#### **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.
- MFA requires complex password and One Time Password (OTP) from Microsoft Authenticator App (soft token).
- None of the authentication factors on their own can be used for single-factor authentication to another system.
- Azure MFA is enforced for all users accessing Office 365 content.
- Azure AD self-service password reset requires users to verify their identity before resetting their password in accordance with password complexity requirements.
- Local Area Network (LAN) Manager is not used by the HybridSystem, however New Technology LAN Manager (NTLM) is used within the system.
- Credentials are stored within Azure AD. Azure AD Identity Protection is enabled to detect leaked passwords.
- 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 terminating user sessions and rebooting workstations outside of business hours.

## Virtualisation hardening

**Applicability to HybridSystem** All in scope servers are provided by Microsoft and secured in line with the controls outlined in the Microsoft Office 365 and Azure IRAP Assessments.

**HybridSystem compliance approach** Agencies are responsible for securing any servers that they deploy in line with the controls in this section outlined within the ISM.

**Security controls provided by the HybridSystem** Not applicable.

**Residual controls to be addressed by the Agency** The Agency is responsible for managing non-Microsoft 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 in Table 4.

Table 4 Microsoft Management Portals

Portal	URL
Microsoft Defender ATP portal	<a href="https://securitycenter.windows.com">https://securitycenter.windows.com</a>
Cloud App Security portal	<a href="https://portal.cloudappsecurity.com">https://portal.cloudappsecurity.com</a>
Azure portal (including Azure AD)	<a href="https://portal.azure.com">https://portal.azure.com</a>
Microsoft 365 Compliance Center	<a href="https://compliance.microsoft.com">https://compliance.microsoft.com</a>
Microsoft 365 Security Center	<a href="https://security.microsoft.com">https://security.microsoft.com</a>
Office 365 homepage	<a href="https://portal.office.com">https://portal.office.com</a>
Azure ATP portal	<a href="https://portal.atp.azure.com">https://portal.atp.azure.com</a>

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 leverage by the HybridSystem are listed in Table 5.

Table 5 Microsoft Management Portals

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 SCCM policies setting the frequency, installation options and reporting values.

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

For patching endpoint devices deployed by the Agency, the HybridSystem provides configuration of which patches to apply, deferral periods, update behaviour and reporting.

### **Security controls provided by the HybridSystem**

- The HybridSystem provides the types of updates that are applied to endpoints.
- The HybridSystem configures the intervals for checking for new updates.
- The HybridSystem provides the reporting of device status to determine which devices have received updates.
- The HybridSystem includes a system administration SOP which specifically references patching.
- All configurations are included in the relevant ABAC.
- Application and driver patches will be automatically deployed via Intune or SCCM for the HybridSystem Windows 10 SOE.
- Operating system patches will be automatically deployed via Intune or SCCM for the HybridSystem Windows 10 SOE.
- Intune or SCCM provides a centralised and managed approach to patching.
- Windows Update verifies the integrity of patches before installing them.

### **Residual controls to be addressed by the Agency**

- The Agency is responsible for system patching for all systems deployed within the HybridSystem.
- The Agency is responsible for any firmware patching dependent on the specific hardware model chosen by them.
- The Agency is responsible for viewing the reporting and alerts and rectification of faults as they occur.

### **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 data backups data and configurations stored in 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 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

- Microsoft Defender ATP and Office 365 ATP centralise logs relating to the security of devices and Office services respectively.
- Windows Time is used as the time source for all HybridSystem components.
- Azure AD sign-in and audit logs are centralised by Log Analytics.
- Update Management and Security Center logs are centralised by 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 don't 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 centralising local event logs from Windows 10 endpoints if required by their event logging policy.
- 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.

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 in accordance with the Protective Security Policy Framework (PSPF) 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.
- Office 365 ATP 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 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 Office 365 ATP, including Safe Attachments and Safe Links which provide sandboxing of attachments and inspection 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.
- 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.
- Office 365 ATP provides content filtering including sandboxing of attachments (Smart Attachments) and inspection of links (Smart Links).

#### **Residual controls to be addressed by the Agency**

- The Agency is responsible for controls implemented by their existing email gateway.
- 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.

### Security controls provided by the HybridSystem

- The Office 365 design which includes the high-level network design has a document control table listing the last update date.

### 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.

### 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 majority controls relating to service continuity for online services controls are not applicable to the HybridSystem as it does not host online services. As the Blueprint is dependent on online services hosted by Microsoft some controls are applicable.

**HybridSystem compliance approach** Microsoft is the service provider for the online services used by the HybridSystem, specifically Azure and Office 365. The HybridSystem inherits Microsoft's implementation of controls to mitigate this risk of Denial of Service (DoS) events targeting their services.

**Security controls provided by the HybridSystem** Not applicable.

### Residual controls to be addressed by the Agency

- The HybridSystem does not host online services. The Agency is responsible for the procurement and management of online services.
- The Agency is responsible for documenting the functionality and quality of services, how to maintain such functionality, and what functionality can be lived without during a DoS attack in relation to the Microsoft services used by the HybridSystem.

- The Agency is responsible for discussing DoS prevention and mitigation strategies with Microsoft as the service provider for Azure and 365 services.

## 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 .

### 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 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.
- Microsoft Azure and Office 365 services use Secure Hash Algorithm (SHA)-256 for hashing.
- Microsoft Azure and Office 365 services do not use Electronic Codebook Mode (ECM).
- Microsoft Azure and Office 365 services do not use Triple Data Encryption Standard (3DES).

**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 AACAs 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. If an Agency's risk profile requires a web proxy service, the DTA recommend the use of a certified SIG provider.

**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 controls relating to the web proxies as required by their risk profile.

## **Web content filters**

**Applicability to HybridSystem** The controls relating to web content filters are applicable to the HybridSystem as the solution leverages an Agency's SIG for web content filtering.

**HybridSystem compliance approach** The HybridSystem does not include a web content filtering service. If an Agency's risk profile requires a web content filtering service, the DTA recommend the use of a certified SIG provider.

**Security controls provided by the HybridSystem** Not applicable.

**Residual controls to be addressed by the Agency**

- The Agency is responsible for the controls relating to web proxies as required by their risk profile.

## **Content filtering**

**Applicability to HybridSystem** The controls relating to content filtering are applicable to the HybridSystem in relation to the filtering of email content.

**HybridSystem compliance approach** The HybridSystem leverages Office 365 capabilities including Office 365 ATP and EOP to inspect and manage email traffic. Content validation is not performed.



### **Security controls provided by the HybridSystem**

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

### **Residual controls to be addressed by the Agency**

- The Agency is responsible for any additional content filtering controls required based on their risk profile.

### **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 ATP to assist with the inspection and auditing of data transfer to and from the HybridSystem endpoints. Event logs are generated when data is transferred to external media from a Windows 10 endpoint.

### **Security controls provided by the HybridSystem**

- Defender ATP 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.