Australian Government
Digital Transformation Agency

Protected Utility Blueprint

Solution Overview

March 2020

dta

Contents

Introduction

Background

The DTA developed the Protected Utility Blueprint to enable Australian Government agencies to transition to a secure and collaborative Microsoft Office 365 platform. The solution is underpinned by proven technologies from the Microsoft Modern Workplace solution (Microsoft 365 including Office 365, Enterprise Mobility + Security, and Windows 10). The Blueprint design is delivered as three distinct documents:

- **Platform** – Provides technologies that underpin the delivery of the solution,
- **Workstation** – The client device, which is configured and managed by Microsoft Intune, and
- **Office 365** – Microsoft Office 365 productivity applications.

The Blueprints are accompanied by Configuration Guides and Security Documentation adhering to the Australian Cyber Security Centre (ACSC) PROTECTED requirements for Information and Communication Technology (ICT) systems handling and managing Government information. These artefacts provide a standard and proven Microsoft 365 solution aimed to fast track the adoption of the Microsoft Modern Workplace experience.

The following Blueprint documentation contains considerations for best practice deployment advice from the Australian Government Information Security Manual (ISM), relevant Microsoft hardening advice, the ACSC Essential Eight and the ACSC hardening guidelines for Microsoft Windows 10.

Associated Documents

Table 1 identifies the documents that were referenced during the creation of this overview.

Table 1 Associated Documentation

Name	Version	Date
ACSC - Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 20161	N/A	01/2020
ACSC - Hardening Microsoft Windows 10, version 1709, Workstations2	N/A	01/2020
Azure - ACSC Consumer Guide - Protected - 2018	N/A	08/2018
Australian Government Information Security Manual (June 2019)	N/A	10/2019

[1] https://www.cyber.gov.au/publications/hardening-microsoft-office-2016
[2] https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-build-1709

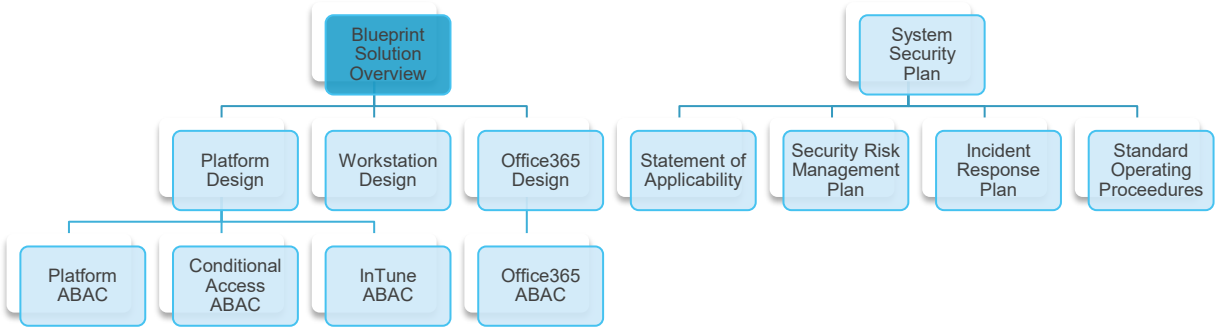
DTA – Platform Design	March	03/2020
DTA – Workstation Design	March	03/2020
DTA – Office 365 Design	March	03/2020
DTA – Office 365 – ABAC	March	03/2020
DTA – Platform – ABAC	March	03/2020
DTA – Intune Security Baselines – ABAC	March	03/2020
DTA – Software Updates – ABAC	March	03/2020
DTA – Intune Applications – ABAC	March	03/2020
DTA – Intune Enrolment – ABAC	March	03/2020
DTA – Conditional Access Policies – ABAC	March	03/2020
DTA – Intune Compliance – ABAC	March	03/2020
DTA – Intune Configuration – ABAC	March	03/2020
Protective Security Policy Framework – Sensitive and classified information3	2018.2	02/2018

Document Structure

This is the first document from the Blueprint set as shown in *Figure 1.* The Solution Overview is designed for a non-technical audience who are expected to have a general understanding of what they want to achieve from their IT system.

[3] https://www.protectivesecurity.gov.au/sites/default/files/pspf-infosec-08-sensitive-classified-information.pdf

Figure 1 - Blueprint Documentation Set



The document provides a high-level overview of the Blueprint, some of the key design decisions and the Blueprint Essential Eight compliance and maturity level. This document should be read first as the starting point for an agency journey. A summary of this document can be found in *Table 2.*

Table 2 Document Overview

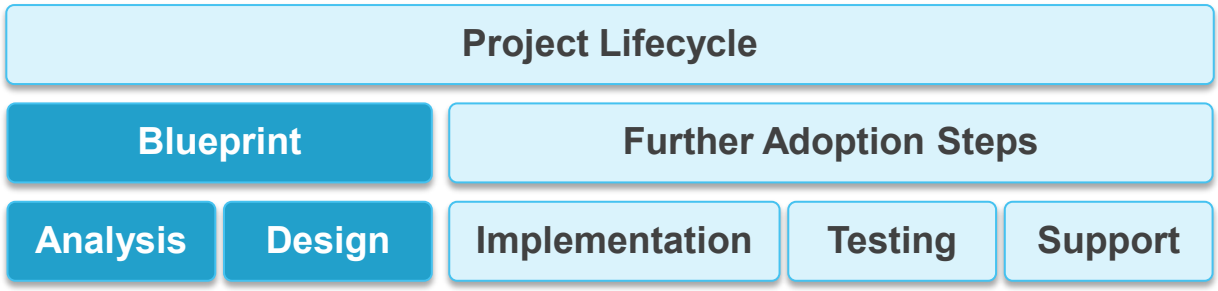
Heading	Description
Purpose of the Blueprint	This section describes how the Blueprint can accelerate the implementation of a secure Microsoft Modern Workplace solution
Where to Start	This section describes how an organisation should consume the Blueprint
Design Considerations	Factors affecting the design decisions, particularly the use of PROTECTED vs OFFICIAL
Blueprint Components	This section describes the components that make up the Blueprint
Security	This section provides an overview of the security documentation that is provided
Design Decisions	This section describes high-level design decisions for the solution
Essential 8 Compliance	This section describes the Blueprint's Essential Eight compliance and rationale

Blueprint

Purpose of the Blueprint

The Blueprint is provided to fast track agencies straight to implementation under the project lifecycle shown in *Figure 2*; saving agencies time and money.

Figure 2 - Blueprint position in project lifecycle



The Blueprint assumes that agencies are aiming to provide their workforce with secure, flexible and mobile solutions by pairing the Blueprint with mobile devices (laptops and iPhones) and onsite printing capabilities.

The Blueprint is designed with a security focus and employs native Microsoft technologies that provide seamless integration and improved end-user experience. Third-party software recommendations are provided where appropriate for Government use.

Where to start

The Solution Overview (this document) provides a general overview of the solution and is suitable for all audiences.

In order to fully understand the Blueprint, the following technical documents are provided:

- Windows 10 Design – Client component only.
- Office 365 Design – Exchange Online, SharePoint Online, OneDrive for Business and Teams.
- Platform Design – All supporting components for the Windows 10 and Office 365 components of the design including Intune.

The design documents provide a brief description of the components and the decision points that are required, the decision itself and the justification for that decision.

In order to implement the Blueprint, the following technical As Built As Configured (ABAC) documents are also provided:

- DTA Platform ABAC
- DTA Office 365 ABAC
- DTA Conditional Access Policies ABAC
- Intune ABACs
  - Intune Enrolment ABAC
  - Intune Compliance ABAC
  - Intune Configuration ABAC
  - Intune Security Baseline ABAC
  - Intune Software Updates ABAC
  - Intune Applications ABAC

The ABAC documents provide tables of settings that detail if a setting is turned on or off, set to a value, etc. The ABAC documents do not provide justification for individual settings.

Design Considerations

Information Management

Information Management approaches will be determined by each agency depending on their specific operational requirements. The following information management tools are available within the Blueprint, with a description of how each could be used in an agency implementation:

- **OneDrive** – Used for data that is relevant to the individual, automatically synchronised to the cloud so it is available anywhere and backed up. This data is likely to not yet be ready to share within a team (i.e. used for an initial draft).
- **Microsoft Teams** – When the data has matured to the point that it is ready to be shared in a Read/Write format with work colleagues and potentially external guests it should be moved to Microsoft Teams. Everyone that is a team member has read write access. People that do not need access are not a member of the team. In addition to document collaboration team members are able to chat, voice and video call, share screens and attend online meetings.
- **SharePoint Online** – When the data has further matured and now there are some people that need to access the data in a Read Only manner. At this point the data should be moved to SharePoint. SharePoint by default allows for document owners (full control), contributors (read write) and visitors (read only). Internal staff and external guests may be added to any of these groups according to the permission they require. Staff can still use the Microsoft Teams client to access the SharePoint site.

PROTECTED vs OFFICIAL

The Blueprint is based on a principle of 'engineered to PROTECTED' to enhance the cyber security postures of consuming agencies, irrespective of whether an agency seeks to attain a PROTECTED certification. The Blueprint details technology and configuration settings to deploy a secure, cloud-only Microsoft 365 solution for any agency planning a new deployment to attain a consistent cybersecurity posture across all environments, PROTECTED or below.

For agencies that wish to implement the Blueprint but do not need connectivity to other agencies at the PROTECTED level however, there are some components that may not be required to be implemented in the same way as a PROTECTED environment. These components are required for the transfer of PROTECTED information outside of an agency's environment and as such, their absence does not reduce the cybersecurity posture of this solution. Notwithstanding, their absence may inhibit an agency's ability to certify the solution to PROTECTED or interact with other agencies at a PROTECTED level.

Components:

- GovLink mail gateway
- Information Protection
- Collaboration components

Agencies that implement this Blueprint must undergo a certification process prior to handling PROTECTED data. While the cybersecurity posture of this Blueprint is consistent with a PROTECTED environment, agencies must not handle data above the classification of their environment.

GovLink

GovLink is a cost-effective solution to enable secure communication between Commonwealth entities across public infrastructure. GovLink (formerly FedLink) provides secure, encrypted and trusted communication across the internet. This allows the Commonwealth to transmit and receive information up to the security classification of PROTECTED. more information is available at https://www.finance.gov.au/government/whole-government-information-communications-technology-services/govlink.

For this Blueprint, PROTECTED email should be sent over GovLink. DTA is currently working with Microsoft and the Department of Finance to simplify an agency's ability to achieve this, however at the time of writing there is no native solution to allow a direct interface between the Office365/Exchange Online environment and the GovLink solution.

DTA can provide further advice to agencies and reference sites of how other Commonwealth entities have achieved this functionality. Future iterations of this Blueprint will provide more detail.

Information Protection

Information protection covers the application of labels to documents and emails according to the classification of the content of the document or email.

Within the Blueprint there are two options for labelling documents and emails. These are:

- Azure Information Protection (AIP) by Microsoft
- A third-party application

For organisations that send PROTECTED emails through a GovLink mail gateway, the labelling product and the gateway itself must support the inspection of the email headers. At the time of writing, Microsoft AIP labelling is not able to format the email headers in a manner that is consistent with what is required to send an email through GovLink and as such, a third-party application is needed.

DTA is currently working with Microsoft to investigate this further.

DTA is able to provide further advice to agencies and reference sites of how other Commonwealth entities have overcome these challenges. Future iterations of this Blueprint will provide more detail.

For organisations that do not need to send PROTECTED emails (and do not need to send emails through GovLink), the use of Microsoft AIP is recommended. The unified labelling client is built into Office 365 and the sensitivity labels are available for use in:

- **Emails** - thick client and Outlook Web Access (OWA).
- **Documents** - all office documents including the web versions of the applications.
- **Teams** - Labelling for Teams is currently in public preview and this will ensure that labels can be applied to Microsoft Teams, Office 365 Groups and SharePoint sites.

Note: At the time of writing (March 2020) there is a known issue[4] where with some tenants it is not possible to force clients to label documents even though this option is selected in the policy. Current work around is to assign a default label and users must then select the correct label. This will be monitored and updated as required.

Collaboration

Cross agency collaboration is possible between two consenting agencies using the Blueprint. Collaboration can take place using Microsoft Teams, SharePoint Online and Planner.

[4] https://support.office.com/en-us/article/known-issues-with-sensitivity-labels-in-office-b169d687-2bbd-4e21-a440-7da1b2743edc

Collaboration between organisations assessed at the same security level is relatively straightforward while collaboration between organisations with networks that have been assessed at different security levels presents additional considerations and risk. The additional risks and considerations are similar to those that already exist for organisations today with activities such as printing or faxing documents, or the risk of photos being taken of materials. These considerations will need to be assessed on a case by case basis and risks accepted by the Chief Information Security Officers (CISO).

Collaboration is initially controlled by whitelisting allowed domains. Individual users from those whitelisted external domains can then be invited individually to participate into Teams as guests. Details of how this will be configured will be covered in the DTA - Platform Design document and again in the Office 365 ABAC document.

The Microsoft Teams application provides the following collaboration functionality using a number of Microsoft supporting products.

- Individual and Group Chat / Instant Messaging
- Individual and Group Voice Call
- Individual and Group Video Call
- Voicemail
- Document collaboration both within Teams and also via SharePoint Online
- Screen and Application Sharing
- Online Meetings
- Email enabled Channels
- Organization Chart
- Planner

Secure Internet Gateway

A secure internet gateway is listed as a requirement in the PSPF (Protective Security Policy Framework), Section 11, Part C.4 for all Non-Corporate Commonwealth Entities (NCCEs) and best practice for all Commonwealth Corporate Entities (CCEs). At the time of writing and while noting that the DTA is undertaking a review of the existing SIG Policy, agencies must follow existing policies relating to SIG services. More information is available at https://www.cyber.gov.au/irap/asd-certified-gateways

Blueprint Components

The Blueprint is designed to be deployed by inhouse agency IT staff, third-party integrators or a managed service provider as a new deployment with no requirement for further design decisions or

design documentation. The Blueprint provides the information, rationale and configuration settings to allow an agency to implement these components.

The Blueprint is flexible enough to allow an agency to deviate from the Blueprint on any technology, licencing requirements, security, platform or design decisions noting that this may affect the security posture and will affect the security documentation set that compliments this Blueprint. If an agency is required to deviate from the Blueprint, a gap analysis should be performed.

In summary, the Blueprint includes the following components to achieve a secure desktop:

- **Cloud Identity** – Azure Active Directory configuration including Multi-Factor Authentication (MFA) and Conditional Access allowing log in from anywhere and appropriate security policies to be applied
- **Office 365** – Configuration of Exchange Online, SharePoint Online, Microsoft Teams and OneDrive for Business allowing cloud-based file storage
- **Device Management** – Management of security and configuration profiles for enrolled devices including the testing against security baselines and confirmation of security compliance. Some endpoint management of iOS devices due to the limitations of not utilising supervisor mode in addition to Windows 10 devices
- **Applications** – Delivery and configuration of applications appropriate to the user
- **Security Stack** – Security configuration of Office 365 and endpoint devices to achieve the Essential Eight compliance shown at the end of this document
- **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 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 deployment of the Microsoft Modern Workplace. The DTA expect to augment the initial service offering with a hybrid model for larger Commonwealth entities with complex or substantially on-premises environments. No Infrastructure as a Service (IaaS) components are required by this Blueprint.

Security

Accompanying the Blueprint is a set of security documentation to enable an agency to conduct a security assessment. These include:

- System Security Plan (SSP)

- Statement of Applicability[5] (SOA)
- Security Risk Management Plan (SRMP)
- Incident Response Plan (IRP)
- Security Standard Operating Procedures (SOPs)

[5] This is now referred to as the SSP Annex.

Design Decisions

The Blueprint is developed against a set of high-level design decisions to enable a secure Microsoft Modern Workplace user experience. These high-level decisions are summarised in *Table 3* below.

Table 3 Agency Design Decisions

Decision Point	Design Decision	Rationale / Justification
Identity	Azure Active Directory (Azure AD)	Blueprint is initially based on a cloud only deployment to provide guidance to agencies on an ideal state to move towards. Azure AD will be the identity source.
Azure AD Connect	Not Configured	Not required as there is no on-premises component. Note: Azure AD Connect will be required for hybrid implementations of the solution.
Azure AD Identity Protection	Configured	Azure AD Identity Protection is a tool that allows organizations 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 a utility for further analysis.
Azure AD Multi-Factor Authentication (MFA)	Configured	Azure AD MFA will be enabled to meet ACSC hardening and Essential Eight compliance. This is discussed in the Platform Design document.
Enterprise Collaboration	Microsoft Teams and SharePoint Online	Microsoft Teams and SharePoint Online will be utilised for Enterprise Collaboration.
Enterprise Email	Exchange Online	Exchange Online and Microsoft Outlook will be deployed for the Enterprise Email solution.
Enterprise File Storage	SharePoint / OneDrive	SharePoint and OneDrive will be deployed for Enterprise File Storage.
Conditional Access Policies	Configured	Conditional Access allows control of the devices and apps that allow connection to email and company resources depending on location.
Workstation	Government issued device	Only government issued devices will be configured.

Decision Point	Design Decision	Rationale / Justification
Remote Access	Limited access depending on the device	Conditional Access policies will limit what users can do while logging in remotely from an unmanaged (non-government issued) device, such as view and edit in the browser without an ability to download or print
Device Standard Operating Environment (SOE) Deployment	Configured	Device configuration will be deployed using Microsoft Autopilot and ongoing configuration will be controlled using Intune.
Workstation Policy Management	Configured	Workstation policy will be deployed and managed using Microsoft Intune.
Windows Updates and Patches	Configured	Configuration of Windows and third-party updates will be managed using Microsoft Intune.
Internet Connectivity	Direct Internet Connectivity	Connectivity is to be enabled so that agencies can work from in the office or at home.
Mail Gateway	Available if required	For organisations require email connectivity to PROTECTED networks this can be configured. For agencies that do not require email connectivity to PROTECTED systems this can be avoided reducing complexity and cost.

Essential Eight Compliance

This section summarises the Blueprint's compliance, justification and maturity level against the Essential Eight. It is important to note that any modifications outside of the Blueprint will require a gap analysis to determine the security implications.

The Essential Eight represents security guidance from the ACSC where they have prioritised a list of mitigation strategies to assist organisations in protecting their systems against a range of cyber threats.

Table 4 identifies the solutions being implemented specifically for the solution to address each strategy identified by ASD.

Table 4 Essential Eight Design Decisions

ASD Strategy	Solution	Justification	Maturity Level
Application Whitelisting	Windows Defender Application Control[6] (WDAC) managed by Intune.	Application whitelisting will prevent all non-approved applications (including malicious code) from executing. WDAC provides all the features of AppLocker with additional functionality and simpler management from within Intune. It is also possible to implement the latest recommended block rules from Microsoft.	3
Patch Applications	Intune used to patch applications on a regular basis.	As direct internet connectivity has been stipulated, applications will be set to auto update. Firmware can be update if an executable file is packaged and deployed via Intune. Note: 0.1 Full Time Equivalent (FTE) minimum is estimated to cover the work required.	3
Patch Operating Systems	Windows Update for Business and Intune to be used for desktop operating systems.	Multiple software update rings provide a staged approach to updates. Reporting is included Firmware can be update if it is an executable file, deployed via Intune. Note: 0.1 FTE minimum is estimated to cover the work required.	3
Configure Microsoft Office Macro Settings	Hardening to be implemented as per the ACSC via Intune.	Only signed macros will be enabled via Intune policies.	3

[6] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

ASD Strategy	Solution	Justification	Maturity Level
User Application Hardening	Hardening to be implemented as per the ACSC via Intune.	Web advertisements that are java or flash based will be blocked. 'Other' web adverts will not be controlled. Web browsers are configured to block or disable support for Flash content for Internet Explorer and Edge. Web browsers are configured to block Java from the Internet for Internet Explorer and Edge. Office 365 applications block flash content by default. Object Linking and Embedding will be disabled by Intune policy.	2
Restrict Administrative Privileges	Intune, Azure AD and Privileged Identity Manager (PIM) controls.	Restriction of administrative privileges for admin accounts will prevent adversaries using these accounts to gain full access to information and systems. WDAC policies are applied to admin users to prevent the ability to run email and web browsers. Admin users will log on with their normal accounts and then authenticate to the Office 365 tenant for management using their privileged account to administer the system.	3
Multi-factor Authentication	Multi-factor authentication solution is provided by Azure MFA for all remote users and administrators.	Stronger user authentication makes it harder for adversaries to access sensitive information and systems. MFA is enabled for all with a soft token. Hard tokens would require an IaaS server in Azure and will not be implemented.	2

ASD Strategy	Solution	Justification	Maturity Level
Daily Backups	Data redundancy and availability configured with native tools.	Configuration settings of Office 365 and Intune are backed up through the ABAC's. Documents, Desktops and Pictures are redirected to OneDrive using Windows Known Folders providing a backup of data to the cloud. Office 365 data is replicated by Microsoft to at least two geographically dispersed data centres. Exchange Online has a recover deleted items from server option. Cloud based files have Recycle bin and Restore options in addition to retention policies. Retention policies are created that ensure that data is retained forever for: • Exchange • SharePoint • OneDrive • Office 365 Groups • Skype for Business • Exchange Public Folders • Teams channel messages • Teams chats Workstation configuration is stored in Intune. (AutoPilot rebuild).	2