



Australian Government  
Digital Transformation Agency

# Blueprint Incident Response Plan

March 2020

Contents

**Introduction .....4**

    Overview .....4

    Purpose.....4

    Scope .....4

**Incident Response Plan.....5**

    Preparation .....5

    Detection and Analysis .....6

    Microsoft Defender ATP .....7

        Incident Criticality Assignment .....9

        Azure Service Outages.....11

        Microsoft 365 Service Outages .....11

    Containment, Eradication, and Recovery ..... 13

        Defender ATP Threat Remediation .....16

        Automated Remediation Notification .....16

    Post-Incident Activity..... 18

**Coordination with External Resources .....20**

    Microsoft Support Requests..... 20

    Australian Cyber Security Centre..... 22

**Appendix A.....23**

    Abbreviations and Acronyms ..... 23

# Introduction

## Overview

This Incident Response Plan (IRP) has been prepared to support to the Digital Transformation Agency (DTA) Blueprint. The document provides guidance for responding to cyber security incidents that may occur in relation to an Agency's operation of the Blueprint.

## Purpose

The purpose of this IRP is to provide guidance to Agencies operating the Blueprint including how to detect cyber security incidents, how to respond and remediate them, along with how to reduce the risk of an incident re-occurring in the future.

## Scope

The scope of this IRP is specific to the use of Microsoft 365 services as part of the Blueprint. As such it is termed a system-specific IRP and is designed to be subordinate to an Agency's overarching IRP. As a result, this IRP does not directly address topics that it is reasonable to assume are discussed in an Agency-level IRP.

The Blueprint IRP is a living document. It is anticipated that, over time, amendments and updates will be applied to the Blueprint IRP specific to agency business needs and lessons learnt from cyber incidents.

# Incident Response Plan

This IRP is based on the four step National Institute of Standards and Technology (NIST) incident response life cycle as documented in Special Publication 800-61 Revision 2<sup>1</sup>. The four steps of the process are illustrated in *Figure 1* and are:

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity.

*Figure 1 Incident Response Process*



Each of the four incident response phases are detailed in the following sections of this document.

## Preparation

The preparation phase of the incident response life cycle is a shared responsibility between the project team and Agency cyber security personnel. The project team is responsible for the design, implementation, and security assessment of the solution. This includes performing a risk assessment and determining which specific Information Security Manual (ISM) controls to implement to reduce and manage the risk of security incidents. The following documentation has been produced for the Blueprint and it is recommended that the Agencies cyber security personnel familiarise themselves with the content to aid them in their preparation to manage an incident:

- **DTA – Solution Overview** which describes the solution, which features have been enabled/disabled for the Agency, and how the solution has been structured.
- **DTA – Blueprint Security Risk Management Plan (SRMP)** which includes the details of the risk assessment performed and the recommended treatments.
- **DTA – Blueprint System Security Plan (SSP)** which describes how controls identified in the SoA are implemented by the system.
- **DTA – Blueprint System Security Plan Annex** which states the compliance of the solution with the October 2019 version of the ISM.
- **DTA – Standard Operating Procedures** which describe the steps required to perform multiple operational tasks within the environment.
- **DTA – Platform Detailed Design** which describes the technologies used that make up the 'platform' portion of the solution and how they are implemented.

<sup>1</sup> Computer Security Incident Handling Guide. [August 2012]. Available at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

- **DTA – Workstation Detailed Design** which describes the technologies used that make up the Windows 10 portion of the solution and how it is implemented.
- **DTA – Office 365 Detailed Design** which describes the technologies used that make up the Office 365 portion of the solution and how it is implemented.

In addition to having ongoing access to the above documentation it is assumed that Agency cyber security personnel have access to tools and resources as described in the Agency IRP.

Specific resources that are also required by Agency cyber security personnel to detect and respond to security incidents include:

- Access to the various Microsoft management portal required to administer the Blueprint, as listed below in Table 1
- Membership of the role(s) required to perform any actions related to the incident

*Table 1 Microsoft Management Portals*

Portal	URL
Microsoft Defender ATP portal	<a href="https://securitycenter.windows.com">https://securitycenter.windows.com</a>
Cloud App Security portal	<a href="https://portal.cloudappsecurity.com">https://portal.cloudappsecurity.com</a>
Azure portal (including Azure AD)	<a href="https://portal.azure.com">https://portal.azure.com</a>
Microsoft 365 Compliance Center	<a href="https://compliance.microsoft.com">https://compliance.microsoft.com</a>
Microsoft 365 Security Center	<a href="https://security.microsoft.com">https://security.microsoft.com</a>
Office 365 homepage	<a href="https://portal.office.com">https://portal.office.com</a>

## Detection and Analysis

Multiple detection methods are available to the Agency's cyber security personnel to aid them in discovering and categorising security incidents. These detection methods include:

- **Alerts from Azure AD (including Azure AD Identity Protection)** including risky sign-ins and users flagged for risk.
- **Azure AD logs** stored in Azure and available via the portal, including the audit log for all administrative activities relating to Azure AD.
- **Office 365 ATP alerts and reports** for each of the ATP capabilities including Safe Attachments, Safe Links, ATP for SharePoint, OneDrive and Microsoft Teams, and ATP anti-phishing protection.
- **Microsoft Defender ATP** including the Security Operations, Incidents, and Alerts Queue dashboards which provide tailored information and actions for cyber security personnel.
- **Microsoft Cloud App Security (MCAS)** Threat Detection, Privileged Accounts, and Access Control dashboards spanning the whole Microsoft 365 deployment, along with configurable email alerts and automatic response capabilities.

- **Local Windows 10 events logs** written to each Windows 10 endpoint including authentication attempts, firewall activities, and Windows Defender Application Control (WDAC) events.

Due to its containment, eradication and recovery capabilities in addition to its detection and analysis functionality, Microsoft Defender ATP is the primary incident response tool for the Blueprint and is described in further detail in the section below.

## Microsoft Defender ATP

The solution leverages Microsoft Defender ATP to monitor, detect, investigate, and respond to threats targeting Windows 10 endpoints. When an alert is triggered of sufficient severity, an email is automatically sent to a specified recipient email address (typically the Agency cyber security team mailbox or similar). Additional email recipients can be configured as required.

### Recommendation

Agency should ensure a recipient email address (typically the Agency cyber security team mailbox or similar) shared with multiple users is created and monitored.

A majority of alerts generated within the Microsoft Defender Security Center – the Microsoft Defender ATP portal – relate to automatically detected issues and are informational in nature. This means that they are not necessarily harmful to the system but must be reviewed and accounted for. Alerts are organised by severity as they enter the 'Alerts queue', the severity of which is detailed below in *Table 2*.


*Table 2 Microsoft Defender Security Center Alert Severities*

Severity	Description
<b>High</b>	Threats marked as <b>High</b> have the potential to cause severe damage to the system and devices using it. These alerts must be treated with urgency.
<b>Medium</b>	Threats marked as <b>Medium</b> must be treated with some importance but typically will indicate anomalous behaviour within the environment such as the execution of suspicious files, un-sanctioned registry changes, or observed behaviours typical of a cyber threat or attack.
<b>Low</b>	<b>Low</b> urgency threats will typically be identified as commercial/known malware or hacking tools, their function is generally well understood and the ability to stop it is high.
<b>Informational</b>	<b>Informational</b> alerts are those that might not be considered harmful to the network but are good to track.

*Figure 2* shows an example of an alert from Defender ATP which detected a suspicious sequence of activities and automatically generated an incident detailing the severity, timestamps, devices affected, applications called, and more.

Figure 2 Suspicious sequence of activities

⚡ Alerts > ⚡ **Suspicious sequence of exploration activities**



**Suspicious sequence of exploration activities**  
This alert is part of incident (3)

Automated investigation is not applicable to alert type

Alert context

<device>  
<domain/username>

First activity: 01.13.2020 | 04:52:32  
Last activity: 01.13.2020 | 04:54:10

Severity: Low  
Category: Discovery  
Technique: T1018: Remote System Discovery, T1087: Account Discovery, T1016: System Network Configuration Discovery, T1135: Network Share Discovery, T1049: System Network Connections Discovery  
Detection source: EDR  
Detection technology: Behavioral  
Detection status: Detected

Actions

Description

A process called a set of windows commands. These commands can be used by attackers in order to identify assets of value and coordinate lateral movement after compromising a machine.

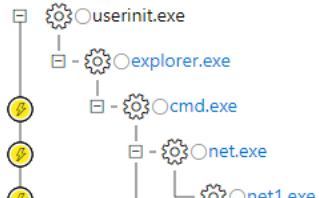
Recommended actions

Validate the alert

1. Check with the user of this machine to see if
2. Review the machine timeline for suspicious i after the time of the alert.
3. If you determine this to be a true positive, c

Show more

Alert process tree



When the Agency's cyber security personnel receive an alert, they should perform analysis to determine the cause and any potential impact, including recommended actions within the Microsoft Defender Security Center portal. If an alert occurs during an approved change window and relates directly to the contents of the change, for example an unapproved/not whitelisted executable runs during an application deployment, then it is unlikely that a security incident has occurred. However, if an alert is triggered outside of a change window and without an obvious cause then the probability of the event being a security incident probable.

**Note,** Microsoft assign a criticality to each alert based on an internal rating system. It is up to the Agency's cyber security team to make their own assessment of the criticality of all potential security incidents in accordance with the Agency's overarching IRP.

The assignment of criticality to an incident is an important step and due care must be applied to avoid the risks associated with both under and over classifying an incident. If there is ever any doubt, cyber security personnel should always investigate further.

The alerts captured in the Defender Security Center should be leveraged by Agency cyber security personnel to detect and analyse potential security incidents. The Windows Defender ATP portal provides far deeper detail than is available from the email alerts, these emails should only serve as a cursory notification, not an in-depth analysis of the incident.

Within the Defender Security Center there are two capabilities that should be utilised by Agency cyber security personnel for the purpose of detection and analysis of incidents on a day-to-day basis.

- **Incidents** lists all automatically generated incidents detected by Defender ATP, including the severity of the incident, the machines and users involved, last activity, assignment of the incident, et cetera. All incidents should be assigned as they are generated and managed based on the Agency's operating procedures by cyber security personnel.
- **Alerts queue** lists all alerts based on the alert type not the incident case that is generated, this can be supremely helpful when attempting to identify patterns of behaviour. This alerts queue will also sort by severity, which incident it is related to, status, and investigation state.

For both the Incidents and Alerts queue Agency cyber security personnel can select individual records to access detailed information on the specific activity.

## Incident Criticality Assignment

Regardless of the detection source for a potential incident, all incidents should be assigned a criticality in a consistent manner. In accordance with guidance issued by the Agency's Information Technology Security Adviser (ITSA) or other personnel responsible for the daily operational information security of the Agency, all incidents should be assigned a system specific criticality. The criticality ratings for incidents have been developed from a number of Federal Government Agencies' overarching risk frameworks, specifically the consequence definitions. These definitions are listed below in *Table 3*.

Note, if incident criticality definitions are included in the Agency IRP cyber security personnel should use those in preference to the criticalities defined below. The Business Impact Levels (BILs) defined in the Protective Security Policy Framework (PSPF) should also be considered in the assessment of incident criticalities.



Table 3 Incident Criticality Definitions

Incident Criticality	Performance Metrics	Reputational Metrics
<b>Extreme</b>	<ul style="list-style-type: none"> <li>Major impact on departmental outcomes and performance</li> <li>Requires major additional management effort by Senior Executive to control the impact</li> <li>Unavailability of agency mission critical systems including the delivery of Government outcomes (e.g. a public facing system that is used in emergency procedures, a grants system)</li> <li>Catastrophic breach and or loss and or destruction of agency information containing sensitive and personal information of Australian citizens and or classified information</li> </ul>	<ul style="list-style-type: none"> <li>Significant adverse publicity</li> <li>Loss of stakeholder confidence requiring intervention by Secretary</li> <li>Reporting to accountable authorities outside of the Agency e.g. Privacy Commissioner, Minister of Department etc</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>Moderate impact on achievement of outcomes and performance</li> <li>Requires additional management effort by business area, Senior Executive to control the impact</li> </ul>	<ul style="list-style-type: none"> <li>Substantial adverse publicity</li> <li>Loss of stakeholder confidence requiring intervention at Executive level</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Minor impact on achievement of outcomes and performance</li> <li>Requires additional management effort within the business area to control the impact</li> </ul>	<ul style="list-style-type: none"> <li>Some adverse publicity</li> <li>Minor loss of stakeholder confidence</li> </ul>
<b>Low</b>	<ul style="list-style-type: none"> <li>Insignificant impact on achievement of outcomes and performance</li> </ul>	<ul style="list-style-type: none"> <li>Some adverse publicity</li> <li>Minor loss of stakeholder confidence</li> </ul>

Agency cyber security personnel should use the above table to define the criticality of incidents based on the data available to them at the time of detection and analysis. If this data is updated or found to be inaccurate Agency cyber security personnel should re-assess the criticality of the related incident(s). The criticality of an incident should be used to determine the resources, timeframes and reporting requirements related to it.

## Azure Service Outages

An additional data source that can be leveraged by Agency cyber security personnel when analysing potential security incidents is the Azure status dashboard. This dashboard is published by Microsoft and reports on the current status of all Azure-based services, including any current warnings or errors. An example of the dashboard is shown below in *Figure 3*.

The Azure status dashboard is available at <https://status.azure.com/> and does not require the user to be logged into Azure to view the current status.

Figure 3 Azure Status Dashboard

Microsoft Azure

Contact Sales: 1-800-867-1389

Search

My account

Portal

Overview
Solutions
Products
Documentation
Pricing
Training
Marketplace
Partners
Support
Blog
More

# Azure status

Last updated 12 seconds ago

RSS

Refresh every

2 minutes

Good
 Warning
 Error
 Information

	Americas	Europe	Asia Pacific	Azure Government								
PRODUCTS AND SERVICES	NON-REGIONAL*	SOUTHEAST ASIA	EAST ASIA	AUSTRALIA EAST	AUSTRALIA SOUTHEAST	AUSTRALIA CENTRAL	AUSTRALIA CENTRAL 2	CENTRAL INDIA	WEST INDIA	SOUTH INDIA	JAPAN EAST	JAPAN WEST
COMPUTE												
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SAP HANA on Azure Large Instances				✓	✓							✓
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Agency cyber security personnel can use the dashboard to determine if a potential incident is local to the Agency's system or is a widespread issue affecting the underlying Azure service(s).

### Recommendation

It is recommended that at least one Agency cyber security personnel member is subscribed to the provided Rich Site Summary (RSS) feed to receive updates whenever an Agency-leveraged service is affected.

## Microsoft 365 Service Outages

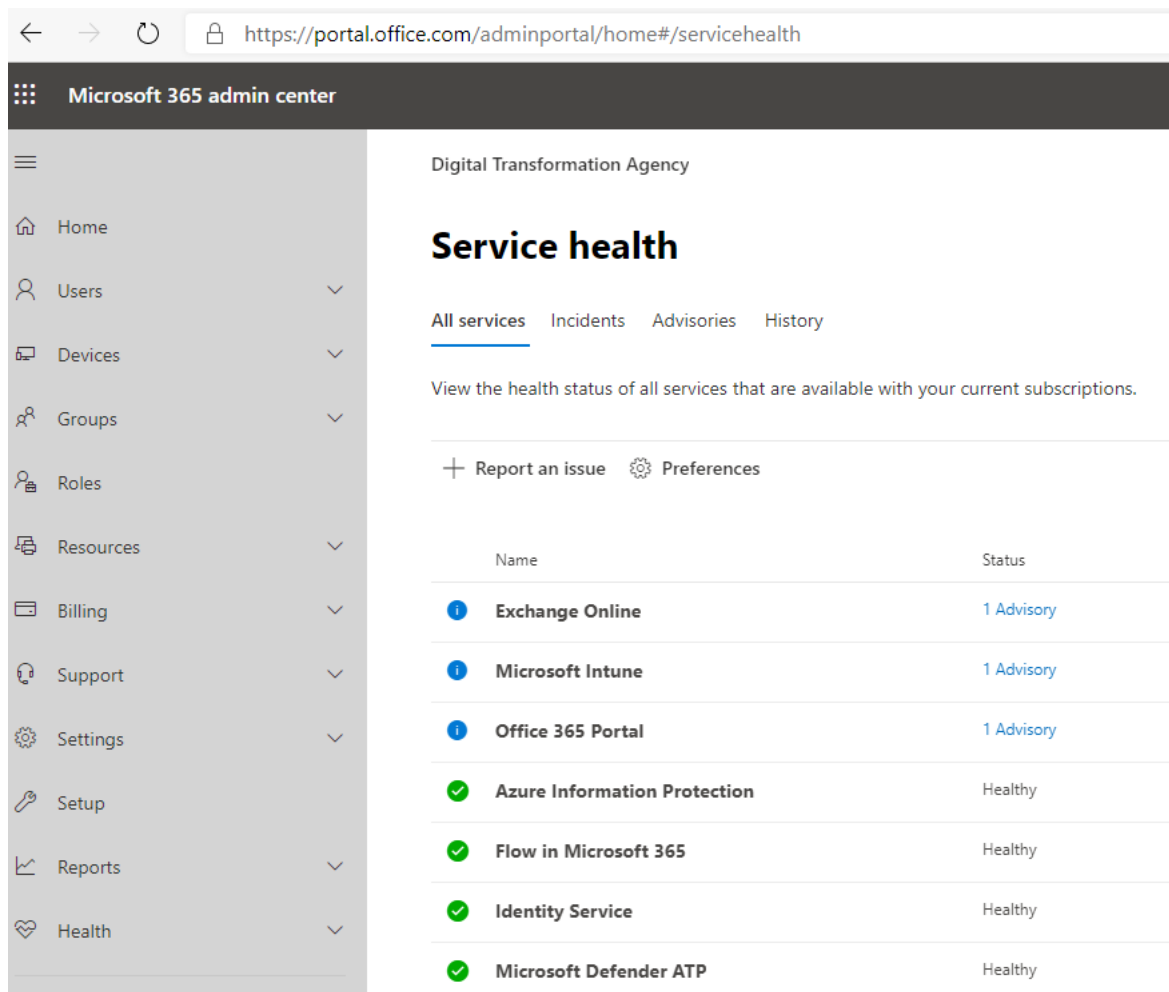
Agency cyber security personnel should review the Microsoft 365 service status (including all Office 365 services) when investigating an incident relating to availability. The following resources are available from Microsoft to identify the status of Microsoft 365 services:

- **Microsoft 365 Service health status** - <https://portal.office.com/adminportal/home#/servicehealth>
- **Microsoft 365 Status Twitter** - <https://twitter.com/msft365status?lang=en>

In the first instance the Microsoft 365 Service health status page should be consulted, followed by the Microsoft 365 Status Twitter account. If no issues are identified by either of these resources, then Agency-specific scenarios should be explored such as loss of Internet connect, Local Area Network (LAN) outage, etc.

As an example on how to navigate the Microsoft 365 Service health status page, please refer to *Figure 4* below.

*Figure 4 Office 365 Service Outages*

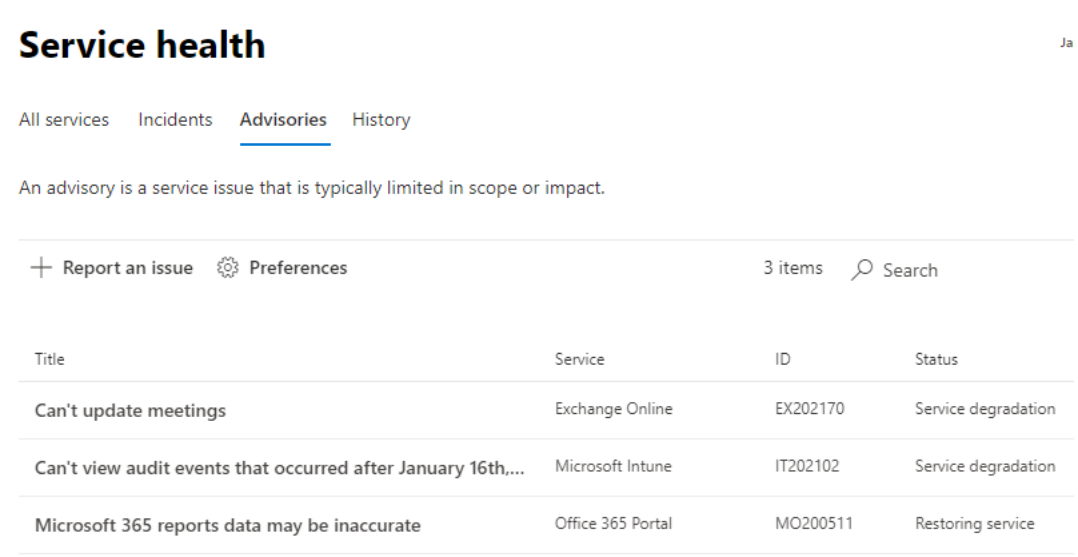


The screenshot shows the Microsoft 365 admin center interface. The left sidebar contains navigation links: Home, Users, Devices, Groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, and Health. The main content area is titled 'Service health' and includes tabs for 'All services', 'Incidents', 'Advisories', and 'History'. Below the tabs, there is a table listing the health status of various services.

Name	Status
Exchange Online	1 Advisory
Microsoft Intune	1 Advisory
Office 365 Portal	1 Advisory
Azure Information Protection	Healthy
Flow in Microsoft 365	Healthy
Identity Service	Healthy
Microsoft Defender ATP	Healthy

Agency cyber security personnel can use the dashboard to determine if a service is down, whether the issue is widespread and affecting the underlying services, or whether there is no identified outage. This page can also be used to review ongoing service advisories such as those identified below in *Figure 5*.

Figure 5 Office 365 Service Health Advisories



Recommendation

It is recommended that at least one Agency cyber security team member, or another person assigned with cyber security responsibilities, review these services daily to ensure there are no ongoing service outages that will affect the availability.

Containment, Eradication, and Recovery

The Agencies cyber security teams’ approach to containment, eradication, and recovery – particularly in relation to resource allocation and priority – should be based on the category of the incident as previously described. However, regardless of the criticality of an incident the basic actions that are required to address the incident are dependent on the specific incident type.

This IRP defines specific incident types that are directly related to the solution, namely:

- Violation of confidentiality of Agency data stored in Office 365 (including Exchange Online)
- Violation of integrity and/or confidentiality of Azure AD accounts
- Violation of integrity of Azure AD configuration
- Violation of integrity of Office 365 configuration
- Loss of availability of Agency data stored in Office 365

The following table provides recommendations for the containment, eradication, and recovery activities associated with the above incident types:

Table 4 Incident Containment, Eradication, and Recovery Activities

Incident type	Containment, Eradication, and Recovery Activities
<p>Violation of confidentiality of Agency data stored in Office 365</p> <p><i>(For example, sensitive information is sent outside the organisational boundaries – data spill)</i></p>	<p><b>Containment</b> – Data Loss Prevention (DLP) policies are in place across Microsoft Teams, Exchange Online, SharePoint Online, and Outlook. All data stored in these corporate data locations is backed by policies to block the egress of what is identified as ‘sensitive’. Note, if DLP policies have been disabled or modified they should be re-enabled and verified by referring to the relevant ABAC.</p> <p><b>Eradication</b> – DLP policies automatically block messages from being sent or redacts and obfuscates data attempting to leave organisational boundaries.</p> <p><b>Recovery</b> – Recovery of sensitive information is automated by DLP. User notifications are linked to DLP policies upon creation. The Agency cyber security team should review DLP policies often to ensure they align with business needs. New policies should be created based on commonly used applications within the organisation.</p>
<p>Violation of integrity and/or confidentiality of Azure AD account(s)</p> <p><i>(For example, user or administrative account compromised)</i></p>	<p><b>Containment</b> – Compromised account credentials can result in catastrophic damage to the system if the account in question has administrative privileges, and breaches of sensitive data. To contain this, Conditional Access and Multi-Factor Authentication (MFA) are employed to control access to all accounts, even if account credentials are compromised. Agency cyber security personnel can perform a global account sign-out and password reset if an account is suspected of being compromised.</p> <p><b>Eradication</b> – Compromised accounts can be disabled from log-ins, passwords reset, and global sign-outs initiated. Agency cyber security personnel should review Azure AD logs to identify the source of the breach from an identity perspective. They should also review sharing audit logs against SharePoint Online and OneDrive for Business prior to the user being given their account credentials back. Additionally, a full audit of the user's log-in habits should be performed to ensure they comply with Agency security requirements.</p> <p><b>Recovery</b> – Once the incident has been remediated the users account should be re-enabled, password reset, and access granted. Simultaneous to this, the Agency cyber security team are to review all appropriate logs dependant on the breach.</p>
<p>Violation of integrity of Azure AD configuration</p> <p><i>(For example, unapproved changes are made to Conditional Access policies)</i></p>	<p><b>Containment</b> – Unauthorised changes to Conditional Access policies can result in gaps within the approved authentication process. To prevent these changes Privileged Identity Management should be utilised to only grant temporary permissions to perform privileged tasks.</p> <p><b>Eradication</b> – Agency cyber security personnel should revert any changes made to the configuration in alignment with the configuration outlined in the ‘DTA – Platform – Detailed Design’ and ‘DTA – Conditional Access – ABAC’ documents.</p> <p><b>Recovery</b> – Ensure all changes have been reverted, to ensure this has been completed successfully refer to the design and ABAC documents. Once the change(s) have been reverted any further authentication attempts will need to pass the conditional access policies. Measures should be in place to record any security incidents and unexpected changes to the configuration due to lack of knowledge.</p>

Incident type	Containment, Eradication, and Recovery Activities
<p>Violation of integrity of Office 365 configuration</p> <p><i>(For example, DLP or retention policies are disabled or modified without authorisation)</i></p>	<p><b>Containment</b> – DLP and retention policies are in place to ensure sensitive data does not improperly leave organisational boundaries. DLP is controlled by Azure AD permissions, as such, all access to it should be controlled by Privileged Access Management (PIM). In the event of an incident PIM can be used to restrict administrative privileges to prevent further changes and provide an audit log of previous actions.</p> <p><b>Eradication</b> – Agency cyber security personnel should revert any changes made to the configuration in alignment with the configuration in the 'DTA – Office 365 – Detailed Design' document. The Azure AD and PIM logs should be scrutinised to review by whom the unapproved change was made.</p> <p><b>Recovery</b> – Ensure all changes have been reverted, to ensure this has been completed successfully refer to the design and ABAC documents. Agency cyber security personnel should review the last modified time of the affected policy and align it with PIM logs. A review of all privileged users and groups is recommended.</p>
<p>Loss of availability of Agency data stored in Office 365</p> <p><i>(For example, the Microsoft Teams service is unavailable, and critical corporate data cannot be accessed)</i></p>	<p><b>Containment</b> – Service availability within the Office 365 and Azure environments is very high, if however, a service is offline or otherwise inaccessible, the Agency cyber security team should ensure the status of the service via the Microsoft 365 Service Health Status portal (see: Microsoft 365 Service Outages). If Microsoft Teams is inaccessible, secondary pathways to the data should be explored, for example, accessing the Teams back-end SharePoint Online site.</p> <p><b>Eradication</b> – Not applicable for availability incidents.</p> <p><b>Recovery</b> – The service is controlled by Microsoft and its availability is backed by Microsoft service level agreements.</p>
<p>Loss of availability of Agency data stored in Office 365</p> <p><i>(For example, the Microsoft Teams service is unavailable, and critical corporate data cannot be accessed)</i></p>	<p><b>Containment</b> – Service availability within the Office 365 and Azure environments is very high, if however, a service is offline or otherwise inaccessible, the Agency cyber security team should ensure the status of the service via the Microsoft 365 Service Health Status portal (see: Microsoft 365 Service Outages). If Microsoft Teams is inaccessible, secondary pathways to the data should be explored, for example, accessing the Teams back-end SharePoint Online site.</p> <p><b>Eradication</b> – Data Loss Prevention policies are in place to ensure sensitive information across all corporate data locations is identified and not allowed to leave the organisational boundaries. If access to the data sources is compromised, Microsoft service level agreements should be referred to.</p> <p><b>Recovery</b> – The service is controlled by Microsoft and its availability is backed by Microsoft service level agreements.</p>

**Note**, the activities listed above are designed to aid Agency cyber security personnel in responding to the specific incident types defined. However, this is not an exhaustive list of all possible responses. Agency cyber security personnel should use their judgement to determine if they are appropriate to a specific incident or if other actions should be taken.

## Defender ATP Threat Remediation

Defender ATP provides the ability to automate responses to detected threats, reducing the total response time for an incident and eliminating the need for manual actions to be taken by the Agency's cyber security team. Five levels of automation are available as listed below:

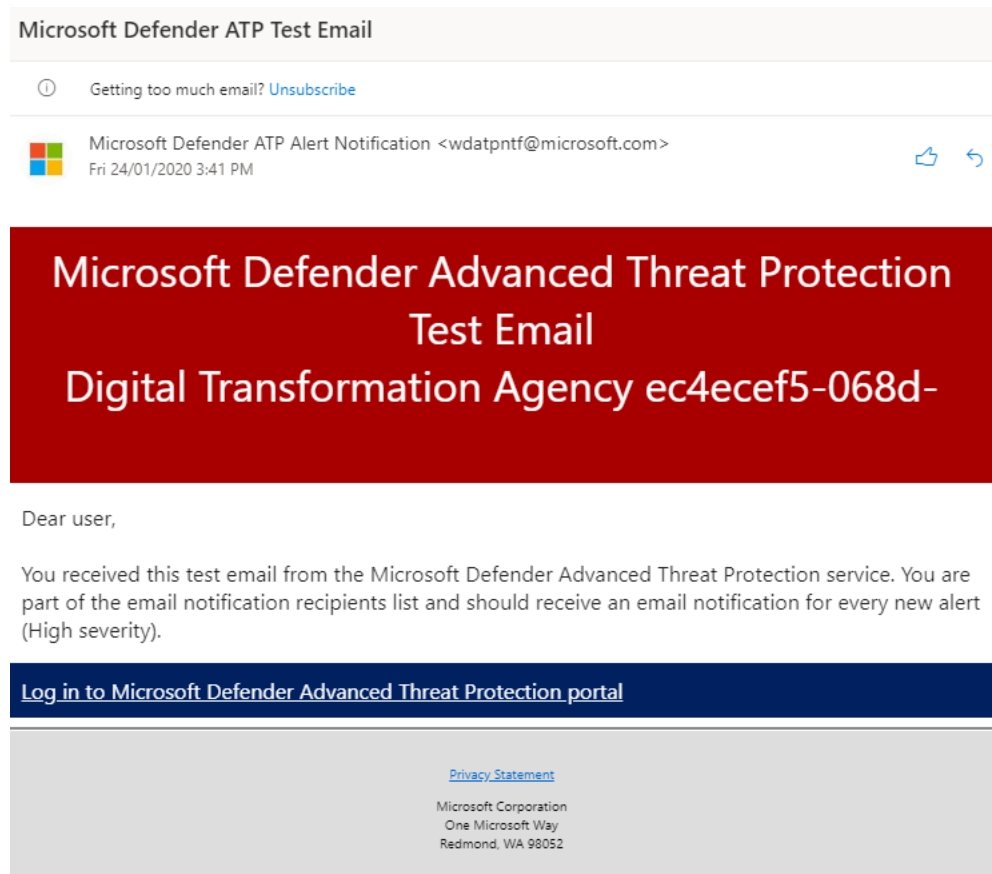
1. **No automated response** – automated investigations are not run, and all activities must be performed by the Agency's cyber security team.
2. **Semi (any folder)** – approval is required from the cyber security team for all remediation activities suggested as part of an automated investigation.
3. **Semi (non-temp folders)** – remediation occurs automatically for temporary folders including users' download folders, remediation for other locations requires approval.
4. **Semi (core folders)** – remediation occurs automatically for all folders other than operating system directories (e.g. Program Files and Window).
5. **Full** – all remediation activities are performed automatically.

The Blueprint uses the default Defender ATP configuration for automated investigations, namely semi (any folder). Therefore, Agency cyber security personnel will be prompted to approve all remediation activities that are recommended as part of Defender ATP automated investigations. The automation level can be adjusted if required based on the specific requirements of the Agency's cyber security personnel.

## Automated Remediation Notification

Depending on the nature of the initial alert, if Microsoft Defender ATP detects a threat and it is resolved automatically it will notify administrators by sending a follow up email. An example of an alert resolution email is shown below in *Figure 6*.

Figure 6 Alert Resolution Email



Agency cyber security personnel should be aware of these notifications but should not rely on them as a trigger to cease investigation and/or recovery activities.

### Recommendation

It is recommended that Agency cyber security personnel verify that an incident resulting from alert is actually resolved before moving to the post-incident phase.



## Post-Incident Activity

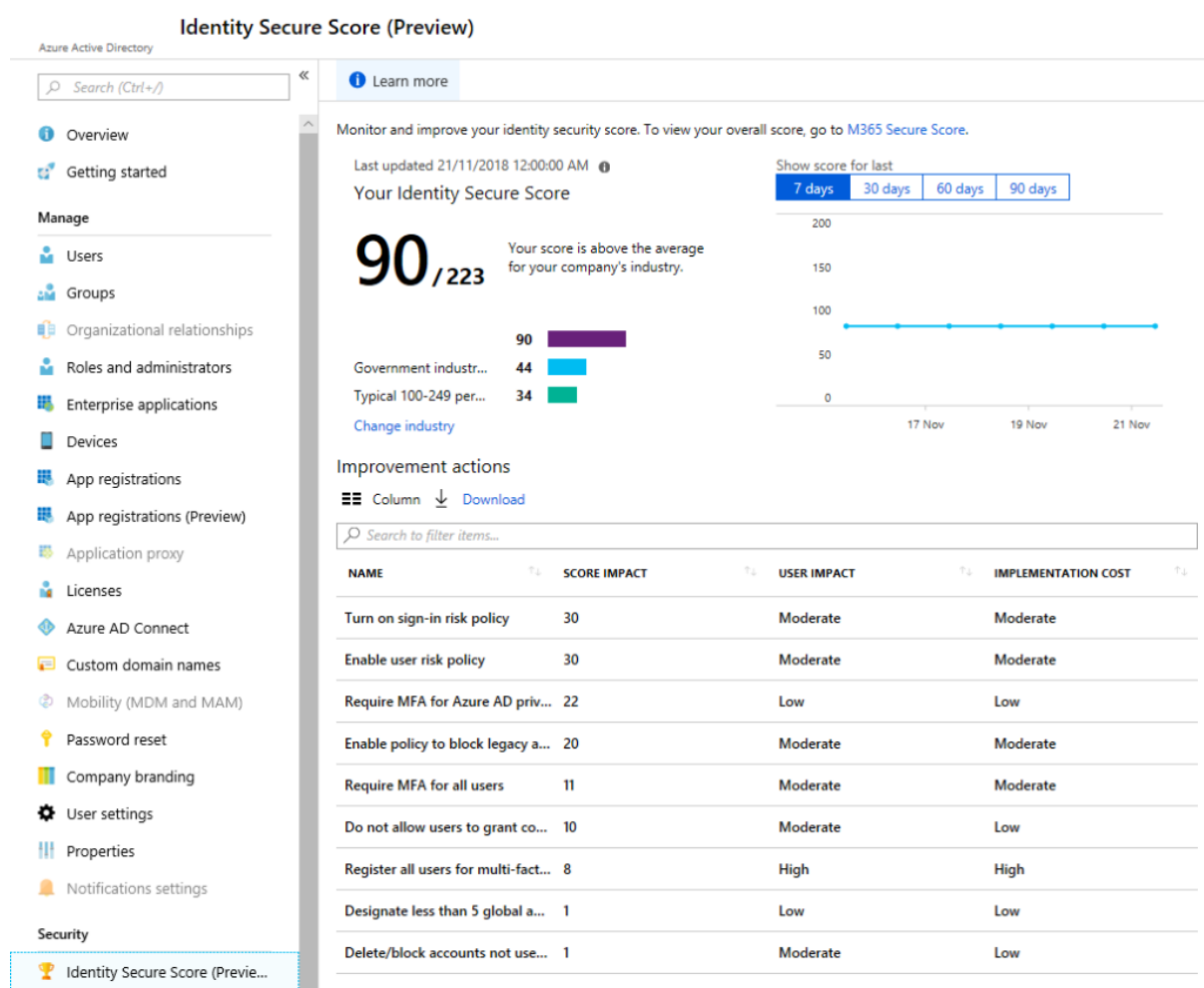
In accordance with the Agency's overarching IRP recommendation, 'lessons learnt' meetings should be held after all major incidents. However, for incidents it is recommended that one of these meetings is held after every incident. This provides an opportunity to assess the current controls in place and evaluate if additional controls can be applied to prevent or minimise the effect of a similar incident occurring again.

Due to the regular update cadence for Azure and Office 365, new features are made available monthly. This often includes Preview features in Azure that provide enhanced capabilities but are still under development by Microsoft. One of the goals of the post-incident meetings should be to assess newly released and preview features for their potential to reduce the risk of the incident re-occurring. This may require specialist resources to attend to present newly available features and discuss how implementing them may reduce the risk to the system.

Note, new capabilities and services – including all Preview features – should be assessed by Agency cyber security personnel before being enabled.

Figure 7 illustrates how a preview feature is presented in the Azure portal using the "... (Preview)" suffix to the feature/service name.

Figure 7 Azure AD Preview Feature



**Note**, as of the time of writing the Azure AD Identity Secure Score feature is no longer in preview and is generally available for all tenants.

The outcomes of all post-incident meetings should be recorded in the report prepared for each incident. This ensures there is a document chain of events for the incident including tasks that will now be undertaken due to the analysis of the incident, but potentially not directly related (for example applying an additional control to prevent a future incident). This report may be the subject of an internal or external audit in accordance with the Agencies reporting requirements and therefore should be treated as a formally controlled document and stored in accordance with existing policies. Additionally, any information collected as part of the incident response should be either be directly included in the report, or its storage location referenced, as applicable.

All other aspects of the 'lessons learnt' meetings and reporting requirements should be undertaken in accordance with the recommendations provided in the Agency's overarching IRP.

## Coordination with External Resources

In some cases, Agency cyber security personnel may require the assistance of additional external resources to aid in one or more phases of the *Incident Response Life Cycle*. When this is required, Agency cyber security personnel should follow existing Agency policies and procedures to appropriately engage and communicate with external resources to assist with incident management and response.

## Microsoft Support Requests

With the introduction of Azure AD an additional external resource becomes available to assist Agency cyber security personnel manage and respond to security incidents. Microsoft *Support Requests* can be made from within the Azure Portal to report issues and access assistance with all Azure hosted services, including Azure AD, Azure MFA, and Conditional Access. *Support Requests* are associated with Azure Subscriptions, and a user must have 'write permissions' for the subscription to raise a support request.

The New *support request* wizard provides a three-step process to detail and submit new support requests via the Azure Portal. The three steps are:

- **Basics** – which includes the issue type (most likely to be technical if raised in relation to a security incident), the subscription affected and the specific service. This is illustrated below in *Figure 8*.
- **Problem** – which includes a technical description of the issue/incident including severity, problem type, category, title, and details. It also provides fields to identify when the problem started and provide the option for the user to upload a file.
- **Contact information** – which includes contact details for a Microsoft engineer to use to assist with the support request. Depending on the reported severity of the issue the *Preferred contact method* and Response may be auto-filled (for example, high severity requests default to phone and 24x7 respectively).

Figure 8 New Support Request

**New support request**  
HELP + SUPPORT

**Basics**  
NEW SUPPORT REQUEST

Try our new case submission experience to submit your request →

\* Issue type  
Technical

\* Subscription  
[Empty]

Can't find your subscription? [Show more](#)

An Azure service outage may be impacting this subscription.

\* Service  
Choose a service

**Azure Active Directory**

- Azure Active Directory App Integration and Development
- Azure Active Directory Compliance and Reports
- Azure Active Directory Directories, Objects and Synchronization
- Azure Active Directory Domain Services
- Azure Active Directory External Users (B2C & B2B)
- Azure Active Directory Sign-In and Multi-Factor Authentication

The progress of support requests can also be tracked from within the Azure Portal under the Help + support page. This is illustrated below in Figure 9.

Figure 9 All Support Requests

Home > Help + support  
Help + support

Search (Ctrl+J)

Overview

SUPPORT

- New support request
- All support requests
- Support plans

HEALTH

- Service issues
- Planned maintenance
- Health advisories
- Health history
- Resource health

GENERAL

- Advisor
- Get started with Azure

Have you tried one of these?

- Get started**  
Learn about Azure's most-used features
- Documentation**  
Azure tutorials and how-to articles
- Learn about billing**  
Tips for monitoring usage and understanding your bill
- Support plans**  
Choose the right Azure support plan

Community

- MSDN Forums**  
Information and discussion by Microsoft and the community  
[MSDN forums](#)
- Stackoverflow**  
Answers to a wide range of Azure programming issues  
[Azure @ Stackoverflow](#)
- @AzureSupport**  
Quickly connect with our problem-solving experts  
[Tweet @AzureSupport](#)
- Serverfault**  
Answers to network infrastructure problems  
[Azure @ Serverfault](#)

Recent support requests

[+ New support request](#) | [Choose the right support plan](#)

TITLE	ID	CREATED (UTC)	SUBSCRIPTION	RESOURCE TYPE	UPDATED	STATUS
users having reader permissions to subscrip...	118041217987367	Thu, Apr 12, 2018, 7:39:05 ...		Subscription management	5 hrs ago	Open
Test ticket	118041217987285	Wed, Apr 11, 2018, 10:43:0...		File	9 hrs ago	Closed
This is test case. Please ignore.	118041217987135	Wed, Apr 11, 2018, 10:10:3...		Virtual Machine running ...	9 hrs ago	Closed
Quota request for Azure RemoteApp	118041117984951	Wed, Apr 11, 2018, 9:08:12 ...		Quota	20 hrs ago	Closed
Quota request for Batch	118041117984949	Wed, Apr 11, 2018, 9:07:51 ...		Quota	20 hrs ago	Closed

[See all support requests](#)

For more information on creating Azure support requests, including any updates to the process, refer to <https://docs.microsoft.com/en-us/azure/azure-supportability/how-to-create-azure-support-request>

## Australian Cyber Security Centre

In the case where an incident has not been able to be resolved using the steps defined previously, the ACSC may be engaged by agency approved staff as per the Agency's overarching IRP.

An incident can be reported to the ACSC via the following methods:

- Website - <https://www.cyber.gov.au/contact>
- Phone number – 1300 CYBER1 (1800 292 371)
- Email – [asd.assist@defence.gov.au](mailto:asd.assist@defence.gov.au)

**Note**, reporting an incident via the phone is preferred when the incident is considered urgent by the Agency.

# Appendix A

## Abbreviations and Acronyms

Table 5 details the abbreviations and acronyms used throughout this document.

Table 5 Abbreviations and Acronyms

Acronym	Meaning
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
ATP	Advanced Threat Protection
Azure AD	Azure Active Directory
BIL	Business Impact Levels
DLP	Data Loss Prevention
DTA	Digital Transformation Agency
IRP	Incident Response Plan
ISM	Information Security Manual
ITSA	Information Technology Security Adviser
LAN	Local Area Network
MCAS	Microsoft Cloud App Security
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
PIM	Privileged Access Management
PSPF	Protective Security Policy Framework
RSS	Rich Site Summary
WDAC	Windows Defender Application Control