Australian Government
Digital Transformation Agency

Blueprint System Security Plan

March 2020

Contents

Introduction

System Name

Blueprint.

System Overview

The Blueprint leverages the Information Security Registered Assessors Program (IRAP) assessed Microsoft Azure and Office 365 platforms and their associated services. The Blueprint includes the following components to improve the security posture of a target Agency:

- **Cloud identity** – Azure Active Directory (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.
- **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.

Note: The initial Blueprint is based on a cloud-only deployment of the Microsoft Modern Workplace, based on the Microsoft 365 E5 licensing tier. The Digital Transformation Agency (DTA) expect to augment the initial service offering with a hybrid model for larger Commonwealth entities with complex or substantially on-premises environments.

System Classification

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

System Purpose and Scope

The Blueprint is intended to achieve a protected standard and raise Australian Government agencies cyber security posture. The Blueprint details technology and configuration settings to deploy a cloud only Microsoft 365 solution for agencies planning a new ‘greenfield’ deployment.

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

System Boundary

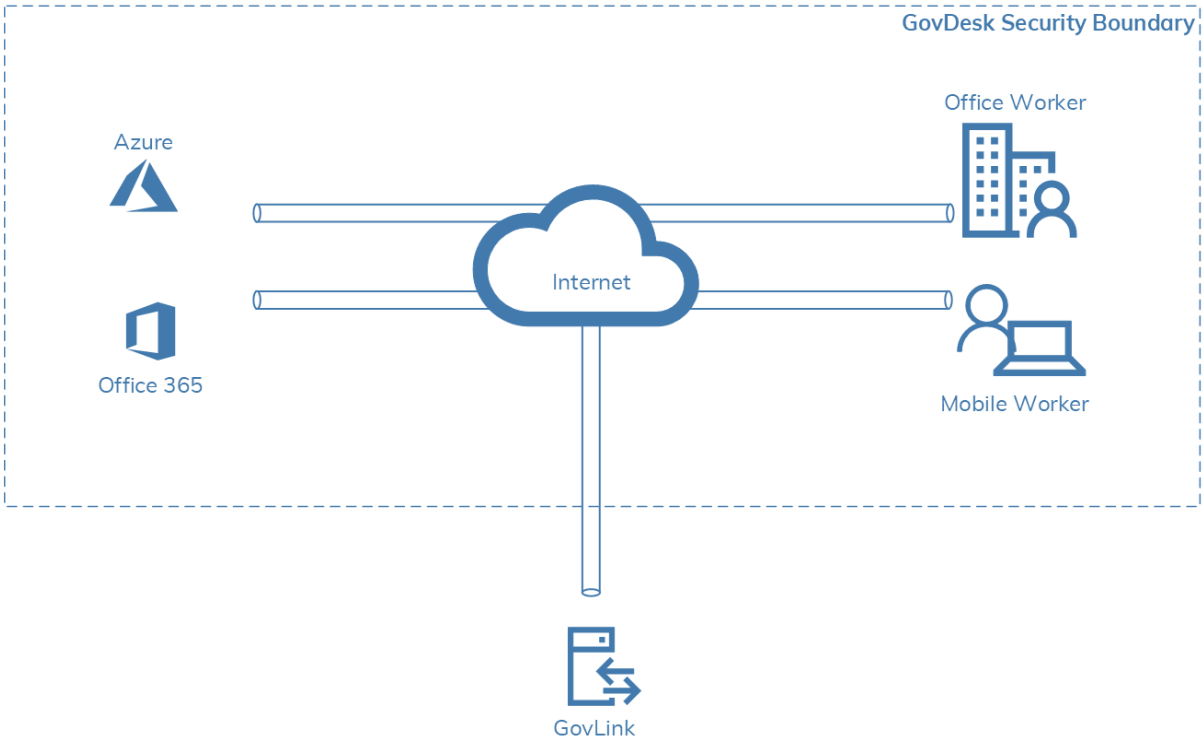
The boundary of the system is the Subscription level of the Microsoft 365 implementation. The tenancy and all Microsoft 365 components (including both Azure and Office 365 hosted services), the transport of data between the endpoint devices and cloud services along with the endpoint devices themselves 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:

- Azure (including Azure AD)
- Multi-Factor Authentication (MFA)
- Subscription and its management
- Tenancy 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 Security Boundary



Document Purpose and Scope

The purpose of this System Security Plan (SSP) is to describe the security implementation of the Blueprint, 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 Blueprint operates securely, the security controls it provides, and the residual controls that must be addressed by an Agency.

For detailed information on how the Blueprint addresses specific controls in the ISM (October 2019 update), refer to the 'DTA - Blueprint - System Security Plan Annex (October 2019)'.

Overarching Security Policies

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

- The Australian Government ISM (October 2019) 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.

Related Security Documentation

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

- Blueprint – Executive Overview
- DTA – Workstation Detailed Design
- DTA – Platform Detailed Design
- DTA – Office 365 Detailed Design
- DTA – Blueprint – System Security Plan (this document)
- DTA – Blueprint – System Security Plan Annex
- DTA – Blueprint – Security Risk Management Plan
- DTA – Blueprint – Security Standard Operating Procedures
- DTA – Blueprint – Incident Response Plan

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 Blueprint, and includes the following[1]:

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

[1] Both IRAP assessment reports are available from Microsoft Service Trust Portal at https://servicetrust.microsoft.com/ViewPage/Australia

Risk Assessment

The results of the threat and risk assessment undertaken on the Blueprint are documented in the 'DTA – 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 Blueprint 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 Blueprint 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	Note: Azure AD is only PROTECTED when configured in accordance with the ACSC consumer guidance.
	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.
	Azure MFA	PROTECTED	N/A
	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	**Note**: Azure AD is only PROTECTED when configured in accordance with the ACSC consumer guidance.
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 Blueprint	For each chapter, the applicability relates to whether the Blueprint provides any technical, process or documentation that need to be assessed. The Blueprints 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.
Blueprint compliance approach	The compliance approach for the Blueprint is described in this section to provide: • The background and context for how the Blueprint address the controls in the chapter • To provide the Agency with information to assist in the assessment of the Blueprint
Security controls provided by the Blueprint	The specific technical, process or documentation that the Blueprint 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 Blueprint, then they are listed in this section.

Summary of Applicability

A summary of the applicability and responsibility for the controls presented in of each chapter of the for the Blueprint 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 Blueprint and the Agency consuming it.
Guidelines for Security Documentation	Applicable	The Blueprint provides system-specific documentation to be read in conjunction with the Agency's cyber security strategy.
Guidelines for Physical Security	Not Applicable	The Blueprint inherits the physical security controls which are implemented by Microsoft for Azure and Office 365 components.
Guidelines for Personnel Security	Not Applicable	The Agency is responsible for the personnel security as it relates to users of the Blueprint.
Guidelines for Communications Infrastructure	Not Applicable	The Agency is responsible for communications infrastructure leveraged by the Blueprint.
Guidelines for Communications Systems	Applicable	The Blueprint includes Microsoft Teams which provides video conferencing functionality.
Guidelines for Enterprise Mobility	Applicable	The Blueprint includes the management and use of mobile devices.
Guidelines for Evaluated Products	Applicable	The Blueprint includes Windows 10 which has been evaluated. Additionally, the Blueprint leverages Office 365 services which include evaluated products.
Guidelines for ICT Equipment Management	Not Applicable	The Blueprint 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 Management	Applicable	The Blueprint is responsible for restricting the use of unapproved media.
Guidelines for System Hardening	Applicable	Hardening of operating systems and applications included in the Blueprint is applicable.
Guidelines for System Management	Applicable	Management of Blueprint system components is applicable.

ISM Chapter	Applicability	Rationale
Guidelines for System Monitoring	Applicable	Monitoring of Blueprint system components is applicable.
Guidelines for Software Development	Not Applicable	The Blueprint is not designed to support software development activities.
Guidelines for Database Systems Management	Not Applicable	The Blueprint does not include the use of databases.
Guidelines for Email Management	Applicable	The Blueprint leverages Office 365 to provide email functionality.
Guidelines for Network Management	Applicable	The Blueprint is designed to run using 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 Using Cryptography	Applicable	The Blueprint makes use of cryptography to protect both data at rest and data in transit.
Guidelines for Gateway Management	Not Applicable	The Agency is responsible for the implementation of security controls relating to their email gateway.
Guidelines for Data Transfers and Content Filtering	Applicable	The Blueprint is responsible for implementing technical controls relating to data transfer and content filtering.

Cyber Security Roles

Chief Information Security Officer

Applicability to Blueprint

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

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

- The Agency must appoint a CISO.
- The Agency must provide strategic level guidance.

System Owners

Applicability to Blueprint

Not applicable as the Blueprint does not designate a system owner.

Blueprint compliance approach

The deployment of the Blueprint into an Agency's environment can be designated as a specific system, or it can form part of a broader system.
By default, the Blueprint is defined as a system and all documentation, including this SSP, is written in that context.

Security controls provided by the Blueprint

Not Applicable.

Residual controls to be addressed by the Agency

- The Agency must designate a System Owner for the Blueprint.

Cyber Security Incidents

Detecting Cyber Security Incidents

Applicability to Blueprint

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

Blueprint compliance approach

 implements technical controls and processes to assist with detecting cyber security incidents related to the system and enables controls and provides the necessary functional components for systems deployed within to leverage tools and services that can assist in detecting cyber security incidents.

Security controls provided by the Blueprint

- utilises Microsoft Defender Advanced Threat Protection (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

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 Blueprint.

Managing Cyber Security Incidents

Applicability to Blueprint

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

Blueprint compliance approach

implements technical controls and processes to assist with managing cyber security incidents related to the system and enables controls and provides the necessary functional components for systems deployed within to leverage tools and services that can assist in managing cyber security incidents.

Security controls provided by the Blueprint

- 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

Reporting Cyber security Incidents

Applicability to Blueprint

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

Blueprint compliance approach

The reporting requirements for cyber security incidents are an Agency responsibility.
implements technical controls and processes to assist with reporting cyber security incidents related to the system and enables controls and provides the necessary functional components for systems deployed within to leverage tools and services that can assist in reporting cyber security incidents.

Security controls provided by the Blueprint

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.

Outsourcing

Information Technology and Cloud Services

Applicability to Blueprint

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

Blueprint compliance approach

The Blueprint leverages Microsoft Azure and Office 365, which are both listed on the ACSC Certified Cloud Services List (CCSL)[2]. Since Azure and Office 365 were listed on the CCSL both platforms have been re-assessed by Shearwater and additional services have been included in the updated IRAP assessment scope. With the exception of Microsoft Defender ATP, all Blueprint services have been IRAP assessed.

Security controls provided by the Blueprint

- Microsoft cloud components, including Azure and Office 365, have been IRAP assessed and are currently on the CCSL. All services used by the Blueprint have been IRAP assessed with the exception of Microsoft Defender ATP.

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.

[2] *ASD Certified Cloud Services*. [January 2019]. Available at https://www.cyber.gov.au/irap/asd-certified-cloud-services

Security Documentation

Development and Maintenance of Security Documentation

Applicability to Blueprint

Development and maintenance of security documentation is applicable to the Blueprint.

Blueprint compliance approach

 provides security documentation that an Agency can review, approve and incorporate into the broader Agency-level security documentation.
 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 system and the security controls included.

Security controls provided by the Blueprint

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

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.

System-specific Security Documentation

Applicability to Blueprint

System-specific security documentation is applicable to the Blueprint.

Blueprint compliance approach

The Blueprint includes a suite of security and operational documentation that are logically connected and consistent.
The Blueprint 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 Blueprint

- provides SOPs for administrators and support staff to understand, monitor and operate the provided security controls.
- includes detailed design, configuration, operational and support documentation.
- 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 – Blueprint Incident Response Plan' that applies to into their Agency-wide IRP.

Physical Security

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

Applicability to Blueprint

Not applicable as the Blueprint 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.

Blueprint compliance approach

The Blueprint inherits physical security controls from the underlying Azure and Office 365 platforms but also provides controls to ensure that only authorised Azure locations and/or services are utilised.

Security controls provided by the Blueprint

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.

Personnel Security

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

Applicability to Blueprint

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

Blueprint compliance approach

 provides a role-based access control implementation and associated operations guide to enable an Agency to easily and securely control access, including privileged access, to Azure and Office 365 services.

Security controls provided by the Blueprint

- enforces a password policy including length, complexity and history requirements for Azure AD accounts.
- provides a framework for identity and access management for Azure and Office 365 resources.
- implements a comprehensive RBAC model for assigning privileges using the principle of least privilege.
- restricts access to administrative portals and tools to only authorised users and locations through Conditional Access policies.
- enforces the use of Azure AD authentication and MFA for access to Azure administrative interfaces through Conditional Access.
- provides SOPs for administrators and support staff to understand, monitor and operate the provided security controls.
- includes detailed design, configuration, operational and support documentation.
- provides security documentation for input into an Agency's security processes.

Residual controls to be addressed by the Agency

- The Agency is responsible for all personnel security controls.

Communications Infrastructure

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

Applicability to Blueprint

Not applicable as the Blueprint 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.

Blueprint compliance approach

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

Security controls provided by the Blueprint

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 Blueprint

This section is not applicable as the Blueprint does not include telephone systems.

Blueprint compliance approach

Not Applicable.

Security controls provided by the Blueprint

Not Applicable.

Residual controls to be addressed by the Agency

Not applicable.

Video Conferencing and IP Telephony

Applicability to Blueprint

This section is applicable as the Blueprint contains Microsoft Teams which provides video conferencing functionality.

Blueprint compliance approach

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

Security controls provided by the Blueprint

- 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 Blueprint

This section is not applicable as the Blueprint does not include fax machines or multifunction devices.

Blueprint compliance approach

Not Applicable.

Security controls provided by the Blueprint

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 Blueprint.

Enterprise Mobility

Mobile Device Management

Applicability to Blueprint

This section is applicable as the Blueprint includes mobile devices.

Blueprint compliance approach

The Blueprint leverages Microsoft Intune to provide both Mobile Device Management (MDM) 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' to maximise usability for the target users. The risk of lightly managed iOS devices is addressed in the DTA – Blueprint – SRMP at R17.

Security controls provided by the Blueprint

- Microsoft Intune provides MDM and MAM capability.
- The Blueprint does not include the use of privately-owned mobile devices. Only Agency-owned devices are enrolled and allowed to access data.
- provides Windows 10 for laptops which is hardened in accordance with ACSC guidance. also provides MDM for iOS but does not fully implement ACSC's guidance for PROTECTED.
- Microsoft BitLocker provides full disk encryption of 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.
- 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.
- 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 Blueprint permits direct connection to the internet for all devices as per the DTA's requirements.

Residual controls to be addressed by the Agency

- The Agency is responsible for developing a mobile device management policy in relation to the Blueprint.

Mobile Device Usage

Applicability to Blueprint

This section is applicable as may contain mobile devices.

Blueprint compliance approach

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

Security controls provided by the Blueprint

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 Blueprint.

Evaluated Products

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

Applicability to Blueprint

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

Blueprint 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[3]. The Blueprint 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 Blueprint

- The Blueprint 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 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.

[3] *Common Criteria Certifications*. [20.03.2019]. Available at https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-platform-common-criteria

ICT Equipment Management

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

Applicability to Blueprint

Not applicable as the Blueprint does not contain any ICT Equipment, 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.

Blueprint compliance approach

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

Security controls provided by the Blueprint

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 Blueprint.

Media Management

Media Usage

Applicability to Blueprint

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

Blueprint compliance approach

The Blueprint implements technical controls to restrict access to removeable media devices that may be connected to endpoints.

Security controls provided by the Blueprint

- Autorun is disabled for removable media via Intune policies.
- Only authorised devices that are whitelisted in Intune policies can be connected to 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 Blueprint.

Media Sanitisation

Applicability to Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

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

Media Destruction

Applicability to Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

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

Media Disposal

Applicability to Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

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

System Hardening

Operating System Hardening

Applicability to Blueprint

Operating system hardening is applicable to .

Blueprint compliance approach

The solution 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 to maintain the latest version of the operating system.

The solution will harden the operating system configuration using a combination of Intune policies to implement ACSC and vendor guidance. These Intune policies achieve the results that would traditionally be performed by group policies. 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 solution will install applications via Intune and not allow standard users the ability to install applications.

The solution will use Windows Defender Application Control (WDAC) to perform application whitelisting. WDAC is the latest system from Microsoft for whitelisting and works in a very similar manner to AppLocker. In addition to performing all of the 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 Blueprint 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 whitelisted devices.

Security controls provided by the Blueprint

- Windows 10 Semi-Annual Channel (SAC) is used as the SOE for the Blueprint.
- The 64-bit version of Windows 10 is used as the SOE for the Blueprint.
- 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.
- RBAC policy defines separate domain and local administrator roles. Standard users do not have permissions to install or uninstall software.
- WDAC provides application whitelisting functionality. A combination of hash, publisher certificate and path rules will be used by WDAC for whitelisting of applications. Both publisher and product names are used by WDAC for whitelisting of applications. WDAC writes to the local event log. Standard users cannot disable application whitelisting.
- File permissions prevent standard users from writing to locations that are whitelisted using path rules.
- Microsoft's recommended block rules[4] to prevent known WDAC bypasses are implemented.
- The 'Exploit protection' feature is enabled as part of the Blueprint Windows 10 SOE.
- Windows Defender Exploit Guard and Defender ATP provide HIPS functionality as part of the Blueprint Windows 10 SOE.
- Windows Defender Firewall is enabled as part of the Blueprint Windows 10 SOE.
- Defender Antivirus and Defender ATP provide antivirus including signature and heuristic-based detection. Reputation rating features are enabled.
- Intune provides device whitelisting and blacklisting by DeviceID or Device Class.

Residual controls to be addressed by the Agency

Not applicable.

Application Hardening

Applicability to Blueprint

Application hardening is applicable to .

Blueprint compliance approach

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

The Blueprint 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

[4] *Microsoft recommended block rules*. [09.04.2019]. Available at https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

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 solution 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 Blueprint

- All applications are supplied by Microsoft which has made a commitment to secure development. The Blueprint 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.
- 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 Blueprint endpoints. The United Kingdom Government provides guidance on hardening Chrome specifically which Agencies may choose to follow[5].

[5] *Browser Security Guidance: Google Chrome*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/380011/Browser_Security_Guidance_-_Google_Chrome.pdf

Authentication Hardening

Applicability to Blueprint

The authentication hardening section is applicable to .

Blueprint compliance approach

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

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

 provides security controls and an identity management framework that can be utilised to manage system access for systems deployed within . 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 solution uses a soft-token to reduce the need for purchase, distribution and management of hard-tokens.

 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 Blueprint

- Azure AD is configured to require all users to be authenticated before granting access.
- Azure MFA is enforced for all standard and privileged users.
- The Blueprint does not include remote access.
- MFA requires complex password and One Time Password (OTP) from Microsoft Authenticator App (soft token).
- Azure AD password complexity enforces a minimum character length of 14 characters.
- 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 Smart Lockout is configured to lock account after five failed logon attempts.
- The Agency is responsible for investigating repeated lockouts.
- 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 Blueprint.
- Credentials are stored within Azure AD. Azure AD Identity Protection is enabled to detected leaked passwords.

- The Blueprint Windows 10 SOE is configured with a screen saver after 15 minutes which requires users to re-authenticate.
- The Blueprint 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.

System Management

System Administration

Applicability to Blueprint

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

Blueprint compliance approach

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

All administration of the solution 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	https://securitycenter.windows.com
Cloud App Security portal	https://portal.cloudappsecurity.com
Azure portal (including Azure AD)	https://portal.azure.com
Microsoft 365 Compliance Center	https://compliance.microsoft.com
Microsoft 365 Security Center	https://security.microsoft.com
Office 365 homepage	https://portal.office.com

 protects access to these portals through authentication via Azure AD and enforcement of MFA and location-based policies through Conditional Access. Privileges within 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 Blueprint.

Security controls provided by the Blueprint

- 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 administration.

System Patching

Applicability to Blueprint

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 policies setting the frequency, installation options and reporting values.

Blueprint compliance approach

The Blueprint 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, provides configuration of which patches to apply, deferral periods, update behaviour and reporting.

Security controls provided by the Blueprint

- provides the types of updates that are applied to endpoints.
- configures the intervals for checking for new updates.
- provides the reporting of device status to determine which devices have received updates.
- The Blueprint 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 for the Blueprint Windows 10 SOE.
- Operating system patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE.
- Intune 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 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 Blueprint

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

Blueprint compliance approach

The Blueprint integrates with an Agency's existing change management process.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for all change management processes.

Data Backups

Applicability to Blueprint

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

Blueprint compliance approach

The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for data backups data and configurations stored in the Blueprint.

System Monitoring

Event Logging and Auditing

Applicability to Blueprint

The controls relating to the logging and auditing of events for components included in the Blueprint are applicable. The Blueprint does not include web applications, databases, Domain Name System (DNS) or proxy services, and therefore the controls relating to these components are not applicable.

Blueprint compliance approach

 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 are stored in a centralised storage account. 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 Blueprint

- 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 Blueprint 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.

Vulnerability Management

Applicability to Blueprint

Vulnerability management is not applicable to the Blueprint as it is an Agency's responsibility to develop a vulnerability management strategy and perform vulnerability assessments and penetration tests.

Blueprint compliance approach

Not applicable. Note, a Vulnerability Assessment (VA) has been undertaken by an independent third party of the Blueprint prior to the release of the Blueprint. Any vulnerabilities discovered during the VA were addressed and remediated prior to publication of the Blueprint.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for all vulnerability management controls.

Software Development

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

Applicability to Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

- The Agency is responsible for all application development controls but can leverage the 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 Blueprint

Not applicable as the Blueprint does not include any database servers, database management system software or databases.

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

Not applicable.

Email Management

Email Usage

Applicability to Blueprint

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

Blueprint compliance approach

The Blueprint provides the capability for users to apply protective markings to emails based on their classification.

The Blueprint does not include a proxy services and therefore non-approved webmail services are not blocked. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway (SIG) provider.

Security controls provided by the Blueprint

- The Blueprint 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 Blueprint users.
- Users are prevented from lowering the classification of emails.
- 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.

Email Gateways and Servers

Applicability to Blueprint

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

Blueprint compliance approach

The Blueprint leverages Exchange Online, part of Office 365, to email capability without the need to deploy traditional email servers and gateways. Native Exchange Online security capabilities are enabled to prevent against email-related threats such as spoofing and phishing. As required, and Exchange Online will route email 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 inspective of hyperlinks respectively, are enabled by the Blueprint. This provides email content filtering and expands on the default protections offered by Exchange Online Protection (EOP).

- ## Security controls provided by the Blueprint

- 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 Blueprint

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

Blueprint compliance approach

The Blueprint 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 Blueprint designs the interfaces between endpoints and services, including how data traverses' public networks such as the internet.

Security controls provided by the Blueprint

- 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 Blueprint.
- The Agency is responsible for implementing security controls within their email gateway.

Wireless Networks

Applicability to Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

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 Blueprint endpoints and Azure/Office 365 services.

Service Continuity for Online Services

Applicability to Blueprint

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

Blueprint compliance approach

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

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

- The Blueprint 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 denial-of-service attack in relation to the Microsoft services used by the Blueprint.
- The Agency is responsible for discussing denial-of-service attack prevention and mitigation strategies with Microsoft as the service provider for Azure and 365 services.

Using Cryptography

Cryptographic Fundamentals

Applicability to Blueprint

The controls relating to cryptographic fundamentals are applicable to the Blueprint.

Blueprint compliance approach

The Blueprint 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 Blueprint 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 stated that versions 1.0 and 1.1 are currently not supported and will become deprecated for Office 365 services from June 2020[6].

Security controls provided by the Blueprint

- The Blueprint uses Microsoft BitLocker for encryption leveraging AES which is an AACA.
- Microsoft BitLocker provides full disk encryption of 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.

[6] *Preparing for TLS 1.2 in Office 365 and Office 365 GCC*. [19.12.2019]. Available at https://docs.microsoft.com/en-us/office365/troubleshoot/security/prepare-tls-1.2-in-office-365

ASD Approved Cryptographic Algorithms

Applicability to Blueprint

The controls relating to AACAs are applicable to the Blueprint.

Blueprint compliance approach

The Blueprint leverage's Microsoft's implementation of AACAs in Azure and Office 365.

Security controls provided by the Blueprint

- 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 Blueprint

The controls relating to AACPs are applicable to the Blueprint.

Blueprint compliance approach

The Blueprint leverage's Microsoft's implementation of AACPs in Azure and Office 365.

Security controls provided by the Blueprint

- 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 Blueprint

The controls relating to TLS are applicable to the Blueprint.

Blueprint compliance approach

The Blueprint leverage's Microsoft's implementation of TLS in Azure and Office 365.

Security controls provided by the Blueprint

- 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 Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

Not applicable.

Secure/Multipurpose Internet Mail Extension

Applicability to Blueprint

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

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

Not applicable.

Internet Protocol Security

Applicability to Blueprint

The Internet Protocol Security (IPsec) controls are not applicable to .

Blueprint compliance approach

The Blueprint does not include the use of IPsec.

Security controls provided by the Blueprint

Not applicable

Residual controls to be addressed by the Agency

Not applicable.

Cryptographic System Management

Applicability to Blueprint

Cryptographic system management is not applicable to .

Blueprint compliance approach

The Blueprint does not include the use of Commercial Grade Cryptographic Equipment (CGCE) equipment.

Security controls provided by the Blueprint

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 Blueprint.

Gateway Management

Gateways

Applicability to Blueprint

The controls relating to gateways are applicable to the Blueprint as the solution may integrate with an Agency's existing email gateway.

Blueprint compliance approach

Not applicable as the Blueprint leverages an existing Agency capability where required.

Security controls provided by the Blueprint

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 Blueprint.

Cross Domain Solutions

Applicability to Blueprint

The cross-domain solutions section is not applicable as the Blueprint does not include any cross-domain solutions.

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

Not applicable.

Firewalls

Applicability to Blueprint

The Firewall controls are not applicable to .

Blueprint compliance approach

The Blueprint does not include firewalls for the use of separating official/classified and public networks.

Security controls provided by the Blueprint

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 Blueprint.

Diodes

Applicability to Blueprint

The diodes section is not applicable to as does not include any diodes or unidirectional gateways.

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

Not applicable.

Web Content and Connections

Applicability to Blueprint

The controls relating to web content and connections are applicable to the Blueprint as users can directly access online resources from endpoints.

Blueprint compliance approach

The Blueprint does not include a proxy service for managing web content and connections. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.

Security controls provided by the Blueprint

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 management of web content and connections are required by their risk profile.

Peripheral Switches

Applicability to Blueprint

The Peripheral Switches section is not applicable to as does not include any peripheral switches.

Blueprint compliance approach

Not applicable.

Security controls provided by the Blueprint

Not applicable.

Residual controls to be addressed by the Agency

Not applicable.

Data Transfers and Content Filtering

Data Transfers

Applicability to Blueprint

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

Blueprint compliance approach

 includes Microsoft Defender ATP to assist with the inspection and auditing of data transfer to and from endpoints. Protective markings for documents are not implemented by the Blueprint and therefore not protective marking checks are performed.

Security controls provided by the Blueprint

- Defender ATP will scan all data copied onto Blueprint Windows 10 devices.

Residual controls to be addressed by the Agency

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

Content Filtering

Applicability to Blueprint

The controls relating to content filtering are applicable to the Blueprint.

Blueprint compliance approach

The Blueprint 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 Blueprint

- 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.

Appendix A

Abbreviations and Acronyms

Table 5 details the abbreviations and acronyms used throughout this document.

Table 5 Abbreviations and Acronyms

Acronym	Meaning
3DES	Triple Data Encryption Standard
AACA	ASD Approved Cryptographic Algorithm
AACP	ASD Approved Cryptographic Protocol
ACE	ASD Cryptographic Evaluation
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
ATP	Advanced Threat Protection
Azure AD	Azure Active Directory
BIOS	Basic Input/Output System
CCSL	Certified Cloud Services List
CGCE	Commercial Grade Cryptographic Equipment
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DSA	Digital Signature Algorithm
DTA	Digital Transformation Agency
ECHD	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECM	Electronic Codebook Mode
EM+S	Enterprise Mobility + Security

Acronym	Meaning
EMET	Enhanced Mitigation Experience Toolkit
EOP	Exchange Online Protection
GCM	Galois Counter Mode
ICT	Information and Communications Technology
IPsec	Internet Protocol Security
IRAP	Information Security Registered Assessors Program
IRP	Incident Response Plan
ISM	Information Security Manual
LAN	Local Area Network
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MFD	Multifunction Device
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OLE	Object Linking and Embedding
OTP	One Time Password
PAW	Privileged Access Workstation
PFS	Perfect Forward Secrecy
PSPF	Protective Security Policy Framework
RBAC	Role Based Access Control
RSA	Rivest–Shamir–Adleman
SAC	Semi-Annual Channel
SHA	Secure Hash Algorithm
SIG	Secure Internet Gateway
SIP	Session Initiation Protocol
S/MIME	Secure/Multipurpose Internet Mail Extension
SoA	Statement of Applicability
SOE	Standard Operating Environment

Acronym	Meaning
SOP	Standard Operating Procedure
SPF	Sender Policy Framework
SRMP	Security Risk Management Plan
SRTP	Secure Real Time Protocol
SSH	Secure Shell
SSP	System Security Plan
TLS	Transport Layer Security
VA	Vulnerability Assessment
VLAN	Virtual Local Area Network
WDAC	Windows Defender Application Control