Continuous monitoring plan

2021-09-29

This Continuous Monitoring Plan (CMP) has been prepared to support assessment of the ongoing security posture of the Protected Utility blueprint desktop environment. Throughout, this document provides continuous monitoring guidance including:

- Developing an agency-specific continuous monitoring plan
- Developing measurements to assess security controls
- Collecting data relating to areas of security that the agency is responsible for managing
- Aggregating collected monitoring data for analysis
- Analysing monitoring information to identify and assess the severity of security weaknesses, and
- Responding to identified security weaknesses.

Throughout this document several security monitoring tools are identified. While continuous monitoring and security monitoring are not identical, some overlap exists between the two in their purpose. Security monitoring tools gather and record information that enables identification of potential vulnerabilities that arise in a system. This information is useful in assessing the system's overall health and security posture.

Purpose

The Information Security Manual (ISM) requires agencies to create a CMP as one of the system-specific documents prior to a system's operation. This is to assist agencies in identifying, prioritising and responding to security vulnerabilities.

To meet this requirement, this CMP provides agencies leveraging the blueprint desktop environment (the desktop environment) with an outline of implemented technologies that produce continuous monitoring data. This plan also provides guidance for monitoring the security posture of the system and verifying implemented security controls remain fit-for-purpose for the system's operating and threat environment.

The three most common types of continuous monitoring activities are: vulnerability assessments; vulnerability scans; and penetration tests. These are not always possible or appropriate for systems that consume cloud services, such as the blueprint. Therefore, agencies should utilise this plan to consider what mechanisms are available to them to provide appropriate ongoing monitoring.

Scope

The scope of this CMP is specific to monitoring security controls involved with the agency's use of Microsoft 365 services as part of the desktop environment. As the blueprint is implemented in collaboration with Microsoft as the Cloud Service Provider (CSP), a shared responsibility model exists to divide responsibilities relating to the security of the desktop environment.

While continuous monitoring and security monitoring are not identical, overlap exists between the two in that many security monitoring tools gather and record monitoring information that is useful in assessing the overall security posture of a system. Agencies may wish to utilise a Security Information and Event Management System (SIEM) to aggregate monitoring information for the purpose of identifying weaknesses in the desktop environment's security posture.

Continuous monitoring responsibilities that a consumer of the Microsoft 365 solution is not required to manage are out of this document's scope, these include:

- Vulnerability scanning of the Microsoft 365 platform and software

- Penetration testing of the Microsoft 365 platform and software, and
- Vulnerability assessment activities pertaining to the Microsoft 365 platform and software.

This document covers continuous monitoring responsibilities owned by the agency or jointly owned between the agency and Microsoft.

The CMP is a living document. It is anticipated that, over time, amendments and updates may be applied to the plan in the event of changes to the blueprint, the desktop environment or the agency.

Developing a Continuous Monitoring Plan

Agencies are free to develop the structure of their CMP as appropriate for their organisation. The ISM specifies only that agencies must:

- conduct vulnerability scans for systems at least monthly
- conduct vulnerability assessments or penetration tests for systems at least annually
- analyse identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls
- use a risk-based approach to prioritise the implementation of identified mitigations.

Whilst agencies will be able to undertake these activities in relation to on-premise equipment, there is limited ability to conduct vulnerability assessments, vulnerability scans and penetration tests against CSP infrastructure.

Outside of ISM requirements, this document provides further suggestions and mechanisms which are available to agencies to provide ongoing monitoring across their implementation of the blueprint.

The National Institute of Standards and Technology (NIST) outlines a standard process for conducting continuous monitoring information which includes the following initiatives, which agencies should utilise when developing their continuous monitoring strategy:

- **Define** a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities, up-to-date threat information and business impacts
- **Establish** metrics and measures, status monitoring frequencies, control assessment frequencies, and where needed a technical architecture
- **Implement** a continuous monitoring program to collect the security related data required for the defined metrics and measures. Automate collection, analysis and reporting of data where possible
- **Analyze** the data gathered and Report findings, determining the appropriate response. It may become necessary to collect additional information to clarify or supplement existing monitoring data
- **Respond** to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection
- **Review and Update** the monitoring program, revising the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data driven control of the security of an organization's information infrastructure; and increase organizational flexibility.

Continuous Monitoring Plan structure and guidance

The following section provides suggested inclusions and guidance for developing a CMP. The suggested sections are detailed in the table below.

Section	Detail
Roles and Responsibilities	Matrix of assigned roles related to continuous monitoring
Measurements	List of agency specific measurements and expected metric targets sorted by each continuous monitoring domain
Information Sources and Collection	List of information sources required to calculate measurements and procedures for collection (refer to Attachment B: Data Collection Example)

Section	Detail
Timeframes and Frequencies	Define agency specific requirements for timeframes and frequencies
Information Storage and Management	Agency specific policy decisions surrounding aggregation and storage of information
Analysis	Agency specific analysis procedures
Response	Agency policy details around risk assessment, risk tolerance and expected response actions and procedures (refer to Attachment C: Risk Analysis Example)
Continuous Monitoring Assessment	List of measurement assessment tables (refer to Attachment A: Measurements/Metrics Development and Analysis Examples)

Roles and responsibilities

The CMP should document relevant roles and responsibilities associated with performing continuous monitoring and maintaining the capabilities within the agency.

Roles associated with continuous monitoring that may require documentation include:

- Chief Information Security Officer
- System Owner
- Authorising Officer
- Security Operations Centres
- Vulnerability Management Teams
- Desktop Support Teams, and
- Cloud Operations Teams.

Responsibilities associated with continuous monitoring may include collecting, analysing and reporting continuous monitoring data. These responsibilities should be assigned to the relevant defined roles.

Measurements

The CMP should outline measures that the agency will use to evaluate whether security controls are working as intended and whether it is managing risk associated with the desktop environment appropriately.

Measures should align with specific security objectives and aid in providing decision makers with an understanding of how security is performing within the system. The ISM recommends the agency's CISO implement metrics and measures for the organisation.

The agency may wish to refer to guidance outlined in NIST 800-55 Performance Measurement Guide for Information Security. This guidance recommends measures are developed for security controls at the organisational, program and system levels to assess the following aspects of a security control:

- Implementation – progress in implementing information security programs, specific security controls and associated policies and procedures
- Effectiveness/efficiency – validating that security controls are implemented correctly, operating as intended and meeting their desired outcome
- Impact – the impact of a control on the agency's mission

For holistic assessment of security, measures should be mapped to controls within the agency's security control framework.

Examples of security control measurements have been included in Attachment A: Measurements/Metrics Development and Analysis Examples.

Information sources & collection

The CMP should list any sources of information necessary to assess the defined measures. The agency should detail how this information will be collected, the purpose it is collected for and relevant details

such as corporate business owners.

The agency may consider utilising the example table provided in Attachment B: Data Collection Example to document their data collection requirements and methods.

Data gathering tools and sources Corporate desktop environments generate vast quantities of digital information from sources such as network devices, databases, servers and endpoints. Agencies will need to consider which information sources they require to maintain an awareness of the current state of their environment.

Cloud based systems generate a wide range of information about their operation and use. This section provides examples of various information sources available that agencies may collect and monitor to provide visibility over the posture of their security program.

The below table lists each continuous monitoring security domain alongside applicable Microsoft and agency tools and sources of information. The agency may consider monitoring information from these sources to measure each domain's security controls.

Domain	M365 Tools	Agency Tools and Sources
Vulnerability & Patch Management	Windows Server Update Service Microsoft Endpoint Configuration Manager Microsoft Intune Microsoft Defender for Endpoint	Vulnerability scanner Vulnerability database Patch Management database Software registry
Event & Incident Management	MECM Endpoint Detection and Response Microsoft Defender for Identity (Azure Advanced Threat Protection) Microsoft Defender for Office 365	Incident database SIEM
Malware Detection	Microsoft Defender for Identity (Azure Advanced Threat Protection) Microsoft Defender Antivirus Microsoft Defender for Office 365 Microsoft Defender for Endpoint	Incident database
Asset Management	Microsoft Cloud App Security (MCAS) Microsoft Intune Microsoft Endpoint Configuration Manager	Asset management registry
Configuration Management	Microsoft Secure Score Security Center Compliance Center Microsoft Attack Surface Reduction Azure Active Directory Identity Protection Azure Conditional Access Azure Active Directory	Agency configuration database Certification and authorisation registry
Network Management	Microsoft Cloud App Security (MCAS) Windows Defender Application Control Conditional Access Windows Firewall Microsoft Intune Microsoft Endpoint Configuration Manager	Network perimeter firewall
License Management	Microsoft 365 Admin Center	Software asset registry

Domain	M365 Tools	Agency Tools and Sources
Information Management	Microsoft Information Protection Windows Information Protection Information Protection (Office 365) Retention Labels & Policies Microsoft Cloud App Security (MCAS)	Data classification and categorization policies

Reference data sources The agency should consider monitoring updates to the below reference data sources to gather information on software and configuration vulnerabilities.

To identify and assess known vulnerabilities, the agency should consider subscribing to receive security notifications when relevant vulnerabilities are identified in Microsoft's tools and products. In addition, the agency should also consider subscribing to other vulnerability advisory services to receive vulnerability updates about any non-Microsoft applications they may utilise.

To assess the security of their system's architecture, the agency should consider monitoring updates to the blueprint, relevant compliance standards and configuration benchmark advisories.

Category	Reference Data Source
Vulnerability & Patch Management	Microsoft Security Notification Service National Vulnerability Database US-CERT ACSC Security Notifications AusCERT
Configuration Management	Australian Government Information Security Manual ACSC Essential Eight ACSC Publications Protected Utility blueprint Center for Internet Security (CIS) Benchmarks

Continuous monitoring information elicitation activities To elicit information about potential vulnerabilities within the organisation's information security program, the agency should perform the below activities.

Technique	Detail
Control effectiveness assessments	This technique would elicit detail on the coverage, effectiveness, impact and efficiency of the agency's security controls
Vulnerability scans	Vulnerability scans can be performed to identify known vulnerabilities in the agency's deployed software or weaknesses in the system's configuration
Vulnerability assessments or penetration tests	Vulnerability scans can be performed to find known vulnerabilities in the agency's deployed software or weaknesses in the system's configuration

Timeframes and frequencies

The CMP should outline when and how often effectiveness reviews and testing activities are performed for each security control and associated measurement. When determining timeframes and frequencies, the agency should establish achievable assessment frequencies commensurate with their risk appetite. Factors the agency may wish to consider when determining frequencies include:

Consideration	Detail	Impact
Criticality of controls	Is the control critical to the effectiveness of the security program? Is the control critical to the agency's priorities?	Controls providing highly critical functionality should be more frequently monitored
Volatility of control	Is the effectiveness of the security control likely to change as the system evolves?	Controls expected to be volatile should be more frequently monitored
Robustness of controls	Does the control have any current weaknesses inhibiting its effectiveness?	Controls with known weaknesses should be more frequently monitored until remediated
Risk tolerance	Does the timeframe align with the agency's risk tolerance?	Agencies with higher risk tolerance could perform less frequent monitoring
Threat advisories/Vulnerability information	Has the agency received information that may impact the effectiveness of a control?	An ad hoc control assessment may need to be performed or monitoring frequencies altered
Regulatory requirements	Do mandatory timeframes exist within the agency's regulatory requirements?	The agency may need to alter timeframes to align with requirements
Reporting Requirements	Has the agency defined specific reporting requirements that need to be met?	The agency may need to alter timeframes to align with requirements

When defining assessment and response frequencies, the agency may specify tasks assigned to applicable roles defined in Roles and Responsibilities section above. Examples of tasks include:

- Desktop teams will review Intune reports monthly, and
- Office 365 administrators will review Active Directory weekly.

Required ISM timeframes For infrastructure under the control of the agency, such as on premises Exchange and Active Directory servers, the ISM specifies required timeframes for the activities defined in the below table:

Activity	Frequency
Vulnerability scans	At least monthly
Vulnerability assessments or penetration tests	At least monthly
Review SOEs	At least monthly
Review security documentation	At least monthly

Information aggregation, storage and management

The CMP should document how information required for continuous monitoring will be stored and managed. This should include where information will be stored and relevant parties responsible for the information.

Security Information and Event Management System (SIEM) To enhance the ability to identify inappropriate or unusual activity, agencies may wish to integrate the analysis of vulnerability scanning information, network monitoring, and system log information through the use of a SIEM.

Security management dashboards Security management dashboards are virtual security management workspaces provided by Microsoft's customer security and compliance teams the agency could leverage Microsoft's security management dashboards to achieve automation of information aggregation.

These solutions are integrated across Microsoft 365 services and provide actionable insights to help reduce risks and safeguard Microsoft 365 deployments. They provide the ability to aggregate and view monitoring information in a single location.

Dashboard	Detail
Microsoft 365 Security Center	Agencies can utilise Security Center to view alerts and incidents related to their infrastructure and reports measures within Microsoft Secure Score. Agencies can utilise Secure Score to determine the security baseline of their Microsoft 365 configuration. Secure Score can scan a Microsoft environment, assign an overall security score to the environment's configuration and provide recommendations to improve the security of the environment.
Microsoft 365 Compliance Center	Agencies can use Compliance Center to track specific compliance issues and risks. Compliance Center also provides customisable policies which can alert agencies when Microsoft 365 contravenes a particular policy.
Microsoft Cloud App Security Dashboard	Agencies can utilise the Cloud App Security Dashboard to view security information of their cloud environment including open alerts, discovered apps, files infected with malware, azure security configuration recommendations and DLP alerts.

Analysis

The CMP should document procedures for conducting analysis of collected information against defined measures. These processes could take the form of runbooks or work instructions. This would facilitate assessment of potential vulnerabilities or weaknesses in a manner that is repeatable and consistent.

To analyse collected data, the agency should calculate the measurements that were defined as part of the Roles and Responsibilities section. To perform this analysis, the agency may wish to refer to the example measurements analysis tables included in Attachment A: Measurements/Metrics and Analysis Examples.

Response

Assessment The CMP should set out the process for how identified system weaknesses and vulnerabilities will be prioritised for response. Once analysis has been completed and vulnerabilities are identified or controls do not meet their expected measurement target, the agency should assess and manage the risk involved utilising methods detailed in their Security Risk Management Plan (SRMP). Example details of the risk assessment table have been included in Attachment C: Findings Analysis Example.

The agency should undertake analysis which allows them to reach a thorough understanding of the potential impacts of identified vulnerabilities and the risk that is posed to the agency. This may include asking questions such as:

- What is the likelihood of the vulnerability being exploited?
- What happens/what is the impact if the vulnerability is exploited?
- How effective are current controls in reducing potential risk?

Prior to the determination of a mitigating response, the agency should consider their risk tolerance levels and determine if other actions are appropriate such as:

- Accepting
- Transferring, or
- Avoiding the risk.

Assessments should be conducted by suitably skilled personnel, where possible independent of the system owner or developer, or by a third party who is independent of the target of the assessment. Assessments may be performed by either using automated assessment tools or manually by appropriately skilled ICT professionals.

When assessing vulnerabilities, the agency may consider vendor security bulletins or the severity ratings assigned to security vulnerabilities under schemes such as the Common Vulnerability Scoring System.

Responsive actions The CMP should document potential responsive actions. These may include actions such as system configuration changes, training, procuring security tools, changing system architecture, establishing new procedures or updating security policy documentation.

When determining the appropriate responsive action, the agency should asking the following questions:

- What are the available mitigation techniques?
- How effective are those mitigations likely to be?
- Who is responsible for implementing any mitigations?
- What will the cost of implementing the mitigations be?

When deciding on a responsive action, Agencies should consider change management and approval requirements.

Prioritisation of response The CMP should outline how identified weaknesses and vulnerabilities will be prioritised based on their assessed risk or impact and the timeframes within which actions will be taken.

The agency may wish consider the timeframes specified within the ISM under which action must be taken as outlined in the below table.

Vulnerability Risk	Timeframe
Extreme	48 hours
High	Two Weeks
Moderate	Four Weeks
Low	Four Weeks

Depending on the vulnerability identified and its severity, action may be required immediately or may be implemented over a period of time. Agencies should consider their risk tolerance levels and verify that processes exist to track the progress of remediation actions as they occur.

Reporting

The CMP should document requirements of reporting in relation to continuous monitoring. This may include details as set out in the below table.

Activity	Detail
Generating Reporting	Specific personnel and roles responsible for generating reporting information
Stakeholders and Audience	Personnel and roles that will be receiving generated reporting
Content and Format	Content included in reporting and expected format the report will be presented in
Reporting Frequency	How often reporting is to be generated and sent to its audience
Tools Used for Reporting	Any tools used to generate or automate reporting

Many of these details would be included in the analysis tables as shown in Attachment A: Measurements/Metrics and Analysis Examples.

Review and update

The CMP should outline when and under what conditions review and updates to the continuous monitoring strategy and approach will occur. Continuous monitoring processes should not be static, they should adapt based on changes in agency's threat and risk and when changes are made to desktop environment

technology and architecture. The CMP should be reviewed to ensure that it supports the agency in operating within its acceptable risk tolerance levels, that chosen measurements remain relevant, and that data is current and complete.

The agency should review the contents of the CMP annually or bi-annually.

Attachment A: Measurements/metrics development and analysis examples

Measures have been provided in this section as examples for how the agency could approach monitoring security controls. It is important to note that the agency should develop custom measurements, this list is for reference and is not intended to be exhaustive. These examples have been developed leveraging methods detailed in NIST 800-55 Performance Measurement Guide for Information Security.

Additionally, this section identifies relevant guidance on identifying and populating required data collection details.

Guidance

Agencies may refer to above guidance on developing measures and populating information. These include:

- Roles and Responsibilities
- Developing Measurements
- Data Collection Sources
- Collection and Reporting Frequencies
- Reporting Details

Configuration management measurement example The below table provides an example configuration management measure.

Field	Data
Measure ID	CM-1
Goal	All system users are identified and authenticated in accordance with the agency's information security policy
Related Controls	ISM 0974, 1173
Measure	Percentage (%) of accounts without MFA enabled
Type	Effectiveness/Efficiency
Formula	(Number of MFA-enabled accounts/total number of accounts) * 100
Target	(Percentage (%) target defined in accordance with agency risk tolerance)
Implementation Evidence	CM-1.1 Number of users with access to the system. CM-1.2 Number of users exempt from MFA requirements
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Active Directory, Azure Conditional Access Policies, Microsoft Security Center
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Vulnerability and patch management measurement example The below table provides an example vulnerability and patch management measure.

Field	Data
Measure ID	VPM-1
Goal	All system vulnerabilities are identified and remediated in accordance with the agency's information security policy
Related Controls	ISM 0304, 1143, 1493, 1643
Measure	Percentage (%) of security vulnerabilities not mitigated
Type	Effectiveness/Efficiency
Formula	(Number of mitigations (patches or other) applied + Number of vulnerabilities accepted within risk tolerance) / (Total number of system vulnerabilities) * 100
Target	(Percentage (%) target defined in accordance with agency risk tolerance)
Implementation Evidence	VPM-1.1 Number of vulnerabilities identified through advisories. VPM-1.2 Number of vulnerabilities identified through vulnerability scanning activities. VPM-1.3 Number of mitigations (patches or other) applied. VPM-1.4 Number of vulnerabilities determined not applicable. VPM-1.5 Number of vulnerabilities accepted within risk tolerance
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Software Registry, Vulnerability Database, Patch Management Database, Microsoft Intune, Microsoft Defender for Endpoint
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Event & incident management measurement example The below table provides an example event and incident management measure.

Field	Data
Measure ID	EIM-1
Goal	Security incidents are reported within timeframes defined in the agency's Incident Response Policy
Related Controls	ISM 0123, 0125, 0140
Measure	Percentage (%) of incidents reported within acceptable timeframes (calculated for each incident category)
Type	Effectiveness/Efficiency
Formula	For each incident category (number of incidents reported within agency defined timeframes / number of reported incidents) * 100
Target	(target defined in accordance with agency risk tolerance)

Field	Data
Implementation Evidence	EIM-1.1 Number of incidents reported for: Category 1: (Incident category defined in agency's IRP) Category 2: (Incident category defined in agency's IRP) Category N: (Incident category defined in agency's IRP) EIM-1.2 Of incidents reported for each category, how many were reported within agency defined timeframes? Category 1: (Incident category defined in agency's IRP) Category 2: (Incident category defined in agency's IRP) Category N: (Incident category defined in agency's IRP)
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Incident database
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Malware detection measurement example The below table provides an example malware detection measure.

Field	Data
Measure ID	MD-1
Goal	Effectively detect and prevent instances of malware installation/execution
Related Controls	ISM 1288
Measure	Calculated or each malware detection tool (percentage (%) of malware detection false positives.)
Type	Effectiveness/Efficiency
Formula	For each malware detection tool (Number of alerts identified as false positives / Number of alerts) * 100)
Target	(Percentage (%) target defined in accordance with agency risk tolerance)
Implementation Evidence	MD-1.1 Number of malware detection alerts marked as false positives for: <Tool 1> <Tool 2> <Tool 3> MD-1.2 Total number of malware detection alerts for: <Tool 1> <Tool 2> <Tool 3>
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Microsoft Defender Antivirus, Microsoft Defender for Endpoint, agency specific malware and endpoint detection tools
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Asset management measurement example The below table provides an example asset management measure.

Field	Data
Measure ID	AM-1
Goal	All devices are managed within the agency's device management policy
Related Controls	ISM 1533, 1195, 1482, 0869, 1085, 1202
Measure	Percentage (%) of managed endpoints not compliant with MDM security policy
Type	Implementation
Formula	(Number of managed endpoints identified as out-of-compliance / Total number of managed endpoints) * 100
Target	(Percentage (%) target defined in accordance with agency risk tolerance)
Implementation Evidence	Number of managed endpoints identified as out-of-compliance Total number of managed endpoints
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Microsoft Intune, Microsoft Endpoint Configuration Manager, Asset Management Register
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Network management measurement example The below table provides an example network management measure.

Field	Data
Measure ID	NM-1
Goal	All devices are managed in accordance with the agency's Asset Management Policy
Related Controls	ISM 1301, 1418
Measure	Percentage (%) of devices discovered on the network that are unrecognised
Type	Effectiveness/Efficiency
Formula	Number of unrecognised devices discovered on the network / Total number of discovered devices * 100
Target	(Percentage (%) target defined in accordance with agency risk tolerance)
Implementation Evidence	Number of unrecognised devices discovered during network discovery. Total number of devices discovered during network discovery
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Asset Management List, Microsoft Defender for Endpoint, Microsoft Endpoint Manager
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

License management measurement example The below table provides an example license management measure.

Field	Data
Measure ID	LM-1
Goal	Software lifecycle is effectively managed in accordance with the agency's Information Security Policy
Related Controls	ISM 1467, 1483, 1407
Measure	Percentage (%) of deployed software that has reached End of Support
Type	Effectiveness/Efficiency
Formula	Number of software license versions that have reached End of Support / Total number of software licenses * 100
Target	(Percentage (%) target defined in accordance with agency risk tolerance)
Implementation Evidence	Number of software license versions that have reached End of Support. Number of software licenses
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	Software Registry, Microsoft Defender for Endpoint
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Information management measurement example The below table provides an example information management measure.

Field	Data
Measure ID	IM-1
Goal	Information is identified and protected in accordance with the agency's information security policy
Related Controls	ISM 1187, 1297, 0663
Measure	Number of data loss prevention policy exceptions granted during monitoring period
Type	Effectiveness/Efficiency
Formula	Total number of policy exceptions granted during monitoring period
Target	(Target total defined in accordance with agency risk tolerance)
Implementation Evidence	Policy exceptions granted during monitoring period
Frequency	Collection frequency: (e.g. monthly) Reporting frequency: (e.g. monthly)
Responsible Parties	Applicable roles and responsibilities, e.g. collector, owner, stakeholders
Data Source	MCAS, Microsoft Defender for Endpoint, MIP
Reporting Format	(Agency's preferred reporting method i.e. bar graph in Monthly Health Check report)

Attachment B: Data collection example

This section provides an example data collection table the agency may wish to utilise to record data collection details. Additionally, this section identifies relevant guidance on identifying and populating

required data collection details.

Guidance For each measurement, the agency should create data collection tables for each item under "Implementation Evidence".

The following lists sections the agency may refer to for guidance developing measures and populating information:

- Roles and Responsibilities
- Data Collection Sources
- Collection and Reporting Frequencies

Data collection table example The below table provides an example table the agency may wish to utilise to record data collection details.

Field	Data
Relevant Measurement	CM-1
Information Detail	List of users without MFA enabled
Collection Frequency	Monthly
Source Tool	Active Directory
Information Owner	(Agency team or position responsible for the tool)
Role Responsible for Collection	(Agency specific role assigned to this task)
Information Collection Method	Agency specific process to elicit this information. Examples are: * Process for logging in to Azure admin portal and performing manual inspection; or, * Process for eliciting information through PowerShell script

Attachment C: Risk analysis example

This section provides an example risk analysis table that the agency may wish to utilise when determining and prioritising a response. Additionally, this section identifies relevant guidance on risk analysis and response.

Guidance The below lists sections the agency may refer to for guidance developing measures and populating information;

- Relevant Assets to Each Security Domain
- Response Assessment and Prioritisation

Risk assessment table example Example detail the agency could capture is provided in the below table. For more detail, and the Risk Matrix refer to the blueprint's Security Risk Management Plan (SRMP) or Hybrid (SRMP).

Field	Detail
Risk Overview	Brief risk statement
Assets affected	List of assets impacted by the risk
Threat sources	Types of threat actors (e.g. Adversarial – Trusted Insider)
Threat events	Events that may occur as a result of this risk being realized
Inherent likelihood	Likelihood rating without controls considered
Inherent consequence	Consequence rating without controls considered
Inherent risk rating	Result from comparing Likelihood and Consequence on Risk Matrix
Ongoing and completed treatments	Treatments being implemented to address the risk
Residual likelihood	Likelihood rating with current controls considered

Field	Detail
Residual Consequence	Consequence rating with current controls considered
Residual risk rating	Result from comparing Likelihood and Consequence on Risk Matrix
Proposed treatments	Risk mitigation treatments for consideration
Target likelihood	Desired likelihood rating with proposed treatments considered
Target consequence	Desired consequence rating with proposed treatments considered
Target risk rating	Result from comparing Likelihood and Consequence on Risk Matrix