

# Hybrid security risk management plan

2021-02-08

This Security Risk Management Plan (SRMP) has been developed to demonstrate the reduction in risk that can be achieved by implementing the HybridSystem 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 HybridSystem 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 HybridSystem. The risk matrix, including definitions of likelihood and consequence, is provided at Risk Matrix. Agencies leveraging the HybridSystem 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
R01	Inadequate privileged account management	High	Medium
R02	Sensitive/classified email sent to unauthorised recipients	High	Medium
R03	Unauthorised access to data hosted within Office 365	High	Medium
R04	Malicious insider disables security capabilities	Medium	Medium
R05	Unskilled administrator misconfigures services	Medium	Medium
R06	Components infected by malicious code	High	Medium
R07	Unauthorised access to email on Exchange Online	High	Medium
R08	Denial of service attacks	High	Medium
R09	Cyber security incident not detected	High	Medium
R10	Inability to recover from a data loss event	Medium	Low
R11	Operating System vulnerability allows exploitation	High	Medium

Risk Event ID	Risk Event Description	Inherent Risk Rating	Residual Risk Rating
R12	Application vulnerability allows exploitation	High	Medium
R13	Attacker bypasses application control capability	High	Medium
R14	Password spray attack directed at Azure AD	High	Medium
R15	Lack of availability due to cloud service provider outage	Medium	Low
R16	Privileged Access Workstations not implemented for administration	High	Medium
R17	Mobile device compromised	High	High
R18	Use of un-assessed cloud services creates exposures	High	Medium
R19	Users declassifying emails without the owner's permission	High	Medium
R20	Comprise of the Azure AD Connect database	Medium	Medium
R21	Comprise of the SharePoint database	Medium	Medium

## Introduction

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

PROTECTED is used throughout 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.

## Purpose

The purpose of this SRMP is to identify the risks and the residual risk to an Agency implementing the HybridSystem.

## Scope

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

The Microsoft Office 365 service is addressed in the Information Security Registered Assessors Program (IRAP) report (available in the Service Trust Portal) 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 HybridSystem.

## 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 Risk Matrix.

## Risk assessment

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 Risk Matrix.

### R01 Inadequate privileged account management

**Risk overview** If a privileged account were to be compromised or system privileges were incorrectly assigned, 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

- All infrastructure (Azure AD, Office 365, on-premises servers, and endpoints)

#### 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 unavailable 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 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
- HybridSystem 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
- Azure Advanced Threat Protection (Azure ATP) monitors

**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 HybridSystem
- Agency training for security and system administrators for the use of Security Centre / Sentinel
- Monitoring of events within Security Centre / Sentinel
- Service accounts are created as part of the group “Managed Service Accounts”
- Privileged accounts are managed as part of the group “Protected Users” security group

**Target likelihood** 1 – Rare

**Target consequence** 2 – Minor

**Target risk rating** 1 – Low

#### **R02 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 unauthorised 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
- HybridSystem treatments
  - Protective markings applied to email by users based on the classification of the content of emails, including attachments
  - Data transfer logs are retained

**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

### **R03 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

**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
- HybridSystem treatments
  - Password complexity is enforced in line with Information Security Manual (ISM) standards, and users are required to change passwords on first use
  - 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
  - Azure Advanced Threat Protection (Azure ATP) monitors privileged (sensitive) accounts for suspicious activities
  - 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
  - Credential Guard is enabled and credential theft is blocked through Microsoft Defender Exploit Guard
  - Pass through authentication (PTA) method is utilized for credentials in Azure authentication
  - Data transfer logs are retained

**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

**R04 Malicious insider disables security capabilities**

**Risk overview** An 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**

- HybridSystem 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
  - Microsoft's attack surface reduction rules are enabled

**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

**R05 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 (Azure AD, Office 365, on-premises servers, and endpoints)

**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**

- HybridSystem 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 HybridSystem
- 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

**R06 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 (Azure AD, Office 365, on-premises servers, 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

### **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
- HybridSystem 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
  - Azure Advanced Threat Protection (Azure ATP) monitors privileged (sensitive) accounts for suspicious activities
  - Windows Defender Application Control (WDAC) provides application control functionality to block unauthorised executables from running
  - Windows Defender Exploit Guard (WDEG) ‘exploit protection’ feature is enabled
  - Hardening of Windows 10 desktops including application control to ACSC recommended practices
  - Microsoft’s attack surface reduction rules are enabled
  - Data transfer logs are retained

**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

## **R07 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**

- HybridSystem treatments
  - Password complexity is enforced in line with ISM standards, and users are required to change passwords on first use
  - Conditional Access enforces MFA for all users and administrators
  - Conditional Access blocks access to Office 365 from external networks
  - Service provider networks are segregated from DTA networks through the use of a Secure Internet Gateway (SIG)
  - Legacy authentication blocked via Conditional Access policies
  - Credential Guard is enabled and credential theft is blocked through Microsoft Defender Exploit Guard
  - Pass through authentication (PTA) method is utilized for credentials in Azure authentication
  - Data transfer logs are retained

**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

#### **R08 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 (Azure AD, Office 365, on-premises servers, and endpoints)
- 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

**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

## **R09 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 (Azure AD, Office 365, on-premises servers and endpoints)
- 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
- HybridSystem treatments
  - Windows Defender ATP is enabled to provide reporting, pre-breach protection, post-breach detection, automation, and response on hosted desktops and platform servers
  - Azure Advanced Threat Protection (Azure ATP) monitors privileged (sensitive) accounts for suspicious activities
  - 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
  - Credential Guard is enabled and credential theft is blocked through Microsoft Defender Exploit Guard
  - Pass through authentication (PTA) method is utilized for credentials in Azure authentication
  - Data transfer logs are retained

**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 / Sentinel
- Monitoring of events within Security Centre / Sentinel

**Target likelihood** 1 – Rare

**Target consequence** 3 – Moderate

**Target risk rating** 2 – Medium

### **R10 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 (Azure AD, Office 365, on-premises servers and endpoints)
- 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
- HybridSystem 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 or Microsoft System Center Configuration Manager (SCCM), and Standard Operating Environments (SOEs) are to be used
  - SOPs provided for administrators

**Residual likelihood** 1 – Rare

**Residual consequence** 2 – Minor

**Residual risk rating** 1 – Low

**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

**R11 Operating system vulnerability allows exploitation**

**Risk overview** Security vulnerabilities are discovered within the operating system versions utilised by the solution allowing exploitation.

**Assets affected**

- Endpoints

**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 treatments
  - The Agency’s support team will monitor patching and perform manual remediation as required
- HybridSystem treatments
  - 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 or SCCM can deploy firmware patches as executable files as required
  - Microsoft’s attack surface reduction rules are enabled

**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

**Target risk rating** 2 – Medium

**R12 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 treatments
  - The Agency’s support team will monitor patching and perform manual remediation as required
- HybridSystem treatments
  - Intune or SCCM 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
  - Microsoft’s attack surface reduction rules are enabled

**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

**Target risk rating** 2 – Medium

**R13 Attacker bypasses application control capability**

**Risk overview** An attacker attempts to bypass the application controls enforced on endpoints.

**Assets affected**

- Endpoints

**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**

- HybridSystem treatments
  - WDAC provides application control functionality to block unauthorised executables from running
  - WDAC policies configured centrally from Intune or SCCM
  - 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
  - Microsoft’s attack surface reduction rules are enabled

**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

### **R14 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 (Azure AD, Office 365, on-premises servers and endpoints)
- 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
- HybridSystem treatments
  - Conditional Access enforces MFA for all users and administrators
  - Password complexity is enforced in line with ISM standards, and users are required to change passwords on first use
  - 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
  - Azure Advanced Threat Protection (Azure ATP) monitors privileged (sensitive) accounts for suspicious activities
  - Credential Guard is enabled and credential theft is blocked through Microsoft Defender Exploit Guard
  - Pass through authentication (PTA) method is utilized for credentials in Azure authentication

**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

**R15 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
- HybridSystem 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

#### **R16 Privileged Access Workstations not implemented for administration**

**Risk overview** An adversary compromises privileged access mechanisms due to the lack of implementation of Privileged Access Workstations (PAWs) within the design.

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 (Azure AD, Office 365, on-premises servers, and endpoints)

#### **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**

- HybridSystem 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
  - 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 control 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
  - Credential Guard is enabled and credential theft is blocked through Microsoft Defender Exploit Guard
  - Pass through authentication (PTA) method is utilized for credentials in Azure authentication

**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

### **R17 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) not being fully implemented due to the usability impacts.

Note, the HybridSystem 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

### **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
- HybridSystem 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
- Data transfer logs are retained

**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

#### **R18 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 HybridSystem that is not currently part of the assessed HybridSystem.

#### **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
- HybridSystem 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
  - Data transfer logs are retained

**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

#### **R19 Users declassifying emails without the owner’s permission**

**Risk overview** Sensitivity labels allow users to apply protective markings to emails to ensure appropriate security controls are applied to information. A user has the ability to change the protective marking without the originators permission but are required to provide a text-based justification.

#### **Assets affected**

- PROTECTED data within emails (including attachments)

#### **Threat sources**

- Adversarial – Individual – Insider, Trusted Insider, Privileged Insider
- Accidental – User/Administrator

#### **Threat events**

- Sensitive and or classified information being:
  - stored on the incorrect system
  - viewed by personnel not cleared for that security level
  - leaked to the general public
- Obtain sensitive and or classified information via exfiltration
- Invalidate the integrity and confidentiality of information

**Inherent likelihood** 3 – Possible

**Inherent consequence** 3 – Moderate

**Inherent risk rating** 3 – High

### **Ongoing and completed treatments**

- Agency treatments
  - Training to Agency users on the appropriate measures for applying and changing protective markings.
- HybridSystem treatments
  - The solution has been configured to require users to provide a justification for changing a label.

**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

### **R20 Comprise of the Azure AD Connect database**

**Risk overview** An unauthorised user (malicious) gains access to the database exposing the username and email addresses used by Azure AD Connect.

#### **Assets affected**

- Domain identities (not including passwords/passphrases)

#### **Threat sources**

- Adversarial – Individual – Insider, Trusted Insider, Privileged Insider

#### **Threat events**

- Adversary could obtain username and email addresses for user/administrator accounts being synchronised to Azure AD

**Inherent likelihood** 3 – Possible

**Inherent consequence** 2 – Minor

**Inherent risk rating** 2 – Medium

### **Ongoing and completed treatments**

- Agency treatments
  - Leverage server-side event logging to monitor login events and network traffic.
  - Enable multi-factor authentication on all domain accounts
  - Hardening of operating systems, applications and database systems to ACSC recommended practices

**Residual likelihood** 4 – Unlikely

**Residual consequence** 2 – Minor

**Residual risk rating** 2 – Medium

**Proposed treatments** None

**Target likelihood** 4 – Unlikely

**Target consequence** 2 – Minor

**Target risk rating** 2 – Medium

## **R21 Comprise of the SharePoint database**

**Risk overview** An unauthorised user (malicious) gains access to the database exposing configuration settings.

### **Assets affected**

- SharePoint Configuration settings

### **Threat sources**

- Adversarial – Individual – Insider, Trusted Insider, Privileged Insider

### **Threat events**

- Adversary could potentially modify or delete the configuration settings.

**Inherent likelihood** 3 – Possible

**Inherent consequence** 2 – Minor

**Inherent risk rating** 2 – Medium

### **Ongoing and completed treatments**

- Agency treatments
  - Leverage server-side event logging to monitor login events and network traffic.
  - Enable multi-factor authentication on all domain accounts
  - Hardening of operating systems, applications and database systems to ACSC recommended practices

**Residual likelihood** 4 – Unlikely

**Residual consequence** 2 – Minor

**Residual risk rating** 2 – Medium

**Proposed treatments** None

**Target likelihood** 4 – Unlikely

**Target consequence** 2 – Minor

**Target risk rating** 2 – Medium