Australian Government

Digital Transformation Agency

Blueprint Security Risk Management Plan

March 2020

dta

Contents

Executive Summary

This Security Risk Management Plan (SRMP) has been developed to demonstrate the reduction in risk that can be achieved by implementing the Blueprint to secure access to Microsoft Office 365 services from Windows 10 endpoints and iOS mobile devices.

Each risk has been assessed in the context of the controls implemented by the Blueprint directly, those implemented by Microsoft as part of the Office 365 service, as well as those that are expected to be implemented by Australian Government Agencies that will leverage the Blueprint. The risk matrix, including definitions of likelihood and consequence, is provided at *Appendix B*. Agencies leveraging the Blueprint should review the risk ratings and align them to their internal risk management framework as applicable.

The residual risk to the Agency has been assessed as Medium. This can be further reduced to Medium-Low by implementing the additional treatments detailed in this document. It is an Agency's responsibility to accept the risks and associated residual risk rating as described within this document. A summary of the identified risks and the assessed risk ratings are listed in *Table 1*.

Table 1 Summary of Risk Events and Risk Ratings

Risk Event ID	Risk Event Description	Inherent Risk Rating	Residual Risk Rating	Target Risk Rating
R01	Inadequate privileged account management	High	Medium	Low
R02	Sensitive/classified email sent to unauthorised recipients	High	Medium	Medium
R03	Unauthorised access to data hosted within Office 365	High	Medium	Medium
R04	Malicious insider disables security capabilities	Medium	Medium	Medium
R05	Unskilled administrator misconfigures services	Medium	Medium	Low
R06	Components infected by malicious code	High	Medium	Low
R07	Unauthorised access to email on Exchange Online	High	Medium	Medium
R08	Denial of service attacks	High	Medium	Low
R09	Cyber security incident not detected	High	Medium	Medium
R10	Inability to recover from a data loss event	Medium	Low	Low
R11	Operating System vulnerability allows exploitation	High	Medium	Medium
R12	Application vulnerability allows exploitation	High	Medium	Medium
R13	Attacker bypasses application whitelisting capability	High	Medium	Medium
R14	Password spray attack directed at Azure AD	High	Medium	Medium
R15	Lack of availability due to cloud service provider outage	Medium	Low	Low

Risk Event ID	Risk Event Description	Inherent Risk Rating	Residual Risk Rating	Target Risk Rating
R16	Privileged Access Workstations not implemented for administration	High	Medium	Medium
R17	Mobile device compromised	High	High	High
R18	Use of un-certified cloud services creates exposures	High	Medium	Medium
R19	Use of un-assessed cloud services creates exposures	High	Medium	Medium

OFFICIAL:Sensitive

Introduction

Overview

This SRMP has been prepared by the DTA to support Agencies planning to leverage the Blueprint. The document demonstrates the controls implemented by the Blueprint that reduce the risk of leveraging Office 365 up to and including PROTECTED[1] security classified information.

Purpose

The purpose of this SRMP is to identify the risks and the residual risk to an Agency implementing the Blueprint Office 365 PROTECTED system.

Scope

The scope of this SRMP is limited to those threats and risks specific to the use of Office 365 as part of the Blueprint.

The Microsoft Office 365 service is addressed in the Information Security Registered Assessors Program (IRAP) report therefore risks specific to the underlying Office 365 service are not reassessed by this SRMP.

Agencies should make themselves aware of any risks identified in the IRAP assessment that have been inherited by the Blueprint.

Methodology

The assessment of the threats and risks presented in this SRMP has been performed in accordance with industry best practice in line with AS/NZS ISO 31000:2009. The risk matrix that was used in the assessment of risk ratings is included in this document at *Appendix B*.

[1] PROTECTED is used thought the document to describe the maximum security classification of information able to be managed by the system. Where PROTECTED is used, the security markings described by the Protective Security Policy Framework (PSPF) such as OFFICIAL and OFFICIAL: Sensitive are inferred.

Risk Assessment

Assessment Details

Detailed assessment of the risks to the operation of the system are outlined in the following tables which demonstrate the controls required to manage risks within the solution. All risk ratings have been updated to align with the risk matrix identified in *Appendix B*.

Table 2 Inadequate privileged account management

Risk Event ID R01	**Risk Event Description** Inadequate privileged account management
Risk Overview	If a privileged account were to be compromised, the environment could be accessed by staff without a legitimate need to know. Once inside, the unauthorised user could use the account to make malicious changes, such as the addition, alteration or deletion of data. Depending on the nature of the account used, the unauthorised user could bring down the environment.
Assets Affected	• Entire Azure tenant and Office 365 components
Threat Sources	• Adversarial – Individual – Trusted Insider, Insider, Outsider • Unintentional – Agency system administrator

Threat Events	• Obtain unauthorised access to:
	  ○ Deny access to agency information to authorised users
	  ○ Modify agency information and making the integrity of the information unviable or no longer trustworthy Obfuscate adversary actions
	• Obtain information by opportunistically stealing or scavenging information systems/components
	• Compromise organisational information systems to facilitate exfiltration of data/information
	• Obtain sensitive and or classified information via exfiltration

Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Risk Event ID R01	**Risk Event Description** Inadequate privileged account management

Ongoing and Completed Treatments	• Agency treatments
	  ○ Agency IT Security Policy for authorised staff to not provide privileged access to unauthorised staff and not allow logging in using service accounts
	  ○ Administrative break glass accounts will only be utilised when no other privileged account can be utilised
	  ○ Approval process to obtain a privileged user account
	  ○ Training to agency nominated system administrators
	• Treatments
	  ○ Conditional Access enforces Multi-Factor Authentication (MFA) for all privileged users
	  ○ Azure AD Identity Protection configured to alert on detected identity-based and sign-in risks
	  ○ Azure AD Privileged Identity Management (PIM) provides Just-In-Time (JIT) privileged access
	  ○ The solution leverages built-in Azure AD / Office 365 Role Groups to implement a robust Role-Based Access Control (RBAC) model
	  ○ All Azure AD and Office 365 logs are centralised into a single Log Analytics workspace
	  ○ Emergency access accounts are configured in accordance with Microsoft best practice to prevent administrators from being locked-out of Azure services[2]

Residual Likelihood	1 – Rare
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	• An annual audit of privileged accounts is performed by the Agency leveraging Azure AD access reviews • Forward logs to a Security Information and Event Management (SIEM) solution • Administrator training provided for specific technologies utilised within the Blueprint • Agency training for security and system administrators for the use of Security Centre / Sentinel • Monitoring of events within Security Centre / Sentinel
Target Likelihood	1 – Rare
Target Consequence	2 – Minor
Target Risk Rating	1 – Low

[2] *Manage emergency access accounts in Azure AD*. [08.11.2019]. Available at https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access

Table 3 Sensitive/classified email sent to unauthorised recipients

Risk Event ID R02	**Risk Event Description** Sensitive/classified email sent to unauthorised recipients
Risk Overview	A user sends an OFFICIAL: Sensitive or PROTECTED classified mail/attachment, or personal information (as defined by the Privacy Act 1988) to an authorised recipient resulting in a data spill.
Assets Affected	• OFFICIAL: Sensitive and PROTECTED data • Personal information
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Unintentional – General user
Threat Events	• Cause disclosure by spilling sensitive and or classified information to a system and or person not authorised to view or handle the information
Inherent Likelihood	4 – Likely
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Agency treatments
	  ○ All email transits via a gateway mail server which enforces email security classification label checking
	  ○ User awareness training to staff
	• Treatments
	  ○ Protective markings applied to email based on the classification of the content of emails, including attachments

Residual Likelihood	2 – Unlikely
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	• Implement a document security classification labelling solution • Implement an automated security classification labelling solution for emails based on the classification of attachments • Data spill processes and procedures are developed and regularly tested
Target Likelihood	1 – Rare
Target Consequence	3 – Moderate
Target Risk Rating	2 – Medium

Table 4 Unauthorised access to data hosted within Office 365

Risk Event ID R03	**Risk Event Description** Unauthorised access to data hosted within Office 365
Risk Overview	An unauthorised user attempts to access data hosted within Microsoft's Office 365 cloud services, including Exchange Online, OneDrive for Business, SharePoint Online, and Teams to gain access to PROTECTED data. The attacker may attempt to use either stolen or guessed credentials or attempt to introduce malicious code into one or more Office 365 services.
Assets Affected	• PROTECTED data within the tenant
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider (including Microsoft support staff) • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State

Threat Events	• Compromise organisational information systems to facilitate exfiltration of data/information
	• Obtain sensitive and or classified information via exfiltration
	• Obtain unauthorised access to:
	  ○ Deny access to agency information to authorised users
	  ○ Modify agency information and making the integrity of the information unviable or no longer trustworthy

Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Risk Event ID R03	**Risk Event Description** Unauthorised access to data hosted within Office 365

Ongoing and Completed Treatments	• Native Office 365 treatments
	  ○ Office 365 service IRAP assessed up to a PROTECTED level
	  ○ All Office 365 traffic is protected using Transport Layer Security (TLS)
	  ○ Exchange Online Protection (EOP) provides built in protection for Exchange Online mailboxes
	  ○ Microsoft's Cyber Defence Operations Centre helps protect, detect, and respond to Office 365 cloud service threats in real time
	• Treatments
	  ○ Password complexity is enforced in line with Information Security Manual (ISM) standards
	  ○ Conditional Access enforces MFA for all users and administrators
	  ○ Office 365 audit logging enabled to provide the ability to audit actions undertaken within the Office 365 services
	  ○ Office 365 Advanced Threat Protection (ATP) Safe Links, ATP Safe Attachments, ATP for SharePoint Online, OneDrive for Business, and Microsoft Teams and ATP Anti-Phishing capabilities enabled to reduce the likelihood of malicious code infiltrating
	  ○ Microsoft Cloud App Security (MCAS) enabled and app connectors and policies configured to detect risky behaviours, violations, or suspicious data points and activities within Office 365
	  ○ Sender Policy Framework (SPF), Domain based Message Authentication, Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) records are configured to mitigate spoofing of emails being sent into the organisation
	  ○ Office 365 services are only utilised within Australian regions

Residual Likelihood	2 – Unlikely
Residual Consequence	2 – Minor
Residual Risk Rating	2 – Medium
Proposed Treatments	None
Target Likelihood	2 – Unlikely
Target Consequence	2 – Minor
Target Risk Rating	2 – Medium

Table 5 Malicious insider disables security capabilities

Risk Event ID R04	**Risk Event Description** Malicious insider disables security capabilities
Risk Overview	An unauthorised user (malicious insider) attempts to disable cloud-based security capabilities (e.g., Azure MFA) increasing the risk of further exploitation.
Assets Affected	• All cloud based infrastructure
Threat Sources	• Adversarial – Individual – Trusted Insider, Insider, or Privileged Insider
Threat Events	• Functionality of security features are reduced or disabled • Level of security monitoring is limited or disabled • Allow malicious activity to be undetected
Inherent Likelihood	2 – Unlikely
Inherent Consequence	3 – Moderate
Inherent Risk Rating	2 – Medium

Ongoing and Completed Treatments	• Treatments
	  ○ Azure AD Identity Protection configured to alert on detected identity-based and sign-in risks
	  ○ Azure AD PIM provides JIT privileged access
	  ○ Leverage built-in Azure AD / Office 365 Role Groups to implement a robust RBAC model
	  ○ All Azure AD and Office 365 logs are centralised into a single Log Analytics workspace

Residual Likelihood	1 – Rare
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	1 – Rare
Target Consequence	3 – Moderate
Target Risk Rating	2 – Medium

Table 6 Unskilled administrator misconfigures services

Risk Event ID R05	**Risk Event Description** Unskilled administrator misconfigures services
Risk Overview	An authorised administrator misconfigures services increasing the risk of further exploitation. This may be due to a misunderstanding of the functionality of specific Azure or Office 365 service due to a lack of training or insufficient procedural documentation.
Assets Affected	• All infrastructure
Threat Sources	• Accidental – Privileged User/Administrator
Threat Events	• Functionality of security features are reduced • Level of security monitoring is limited
Inherent Likelihood	3 – Possible
Inherent Consequence	2 – Minor
Inherent Risk Rating	2 – Medium

Ongoing and Completed Treatments	• Treatments
	  ○ Azure AD Identity Protection configured to alert on detected identity-based and sign-in risks
	  ○ Azure AD PIM provides JIT privileged access
	  ○ Leverage built-in Azure AD / Office 365 Role Groups to implement a robust RBAC model
	  ○ All Azure AD and Office 365 logs are centralised into a single Log Analytics workspace
	  ○ Standard Operating Procedures (SOPs) are provided for administrators

Residual Likelihood	2 – Unlikely
Residual Consequence	2 – Minor
Residual Risk Rating	2 – Medium
Proposed Treatments	• Administrator training provided for specific technologies utilised within the Blueprint • Agency training for security and system administrators for the use of Security Centre / Sentinel • Monitoring of events within Security Centre / Sentinel
Target Likelihood	1 – Rare
Target Consequence	1 – Minimal
Target Risk Rating	1 – Low

Table 7 components infected by malicious code

Risk Event ID R06	**Risk Event Description** Components infected by malicious code
Risk Overview	Malicious code introduced to the environment by one or more vectors leading to the loss of availability or integrity of the solution.
Assets Affected	• All infrastructure (including both cloud services and endpoints)
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Deliver known malicious to internal organisational information systems (e.g. virus via email including spam, whaling, spear phishing etc.) • Deliver modified malicious code to internal organisational information systems • Deliver targeted malicious for control of internal systems and exfiltration of data • Insert untargeted malicious into downloadable software and/or into commercial information technology products • Email contains unknown (zero day) exploit which is undetected by Microsoft security systems and delivered to the user.
Inherent Likelihood	4 – Likely
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Risk Event ID R06	**Risk Event Description** Components infected by malicious code

Ongoing and Completed Treatments	• Native Office 365 treatments
	  ○ EOP provides built-in protection for Exchange Online mailboxes
	  ○ Microsoft's Cyber Defence Operations Centre helps protect, detect, and respond to Office 365 cloud service threats in real time
	• Treatments
	  ○ Windows Defender ATP is enabled to provide reporting, pre-breach protection, post-breach detection, automation, and response on hosted desktops and platform servers
	  ○ Office 365 ATP Safe Links, ATP Safe Attachments, ATP for SharePoint Online, OneDrive for Business, Microsoft Teams, and ATP Anti-Phishing capabilities enabled to reduce the likelihood of malicious code infiltrating the environment
	  ○ Windows Defender Application Control (WDAC) provides application whitelisting functionality to block unauthorised executables from running
	  ○ Windows Defender Exploit Guard (WDEG) 'exploit protection' feature is enabled
	  ○ Hardening of Windows 10 desktops including application whitelisting to ACSC recommended practices

Residual Likelihood	2 – Unlikely
Residual Consequence	2 – Minor
Residual Risk Rating	2 – Medium
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	1 – Rare
Target Consequence	2 – Minor
Target Risk Rating	1 – Low

Table 8 Unauthorised access to email on Exchange Online

Risk Event ID R07	**Risk Event Description** Unauthorised access to email on Exchange Online
Risk Overview	An unauthorised user attempts to access email within mailboxes hosted in Exchange Online which may expose sensitive and or security classified data. This may be attempted using leaked or guessed credentials, or by attempting to intercept legitimate authentication traffic in transit.
Assets Affected	• Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State

Threat Events	• Compromise organisational information systems to facilitate exfiltration of data/information
	• Obtain security classified and or sensitive information via exfiltration
	• Obtain unauthorised access to:
	  ○ Deny access to agency information to authorised users
	  ○ Modify agency information and making the integrity of the information unviable or no longer trustworthy
	• Commit CEO fraud and or Business Email Compromise (BEC)

Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Treatments
	  ○ Password complexity is enforced in line with ISM standards
	  ○ Conditional Access enforces MFA for all users and administrators
	  ○ Conditional Access blocks access to Office 365 from external networks
	  ○ Legacy authentication blocked via Conditional Access policies

Residual Likelihood	1 – Rare
Residual Consequence	3 – Moderate
Residual Risk Rating	2 - Medium
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	1 – Rare
Target Consequence	3 – Moderate

Risk Event ID	Risk Event Description
R07	Unauthorised access to email on Exchange Online
Target Risk Rating	2 – Medium

Table 9 Denial of service attacks

Risk Event ID R08	**Risk Event Description** Denial of service attacks
Risk Overview	An external attacker attempts to disrupt availability by launching a Denial of Service (DoS) attack targeting one or more public facing IP addresses (including Microsoft services).
Assets Affected	• All infrastructure • Agency gateway (if utilised)
Threat Sources	• Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Conduct simple DoS attacks • Conduct Distributed Denial of Service (DDoS) attacks • Conduct targeted DoS attacks
Inherent Likelihood	4 – Likely
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Agency treatments
	  ○ Basic DoS protection is available within the Agency gateway
	• Native Microsoft treatments
	  ○ Microsoft provide underlying DDoS protection for Office 365 services[3]

Residual Likelihood	2 – Unlikely
Residual Consequence	2 – Minor
Residual Risk Rating	2 – Medium
Proposed Treatments	• Enhance DoS/DDoS protection within the Agency's gateway
Target Likelihood	1 – Rare
Target Consequence	2 – Minor
Target Risk Rating	1 - Low

[3] Defend Against Denial-of-Service Attacks in Office 365. [21.09.2019]. Available at https://docs.microsoft.com/en-us/office365/enterprise/office-365-defending-against-denial-of-service-attacks-overview

Table 10 Cyber security incident not detected

Risk Event ID R09	**Risk Event Description** Cyber security incident not detected
Risk Overview	An intrusion is not detected leading to a threat of malicious activity and possible compromise of sensitive and or security classified data and services.
Assets Affected	• All infrastructure • Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State

Threat Events	• Compromise organisational information systems to facilitate exfiltration of data/information
	• Obtain sensitive information via exfiltration
	• Obtain unauthorised access to:
	  ○ Deny access to agency information to authorised users
	  ○ Modify agency information and making the integrity of the information unviable or no longer trustworthy
	• Coordinate a campaign that spreads attacks across organisational systems from existing presence

Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Native Office 365 treatments
	  ○ Microsoft's Cyber Defence Operations Centre helps protect, detect, and respond to Office 365 cloud service threats in real time
	• Treatments
	  ○ Windows Defender ATP is enabled to provide reporting, pre-breach protection, post-breach detection, automation, and response on hosted desktops and platform servers
	  ○ MCAS enabled and app connectors and policies configured to detect risky behaviours, violations, or suspicious data points and activities within Office 365
	  ○ All Azure AD and Office 365 logs are centralised into a single Log Analytics workspace

Residual Likelihood	1 – Rare
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium

Risk Event ID R09	**Risk Event Description** Cyber security incident not detected
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre / Sentinel • Monitoring of events within Security Centre / Sentinel
Target Likelihood	1 – Rare
Target Consequence	3 – Moderate
Target Risk Rating	2 – Medium

Table 11 Inability to recover from a data loss event

Risk Event ID R10	**Risk Event Description** Inability to recover from a data loss event
Risk Overview	The failure of backup procedures leading to the inability to restore critical system components and information when data loss occurs. This risk takes into account the ISM controls relating to 'Data backups' that are not implemented as part of the solution.
Assets Affected	• All infrastructure • Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Availability of Agency information and systems • Cause integrity loss by polluting or corrupting critical data • Cause integrity loss by injecting false but believable data into organisational information systems • Data corruption or accidental deletion
Inherent Likelihood	2 – Unlikely
Inherent Consequence	2 – Minor
Inherent Risk Rating	2 – Medium

Ongoing and Completed Treatments	• Agency treatments
	  ○ Ongoing operational procedures to monitor backups
	• Treatments
	  ○ Configuration settings of Office 365 are backed up through the As-Built As-Configured (ABAC) documentation
	  ○ Documents, Desktops, Pictures on endpoints are redirected to OneDrive using Windows Known Folders providing a backup of data to the cloud
	  ○ Cloud based files have Recycle bin and Restore options
	  ○ Exchange Online has a recover deleted items from server option
	  ○ Retention policies will be created that ensure that 3 months of data is retained for Office 365 services
	  ○ Workstation configuration is stored in Intune
	  ○ SOPs provided for administrators

Residual Likelihood	1 – Rare
Residual Consequence	2 – Minor
Residual Risk Rating	1 – Low

Risk Event ID R10	**Risk Event Description** Inability to recover from a data loss event
Proposed Treatments	• Implement an offline backup solution in the event Office 365 services are unavailable • Data backup and recovery processes and procedures are developed and regularly tested
Target Likelihood	1 – Rare
Target Consequence	2 – Minor
Target Risk Rating	1 – Low

OFFICIAL:Sensitive

Table 12 Operating System vulnerability allows exploitation

Risk Event ID R11	**Risk Event Description** Operating System vulnerability allows exploitation
Risk Overview	Security vulnerabilities are discovered within the operating system versions utilised by the solution allowing exploitation.
Assets Affected	• Fortress Cloud hosted desktops and platform servers
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Exploit recently discovered vulnerabilities • Exploit vulnerabilities on internal organisational information systems • Exploit vulnerabilities using zero-day attacks • Craft attacks specifically based on deployed information technology environment
Inherent Likelihood	4 – Likely
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Agency treatment
	  ○ The Agency's support team will monitor patching and perform manual remediation as required
	• Treatment
	  ○ Windows Update for Business and Microsoft Intune are enabled and configured to automatically update Windows 10 on endpoints
	  ○ Multiple software update rings provide staged approach to updates
	  ○ Intune can deploy firmware patches as executable files as required

Residual Likelihood	2 – Unlikely
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	2 – Unlikely
Target Consequence	3 – Moderate

Risk Event ID	Risk Event Description
R11	Operating System vulnerability allows exploitation
Target Risk Rating	2 – Medium

Table 13 Application vulnerability allows exploitation

Risk Event ID R12	**Risk Event Description** Application vulnerability allows exploitation
Risk Overview	Security vulnerabilities are discovered within applications utilised by the solution allowing exploitation.
Assets Affected	• Applications
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Exploit recently discovered vulnerabilities • Exploit vulnerabilities on internal organisational information systems • Exploit vulnerabilities using zero-day attacks • Craft attacks specifically based on deployed information technology environments
Inherent Likelihood	4 – Likely
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Agency treatment
	  ○ The Agency's support team will monitor patching and perform manual remediation as required
	• Treatments
	  ○ Intune used to patch applications on a regular basis
	  ○ Windows Defender Firewall enabled for inbound connections
	  ○ User Account Control (UAC) enabled to enforce the elevation of privileges to help prevent vulnerability exploitation
	  ○ WDEG 'exploit protection' feature is enabled
	  ○ Local administrator account renamed and disabled via Intune policy

Residual Likelihood	2 – Unlikely
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	2 – Unlikely
Target Consequence	3 – Moderate

Risk Event ID R12	**Risk Event Description** Application vulnerability allows exploitation
Target Risk Rating	2 – Medium

Table 14 Attacker bypasses application whitelisting capability

Risk Event ID R13	**Risk Event Description** Attacker bypasses application whitelisting capability
Risk Overview	An attacker attempts to bypass the whitelisting restrictions enforced on endpoints utilised.
Assets Affected	• Desktops and servers
Threat Sources	• Accidental – Privileged User/Administrator • Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Compromise software of organisational critical information systems
Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Treatments
	  ○ WDAC provides application whitelisting functionality to block unauthorised executables from running
	  ○ WDAC policies configured centrally from Intune
	  ○ WDEG ‘exploit protection’ feature is enabled
	  ○ Windows Defender ATP is enabled to provide reporting, pre-breach protection, post-breach detection, automation, and response on hosted desktops and platform servers

Residual Likelihood	2 – Unlikely
Residual Consequence	2 – Minor
Residual Risk Rating	2 – Medium
Proposed Treatments	• Forward logs to a SIEM solution • Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	2 – Unlikely
Target Consequence	2 – Minor
Target Risk Rating	2 – Medium

Table 15 Password spray attack directed at Azure AD

Risk Event ID R14	**Risk Event Description** Password spray attack directed at Azure AD
Risk Overview	An attacker attempts to gain access by attempting to logon using a number of different passwords against a crafted list of Azure AD accounts over a period of time.
Assets Affected	• All infrastructure • Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State
Threat Events	• Conduct login attempts/password guessing attacks
Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Agency treatments
	  ○ Mandatory security awareness training by the Agency to educate users on the importance of using strong passwords or passphrases
	• Treatments
	  ○ Conditional Access enforces MFA for all users and administrators
	  ○ Password complexity is enforced in line with ISM standards
	  ○ Azure AD Smart Lockout configured to lock out accounts for a period of time after a number of invalid attempts
	  ○ Azure AD Identity Protection configured to alert on detected identity-based and sign-in risks

Residual Likelihood	3 – Possible
Residual Consequence	2 – Minor
Residual Risk Rating	2 – Medium
Proposed Treatments	• Agency training for security and system administrators for the use of Security Centre • Monitoring of events within Security Centre
Target Likelihood	3 – Possible
Target Consequence	2 – Minor
Target Risk Rating	2 - Medium

Table 16 Lack of availability due to cloud service provider outage

Risk Event ID R15	**Risk Event Description** Lack of availability due to cloud service provider outage
Risk Overview	A major outage occurs to the cloud services causing the inability to provide services to the Agency.
Assets Affected	• Microsoft Azure, and Microsoft Office 365.
Threat Sources	• Environmental – Infrastructure Failure/Outage • Environmental – Natural or man-made disaster
Threat Events	• Network communications outage or contention • Interruption to cloud services • Earthquake, fire, flood, hurricane, or tornado • Force majeure
Inherent Likelihood	1 – Rare
Inherent Consequence	4 – Major
Inherent Risk Rating	2 – Medium

Ongoing and Completed Treatments	• Native Microsoft Cloud treatments
	  ○ Azure cloud services are available within multiple regions in Australia classified up to PROTECTED
	  ○ Office 365 services are available within multiple regions in Australia classified up to PROTECTED. Failover of the Office 365 services will be dependent on Microsoft's Service Level Agreement (SLA) for Office 365
	• Treatments
	  ○ The services utilised are available within multiple Azure regions (except any third-party solutions utilised, e.g. Agency gateway and GovLink)

Residual Likelihood	1 – Rare
Residual Consequence	2 – Minor
Residual Risk Rating	1 – Low
Proposed Treatments	None
Target Likelihood	1 – Rare
Target Consequence	2 – Minor
Target Risk Rating	1 - Low

Table 17 Privileged Access Workstations not implemented for administration

Risk Event ID R16	**Risk Event Description** Privileged Access Workstations not implemented for administration
Risk Overview	Privileged Access Workstations (PAWs) are not in scope. Administration of the system is undertaken by authorised privileged users by connecting from a PROTECTED level endpoint to PROTECTED level services and systems.
Assets Affected	• All infrastructure
Threat Sources	• Adversarial – Individual – Trusted Insider, Insider or Privileged Insider • Accidental – Privileged User/Administrator
Threat Events	• Obtain unauthorised access
Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Treatments
	  ○ Conditional Access only allows access to administrative portals from endpoints
	  ○ All endpoints are hardened using the Australian Cyber Security Centre (ACSC) guidance for Windows 10[4]
	  ○ Windows Defender ATP is enabled to provide reporting, pre-breach protection, post-breach detection, automation, and response on hosted desktops and platform servers
	  ○ WDAC provides application whitelisting functionality to block unauthorised executables from running
	  ○ WDEG 'exploit protection' feature is enabled
	  ○ Conditional Access enforces MFA for all privileged users
	  ○ Azure AD Identity Protection configured to alert on detected identity-based and sign-in risks

Residual Likelihood	2 – Unlikely
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	• Agency system administrators to have separate administration account from their normal user account for the management of O365 and Azure.
Target Likelihood	1 – Rare
Target Consequence	3 – Moderate
Target Risk Rating	2 - Medium

[4] *Hardening Microsoft Windows 10, version 1709*, Workstations. [November 2019]. Available at https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-build-1709

Table 18 Mobile device compromised

Risk Event ID R17	**Risk Event Description** Mobile device compromised
Risk Overview	An Apple iOS device used to access Sensitive and or security classified data is compromised as a result of the ACSC's Security Configuration Guide - Apple iOS 12 Devices (September 2019)[5] not being fully implemented due to the usability impacts. Note, the Blueprint does not include the use of devices using the Android operating system.
Assets Affected	• iOS devices • Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Adversarial – Individual – Outsider • Adversarial – Group – Established • Adversarial – Nation State • Unintentional – General user
Threat Events	• Obtain unauthorised access • Exploit recently discovered vulnerabilities • Theft or loss of device
Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

[5] *Security Configuration Guide* - Apple iOS 12 Devices. [September 2019]. Available at https://www.cyber.gov.au/publications/security-configuration-guide-apple-ios-12-devices

Risk Event ID R17	**Risk Event Description** Mobile device compromised

Ongoing and Completed Treatments	• Agency treatments
	  ○ Policy governing the use and management of mobile devices used to access classified information
	  ○ Awareness training for users with mobile devices
	• Treatments
	  ○ Partial implementation of the ACSC's Security Configuration Guide for iOS 12 devices:
	  (1) Supervised mode
	  (2) Long and complex alphanumeric device passcode
	  (3) Biometric device unlock disabled
	  (4) Management of built-in apps (e.g., iOS Camera and Books)
	  (5) Implementation of Intune App Protection policies
	  ○ Conditional Access policies require iOS devices to be compliant, using applications with modern authentication and MFA
	  ○ Conditional Access policies only allow access from specified countries
	  ○ Conditional Access policies block sign-ins that are determined to be high risk
	  ○ Intune enforces configuration policies for iOS devices including requirement for unlock code, device encryption (native iOS AES-256 encryption), minimum software version and jailbreak detection

Residual Likelihood	3 – Possible
Residual Consequence	3 – Moderate
Residual Risk Rating	3 – High
Proposed Treatments	None
Target Likelihood	3 – Possible
Target Consequence	3 – Moderate
Target Risk Rating	3 – High

Table 19 Use of un-certified cloud services creates exposures

Risk Event ID R18	**Risk Event Description** Use of un-certified cloud services creates exposures
Risk Overview	An administrator enables a cloud service for use with the Blueprint that is not currently listed on the Australian Signals Directorate (ASD) Certified Cloud Services List (CCSL). Note, this risk addresses those services that are provided by the Blueprint that are not currently listed on the CCSL, such as Defender ATP.
Assets Affected	• All cloud based infrastructure • Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Accidental – Privileged User/Administrator

Threat Events	• Obtain unauthorised access to:
	  ○ Deny access to agency information to authorised users
	  ○ Modify agency information and making the integrity of the information unviable or no longer trustworthy Obfuscate adversary actions
	• Obtain information by opportunistically stealing or scavenging information systems/components
	• Compromise organisational information systems to facilitate exfiltration of data/information
	• Obtain sensitive and or classified information via exfiltration

Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Risk Event ID R18	**Risk Event Description** Use of un-certified cloud services creates exposures

Ongoing and Completed Treatments	• Agency treatments
	  ○ Agency IT Security Policy for authorised staff to not enable new cloud services
	  ○ Approval process to obtain a privileged user account
	  ○ Training to Agency nominated system administrators
	• Treatments
	  ○ Leverage built-in Azure AD / Office 365 Role Groups to implement a robust Role-Based Access Control (RBAC) model minimising the number of users that can onboard a new service
	  ○ All cloud services included in the Blueprint have been assessed by the project team as part of the development of the Blueprint and the risk of each un-certified service considered against the mitigations it provides to the system as a whole.
	  ○ MCAS is configured to log activity by all users including Global Admins providing an audit trail for new services.
	  ○ Azure AD PIM is enabled and requires Global Admins to provide a reason when requesting elevated privileges. PIM will also log the start time and end time of the elevated privileges.

Residual Likelihood	2 – Unlikely
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	None
Target Likelihood	2 – Unlikely
Target Consequence	3 – Moderate
Target Risk Rating	2 – Medium

Table 20 Use of un-assessed cloud services creates exposures

Risk Event ID R19	**Risk Event Description** Use of un-assessed cloud services creates exposures
Risk Overview	An administrator enables a cloud service - or new feature within an existing cloud service - for use with the Blueprint that is not currently part of the assessed Blueprint.
Assets Affected	• All cloud based infrastructure • Sensitive and or security classified data
Threat Sources	• Adversarial – Individual – Insider, Trusted Insider, Privileged Insider • Accidental – Privileged User/Administrator

Threat Events	• Obtain unauthorised access to:
	  ○ Deny access to agency information to authorised users
	  ○ Modify agency information and making the integrity of the information unviable or no longer trustworthy Obfuscate adversary actions
	• Obtain information by opportunistically stealing or scavenging information systems/components
	• Compromise organisational information systems to facilitate exfiltration of data/information
	• Obtain sensitive and or classified information via exfiltration

Inherent Likelihood	3 – Possible
Inherent Consequence	3 – Moderate
Inherent Risk Rating	3 – High

Ongoing and Completed Treatments	• Agency treatments
	  ○ Agency IT Security Policy for authorised staff to not enable new cloud services or features
	  ○ Approval process to obtain a privileged user account
	  ○ Training to Agency nominated system administrators
	  ○ As new services become available the Agency will undertake a risk assessment of the service and establish if the risk is within the Agency's tolerance before engaging the new service offering
	• Treatments
	  ○ Leverage built-in Azure AD / Office 365 Role Groups to implement a robust Role-Based Access Control (RBAC) model minimising the number of users that can onboard a new service or enable additional features
	  ○ MCAS is configured to log activity by all users including Global Admins providing an audit trail for new services.
	  ○ Azure AD PIM is enabled and requires Global Admins to provide a reason when requesting elevated privileges. PIM will also log the start time and end time of the elevated privileges.

Residual Likelihood	2 – Unlikely

Risk Event ID R19	**Risk Event Description** Use of un-assessed cloud services creates exposures
Residual Consequence	3 – Moderate
Residual Risk Rating	2 – Medium
Proposed Treatments	None
Target Likelihood	2 – Unlikely
Target Consequence	3 – Moderate
Target Risk Rating	2 – Medium

Appendix A

Abbreviations and Acronyms

Table 21 details the abbreviations and acronyms used throughout this document.

Table 21 Abbreviations and Acronyms

Acronym	Meaning
ABAC	As-Built As-Configured
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
ATP	Advanced Threat Protection
BEC	Business Email Compromise
CCSL	Certified Cloud Services List
DDoS	Distributed Denial of Service
DKIM	DomainKeys Identified Mail
DMARC	Domain based Message Authentication, Reporting and Conformance
DoS	Denial of Service
DTA	Digital Transformation Agency
EOP	Exchange Online Protection
ISM	Information Security Manual
JIT	Just-In-Time
MCAS	Microsoft Cloud App Security
MFA	Multi-Factor Authentication
PAW	Privileged Access Workstation
PIM	Privileged Identity Management
RBAC	Role-Based Access Control
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SPF	Sender Policy Framework
TLS	Transport Layer Security

Acronym	Meaning
UAC	User Account Control
WDAC	Windows Defender Application Control
WDEG	Windows Defender Exploit Guard

Appendix B

Risk Matrix

Instructions for using consequence criteria:
Select the highest credible consequence. If your risk occurred, would one or more of the following apply?

		Consequence Criteria				
	Harm to People	• Injury not requiring treatment. • The Agency has a high degree of control over the environment.	• Injury requiring in house first aid treatment. • The Agency has indirect control over the environment.	• Moderate physical or economic injury to program participants, stakeholders, or staff.	• The activity results in major injury or economic harm to program participants, job seekers, or it encourages reckless work practices.	• Advice given by the Agency results in severe injury or economic harm. • The activity design threatens harm to staff, stakeholders, or program participants.
	Non-compliance	• The legal, legislative, and policy environment is well understood and there is little opportunity for non-compliance.	• Non-systematic, accidental non-compliance that will not have a material impact.	• Incidental non-compliance with policy frameworks. • The proposed activity is not supported by a constitutional head of power or there is not legislative authority.	• Reckless non-compliance with regulatory or contractual requirements.	• Intentional non-compliance with legislative (criminal or administrative) requirements. • Creation of an environment that allows systemic non-compliance.
	Financial Mismanagement or Loss	• The potential for and impact of financial loss or mismanagement is insignificant.	• Small financial loss within policy and legal authority and/or little opportunity for fraudulent activity to occur.	• Significant financial loss may occur, but it will be detected in a timely manner.	• Financial loss significant enough to compromise the viability of the program and its ongoing existence.	• Financial loss has the opportunity to compromise the viability of the Agency and its ongoing existence.
	Underperformance	• The proposed activity provides limited opportunity for underperformance.	• The activity is innovative in its nature and has been structured in such a way that should it fail, it will fail quickly and cheaply.	• Expectations may not be met, but there are robust communication strategies in place. • Reduced capacity to sustain critical capabilities.	• Expectations around delivering on time, on budget, and to a quality standard are poorly defined, not achievable, or poorly managed.	• There are multiple ways for outcomes and objectives not to be met and this has not been appropriately communicated to stakeholders.
	Reputational Damage	• The proposed activity has very little opportunity to cause damage to the Agency's reputation.	• Proper fact checking and clearance procedures are in place and will allow the Agency to respond to adverse media coverage quickly and positively.	• The Agency is unable to credibly engage with policy-based criticism or will do so in an inappropriate or poorly conducted manner.	• Significant damage to our relationship with parliament, the minister or other government Departments or Agencies.	• Direct damage to the reputation of the Agency for undertaking its role providing high-quality, apolitical policy advice, and support to government.
		Minimal	**Minor**	**Moderate**	**Major**	**Severe**
Likelihood	• There is a high level of certainty the event will occur. • There is a greater than 90% chance the risk will occur in the life of the plan, project or activity.	**Almost certain**	Medium	Medium	High	Extreme	Extreme
	• It's not certain the risk will occur, but all information indicates the risk has a high probability of eventuating. • There is a 60% to 90% chance the risk will occur in the life of the plan, project, or activity.	**Likely**	Low	Medium	High	Extreme	Extreme
	• There is a reasonable probability the risk could occur. • There is a 40% to 60% chance the risk will occur in the life of the plan, project, or activity.	**Possible**	Low	Medium	High	High	Extreme
	• There is a credible but unlikely possibility the risk may occur. • There is a 10% to 40% chance the risk will occur in the life of the plan, project, or activity.	**Unlikely**	Low	Medium	Medium	High	High
	• There is a high level of justifiable certainty the risk won't occur. • There is a less than 10% chance the risk will occur in the life of the plan, project, or activity.	**Rare**	Low	Low	Medium	Medium	High