

# Hybrid continuous monitoring plan

2021-02-10

This Continuous Monitoring Plan has been prepared to support assessment of the ongoing security posture of the DTA HybridSystem. Throughout, this document provides continuous monitoring guidance including:

- Developing an agency-specific continuous monitoring plan;
- Overview of Microsoft's tools for monitoring security posture and compliance;
- 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 Continuous Monitoring Plan 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 Continuous Monitoring Plan provides agencies leveraging the HybridSystem 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 HybridSystem. Therefore, agencies should utilise this plan to consider what mechanisms are available to them to provide appropriate ongoing monitoring.

## Scope

The scope of this Continuous Monitoring Plan is specific to monitoring security controls involved with the Agency's use of Microsoft 365 services as part of the HybridSystem. As the HybridSystem 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 HybridSystem.

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 SIEM to aggregate monitoring information for the purpose of identifying weaknesses in the HybridSystem'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 HybridSystem Continuous Monitoring Plan 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 HybridSystem 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 (security control 1163) specifies only that agencies must:

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

Whilst agencies will be able to undertake these activities in relation to their on premise equipment, there is limited ability to conduct vulnerability assessments, vulnerability scans and penetration tests against Cloud Service Provider (CSP) infrastructure. This document will assist agencies in identifying mechanisms which are available to them to provide ongoing monitoring across their implementation of the HybridSystem Blueprint.

The National Institute of Standards and Technology (NIST) outlines a standard process for conducting continuous monitoring 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

The following section provides suggested inclusions for CMP's which the Agency may wish to consider.

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

**Information sources** The CMP should list any sources of information that are needed as part continuous monitoring, how it will be collected, the purpose it is collected for and relevant details such corporate business owners.

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 aware of the current state of their environment.

Cloud based systems are able to generate a wide range of information about their operation and use. Later sections within this document the various information sources available from Microsoft that agencies may collect and monitor to provide visibility of their Microsoft Office 365 and Azure instances.

**Information 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.

To enhance the ability to identify inappropriate or unusual activity, organisations may wish to integrate the analysis of vulnerability scanning information, network monitoring, and system log information through the use of Security Information Event Management tools.

**Measurements and metrics** The CMP should outline the metrics and measures that the Agency will use to evaluate whether security controls are working as intended and whether it is managing risk associated with the HybridSystem appropriately. Metrics should align with specific security objectives and should aid in providing decision makers with an understanding of how security is performing within the system.

Metrics and Measures that could be relevant to agencies using the HybridSystem could include things such as:

- unpatched endpoints
- administrator accounts created
- failed logon attempts
- suspected phishing emails received.

**Timeframes and frequencies** The CMP should outline when and how often reviews and testings are performed.

For HybridSystem infrastructure within Office 365 and Azure, the Agency should specify when reviews will be conducted of various information sources. This should include the information sources that will be reviewed and how often that will occur. For example, the Agency may specify tasks such as:

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

For infrastructure under the control of the Agency, such as on premises Exchange and Active Directory servers, the ISM specifies that is should:

- Conduct vulnerability scans at least monthly
- Conducting vulnerability assessments or penetration tests at least annually

**Analysis** The CMP should document procedures for conducting analysis and reviews, this could take the form of things like runbooks or work instructions which allow agency personnel to conduct the necessary analysis in repeatable and consistent ways to identify potential vulnerabilities or weaknesses within the system.

## **Assessment and response**

**Assessment** The CMP should set out the process for how identified system weaknesses and vulnerabilities will be assessed and prioritised for response. The outcome of the assessment should be a determination of the risk to the system and the agency.

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 happens/what is the impact if the vulnerability is exploited?
- 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?

Information that agencies can use to assist with assessing vulnerabilities includes vendor security bulletins or the severity ratings assigned to security vulnerabilities under schemes such as the Common Vulnerability Scoring System.

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.

**Prioritisation** 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 to take into consideration the timeframes specified within the ISM (Information Security Manual. [14.11.2020]. Guidelines for System Management.) under which action must be taken as outlined in Table 1.

Table 1: Information Security Manual vulnerability remediation timeframes

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

**Response** The CMP should document response processes, including change management and documentation requirements, as well as approval processes.

The Agency response to assessed vulnerability may include risk mitigation, risk acceptance, risk avoidance/rejection, or risk sharing/transfer, in accordance with organizational risk tolerance.

Depending on the vulnerability identified and it's severity, action maybe required immediately or maybe implemented over a period of time. Agencies should ensure that they have in place the processes to track the progress of remediation actions as they occur.

**Reporting** The CMP should document requirements of reporting in relation to continuous monitoring.

This should include the specific staff and roles to generate and receive reports, the content and format of the reports, the frequency of reports, and any tools to be used.

**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 organisational threat and risk and when changes are made to HybridSystem technology and architecture. The CMP should be reviewed to ensure that it supports the organisation in operating within its acceptable risk tolerance levels, that chosen metrics remain relevant, and that data is current and complete.

The Agency should review the contents of the CMP annually or bi-annually as required by the Agencies processes.

## Microsoft Security and Compliance Centres

Microsoft 365 Security Center and Microsoft 365 Compliance Center are virtual security management workspaces provided by Microsoft's customer security and compliance teams. These solutions are integrated across Microsoft 365 services and provide actionable insights to help reduce risks and safeguard Microsoft 365 deployments.

Microsoft 365 Security Center is designed to allow for the monitoring and management of security across various identities, data, applications and infrastructure. Agencies are able to utilise Security Center to view alerts and incidents related to their infrastructure and reports and metrics such as 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 is provided by Microsoft to assist with managing system security compliance requirements, including against specific compliance frameworks. 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.

Using Microsoft's security tools can assist agencies in identifying a wide range of common security risks and misconfigurations. Examples of issues that Security Center and Compliance Center may assist with identify include:

- Administrator accounts without Multifactor Authentication enabled;
- Applications using high risk protocols to connect to Azure Active Directory;
- Endpoints without BitLocker enabled; and
- Disabled Microsoft Defender functions.

Microsoft 365 Security Center and Microsoft 365 Compliance Center can assist with aggregating, consuming and analysis of some of the system data detailed within this document.

## Collecting continuous monitoring information

The HybridSystem implements various technologies capable of monitoring security control areas that the Agency is responsible for managing as a consumer of Microsoft's cloud products. Data gathering technologies provide the capability to observe, detect, prevent or log security threats and vulnerabilities.

The Agency's security personnel can leverage technologies defined throughout this section to collect monitoring information relating to areas of security they are responsible for as a consumer of Microsoft's cloud products, including:

- User Authorisation and Authentication;
- Information Protection;
- Application Security; and
- Network Security.

### User authorisation and authentication monitoring

The Agency leveraging the HybridSystem is responsible for ongoing management of the authentication and authorisation of their users. As a result of this, the Agency is also responsible for monitoring the effectiveness of user authorisation and authentication activities within the HybridSystem. The Agency can collect continuous monitoring data pertaining to user authorisation and authentication through the following technologies:

- Azure Active Directory Identity Protection;
- Azure Advanced Threat Protection; and
- Microsoft Cloud App Security.

### Azure Active Directory Identity Protection Identification of Identity Configuration Weaknesses

Azure Active Directory (AD) Identity Protection is configured to monitor, detect and provide automated responses to anomalous authorisation and authentication activity within the HybridSystem environment. Azure AD Identity Protection provides continuous monitoring of access and authorisation to identify

vulnerabilities in identity management configuration and policies to detect actions identified as atypical to standard user behaviour, including:

- User Risk Policy – detects the probability that a user account has been compromised by detecting risk events that are atypical of a user’s behaviour.
- Sign-in Risk Policy – analyses each sign-in of a user with aim to detect suspicious actions that come along with the sign-in. Automated actions can be configured occur if high-risk behaviour is detected. Refer to Azure AD Identity Protection documentation.

## **Azure Advanced Threat Protection**

**Detecting suspicious authentication activities** Microsoft Azure Advanced Threat Protection (Azure ATP) monitors Active Directory (AD) traffic and provides alerts when suspicious authentication-related activities occur. Azure ATP provides User Entity Behavioural Analytics by monitoring authentication requests to on-premises AD Domain Controllers. Refer to What is Microsoft Defender for Identity?

## **Microsoft Cloud App Security (MCAS)**

**Monitoring and Control of Application Access** The Agency can configure MCAS access policies to provide monitoring and control of user logins to identified cloud applications. This information is displayed in the MCAS dashboard.

### **Information protection monitoring**

The Agency leveraging the HybridSystem is responsible for managing their user’s access to and handling of sensitive information. As a result of this, the Agency is responsible for monitoring the security of sensitive information transmitted to and stored within the HybridSystem. Agencies can collect continuous monitoring data of information protection controls through technologies implemented as part of the HybridSystem including:

## **Azure Information Protection**

**Information classification and sensitive information detection** Azure Information Protection (AIP) provides document and email classification labelling, and protections based on those labels, across hybrid environments. MCAS can be configured to scan for AIP classification labels and content inspection warning when new files are detected in connected apps.

**Microsoft Cloud App Security (MCAS)** MCAS components that provide information protection capabilities include:

- File Policies – can be configured to detect sensitive information stored within cloud apps.
- Admin Quarantine – creates alerts when files are matched against an MCAS file policy and stored for administrative review.
- Activity policies – monitors user activities within cloud applications.
- Session policy – provides real-time monitoring and control of user activities within authenticated sessions to identified cloud apps.

### **Application security monitoring**

Microsoft provides resources for patching the HybridSystem’s operating systems and Microsoft’s O365 applications. The Agency is responsible for configuring and deploying software applications to the operating system. As a result, the Agency is responsible for security controls of applications including:

- Application discovery;
- Conditional application access; and
- Application Control.

Agencies can collect continuous monitoring data of application security controls through technologies implemented as part of the HybridSystem including:

## Microsoft Cloud App Security

**Application discovery** MCAS utilises application discovery policies to monitor and discover new unapproved cloud applications and detect anomalous activities within connected, approved cloud applications. Refer to Create Cloud Discovery policies.

**Conditional application access** MCAS integrates with Azure AD Conditional Access to provide conditional application access controls. Agencies can configure access and session control policies to provide users with access to applications based on specific conditions (e.g. device compliance) and monitor a user's session whilst interacting with applications.

## Windows Defender Application Control

**Application control** Windows Defender Application Control (WDAC) provides the Agency with policies to detect and restrict unapproved applications users are attempting to run and restrict the code that runs in the System Core (kernel). WDAC policies can be run in audit mode to discover any applications that were installed or run since the policy was created.

## Network security monitoring

The Agency leveraging the HybridSystem is responsible for configuration and ongoing management of the network rules and network security requirements within the HybridSystem. As a result of this, the Agency is also responsible for monitoring the effectiveness of network security controls within the HybridSystem including:

- Endpoint Malware Detection;
- Email Malware Detection;
- Email Content Filtering;
- Email Policy Filtering;
- Host-based Firewalls; and
- Device Monitoring and Management.

The Agency can collect continuous monitoring data pertaining to user network security through technologies defined in this section.

**Microsoft Defender Antivirus** Microsoft Defender Antivirus provides anti-malware and spyware protection of client devices. These protections include including always-on scanning, scanning of downloaded files, dedicated protection updates and cloud-delivered protection.

## Endpoint malware detection

- Microsoft Defender Exploit Guard – Provides Host-based Intrusion Protection System (HIPS) capabilities.
- Microsoft Defender SmartScreen – Provides malware and phishing website protection including validating sites against a list of known malicious sites and downloaded files against a dynamic list of common files.

## Host-based firewall

- Microsoft Defender Firewall – Provides stateful inspection and blocking of network traffic. Windows Defender Firewall blocks unauthorized network traffic flowing into and out of the client endpoint reducing the attack surface of the device.

**Microsoft Cloud App Security** Microsoft Cloud App Security (MCAS) is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy.

**Device management** MCAS and Conditional Access App Control can identify managed devices within the organisation. Devices that are registered to Azure AD, or are present in Intune are automatically synchronised to MCAS.

**Network security device log collection** A log collector receives logs from supported firewall and proxy devices, providing processing and compression before uploading to MCAS.

### Microsoft security advisories

As a consumer of Microsoft's cloud products, the Agency is responsible for collecting Microsoft's security advisories and assessing potential impact to the system's ongoing authorisation. Security advisories should be assessed in accordance with the system's time and event driven authorisation processes. Refer to Anatomy of a Cloud Assessment and Authorisation.

### Security testing and assurance activities

Security testing and assurance activities such as vulnerability scans, penetration tests and vulnerability assessments provide objective identification and assessment of weaknesses in a system's security posture.

The Agency should perform security assurance activities on:

- Endpoint devices permitted to access HybridSystem,
- On-premises infrastructure that interfaces with the HybridSystem, and
- Gateways the Agency is responsible for.

When determining the required frequency for security testing and assurance activities, agencies should consider their current threat environment and risk tolerance.

In-line with ISM requirements, the Agency should perform vulnerability scans on systems at least monthly, and penetration tests and vulnerability assessments on all systems at least annually. Refer to Guidelines for Security Documentation.

Gateways the Agency is responsible for should be performed at irregular intervals, no more than 6 months apart<sup>27</sup>. As a consumer of Microsoft's cloud products, the Agency is not able to perform testing and assurance on system components managed by Microsoft. The Agency can verify Microsoft's IRAP assessment status via Microsoft's Service Trust Portal.

### Aggregation of continuous monitoring information

Continuous monitoring information is aggregated into security management dashboards to facilitate monitoring performed by the Agency's security team. Additionally, technologies within the HybridSystem can integrate with an Security Information and Event Management (SIEM) solution.

### Security management dashboards

Security management dashboard facilitate the aggregation of security alerts for analysis.

**Microsoft Cloud App Security (MCAS)** MCAS integrates with Microsoft Defender ATP, Azure AD Identity Protection, Azure AD Conditional Access, Azure Information Protection and Windows Defender Application Control to provide a centralised dashboard containing system security alerts and other continuous monitoring information including:

- Number of open alerts;
- Discovered apps;
- Users with high investigation priority;
- Application sessions and actions;
- Malware-infected files;
- Azure security configuration recommendations; and
- DLP alerts.

The Agency can utilise the MCAS security management dashboard monitor the ongoing security posture of the HybridSystem and collect information for reporting.



**Microsoft Defender ATP Security Centre** In addition to the MCAS integration, Microsoft Defender ATP also provides its own dashboard to aggregate and display events originating from:

- Microsoft Defender Antivirus;
- Windows Defender Application Guard;
- Windows Defender Device Guard;
- Windows Defender Exploit Guard; and
- Windows Defender SmartScreen.

Other host-based events such as registry, memory allocation and process events are discoverable in Microsoft Defender ATP Security Centre.

## **SIEM integration**

For the purposes of aggregating continuous monitoring data for analysis, the Agency can integrate technologies within the HybridSystem with their existing SIEM products.

**Microsoft Cloud App Security SIEM integration** In the HybridSystem, MCAS provides SIEM agents to enable MCAS alerts and activities to be integrated into existing security analyst workflows existing in their SIEM products. The SIEM agent only supports Micro Focus ArcSight and generic Common Event Format (CEF). Note, if both Azure ATP and MCAS are configured to send alerts to the same SIEM duplicate alerts will be received with different alert IDs. It is recommended to only send these alerts from one source.

**Azure ATP** In the HybridSystem, Azure ATP can be configured to provide the Agency's security team with syslog notifications when suspicious activities or health alerts occur. The Agency can enable their SIEM to gather all syslog notifications.

## **Analysing monitoring information**

### **Performing analysis**

Continuous monitoring information should be analysed to determine if there are vulnerabilities in the HybridSystem's configuration or deficiencies in the HybridSystem's security controls. When a vulnerability or control deficiency is identified, the Agency should use a risk-based approach to analysis. A risk assessment should be performed on the vulnerability or control deficiency in accordance with the Agency's risk assessment process defined in their Security Risk Management Plan (SRMP).

Once the risk has been identified and assessed, the risk's rating should be compared against the Agency's risk tolerance levels. Next actions and mitigation options should be considered according to their ability to meet an acceptable level of risk.

## **Responding to vulnerabilities and deficiencies**

### **Applying risk treatments**

Once a risk-based analysis of the identified system security deficiencies has been performed, the Agency should decide their next actions in accordance with their risk appetite. The Agency may choose to:

- Mitigate;
- Accept;
- Transfer; or
- Avoid the risk.

### **Patching technologies**

Many security weaknesses identified through monitoring and assurance activities are resolved through installing software patches. If patches are required to mitigate a system vulnerability, the following HybridSystem technologies can deploy software updates and security patches:

- Windows Server Update Service – WSUS enables administrators to deploy the most recent Microsoft updates, control what updates are applied and when.

- Microsoft System Centre Configuration Manager (SCCM) – SCCM integrates with a WSUS server to deliver software patch management. WSUS obtains updates from the internet and SCCM is used to approve and deploy the updates.
- Microsoft Intune – Windows Update for Business provides management policies for several types of updates to Windows 10 devices.
  - Feature updates: security and quality revisions, significant feature additions and changes
  - Quality updates: traditional operating system updates, including security, critical, and driver updates. Windows Update for Business also treats non-Windows updates (such as those for Microsoft Office or Visual Studio) as quality updates.
  - Driver updates: non-Microsoft drivers that are applicable to managed devices.
  - Microsoft product updates: updates for other Microsoft products, such as Office.