

Part 6c – Insider Risk Management

Policies

(Insider Risk Management)

Contents

Disclaimer.....	1
Target Audience.....	2
Document Scope.....	2
Out-of-Scope.....	2
Use Case.....	3
Overview of Document.....	3
Definitions.....	3
Notes.....	4
Pre-requisites.....	4
Part 1 - Policies.....	4
Appendix and Links.....	8

Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience

The Insider Risk Management section of this blog series is geared toward Security and Compliance officers who need to monitor users behavior when it comes to compliance data.

Document Scope

This document is meant to guide an administrator who is “net new” to Microsoft E5 Compliance through the use of Insider Risk Management (IRM).

It is presumed that you already data to search inside your tenant.

We will only step through a basic eDiscovery case (see the Use Case section).

This is will only cover the Policies aspect of IRM

Out-of-Scope

This document does not cover any other aspect of Microsoft E5 Compliance, including:

- Sensitive Information Types
- Exact Data Matching
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices
- Microsoft Cloud App Security (MCAS)
- Records Management (retention and disposal)
- Overview of Advanced eDiscovery (AeD)
- Reports and Analytics available in of Advanced eDiscovery (AeD)

It is presumed that you have a pre-existing of understanding of what Microsoft E5 Compliance does and how to navigate the User Interface (UI).

It is also presumed you are using an existing Information Types (SIT) or a SIT you have created for your testing.

As it relates to Insider Risk Management we will not be covering:

- Permissions
- Settings
- Alerts
- Cases (investigations)
- Users
- Notifications
- Creation of Advanced eDiscovery Cases from IRM

If you wish to set up and test any of the other aspects of Microsoft E5 Compliance, please refer to Part 1 of this blog series (listed in the link below) for the latest entries to this blog. That webpage will be updated with any new walk throughs or Compliance relevant information, as time allows.

[Microsoft Compliance - Paint By Numbers Series \(Part 1\) - Sensitive Information Types - Microsoft Tech Community](#)

Use Case

There are many use cases related to accessing and sharing of sensitive data. One example is – A user is accessing and sharing sensitive data on a regular basis and management needs to know if there are any spikes in access or sharing of that information that might coordinate with negative HR reports, resignations, etc.

Overview of Document

We will walk through a new policy to create a Data Leakage policy. This will monitor activities based on the exfiltration of data. This exfiltration should have been done in Part 3 of the this blog series.

Definitions

- Data Theft – This means data taken/stolen by departing users near their resignation or termination date.
- Data Leakage – Data leaks can range from accidental oversharing of information outside your organization to data theft with malicious intent.
- Indicators – Indicators included in insider risk management policies used to determine a risk score for an in-scope user. These policy indicators are only activated after a triggering event occurs for a user.
- Thresholds – Each indicator uses default thresholds that influences an activity's risk score, which in turn determines whether an alert's severity is low, medium, or high. The threshold is based on the number of events recorded for an activity per day.
- Triggers – Triggering events determine when a policy will begin to assign risk scores to a user's activity.
- Anonymization – Masking a user's name and account information to prevent bias from investigators
- Telemetry – data from the M365 Audit log (ex. deletions, changes, label modifications, uploads, etc),
- Risk Score – Insider Risk Management leverages a score system to track how low or high a risk an activity is 100/100 is the highest risk possible. 0/100 is the lowest risk possible.

Notes

None

Pre-requisites

If you have performed parts 1-3 of this blog series, then you have everything you need to run this . If you have not done those parts of the blog, you will need to populate your test environment with test data for the steps to follow.

You must have enabled at least 1 Insider Risk Management license

It is recommended you have completed Part 3a DLP for Endpoint, or at the least, that you have on-boarded a minimum of one Windows 10/11 device to test the collection of Endpoint DLP policies into Insider Risk management (IRM).

You have loaded an Insider Risk Management (IRM) licensing for at least 1 week in order to collect as much telemetry as possible. That you have run Sensitivity and DLP testing during that 1 week, again, to add telemetry information to your IRM console.

You should have also done steps 6-6b in this series.

Part 1 - Policies

1. In the top ribbon, click on **Policies**.

Policies

2. Click **Create Policy**

+ Create policy

3. Under Categories, click **Data leaks**, and for the template, choose **General data leaks**

Categories

Data theft

Data leaks

Security policy violations (preview)

Health record misuse (preview)

Templates

General data leaks

Data leaks by priority users (preview)

Data leaks by disgruntled users (preview)

4. Give your policy a name and description

Name your policy

Name *

Data Leaks


Description

Data Leaks

5. Under **Choose Users and Groups**, select what you want. I will accept the default of **Include all users and groups**.

Choose users and groups

Choose users and groups within your organization who this policy will apply to.

 Policies detect activity based on what's supported by the user's current license. If a user's license change is included in might change for that user. [Learn more about supported user licenses](#)

- Include all users and groups
- Include specific users and groups

6. In the next section, **Specific content to prioritize**. I will accept the default of **I don't want to specify priority content right now**.

Specify content to prioritize

Specifying content as a priority increases the risk score for any associated activity, which in turn increases the severity of the alert. However, some activities won't generate an alert at all unless the related content type or was specified as a priority on this page. [Learn more](#)

- I want to specify SharePoint sites, sensitivity labels, and/or sensitive info types as priority content
- I don't want to specify priority content right now (you'll be able to do this after the policy is created)

7. On the Triggers page, accept the default of **User performs an exfiltration activity**. Then click **Next**.

Choose triggering event

The triggering event determines when a policy will begin to assign risk scores to activities for this policy template.

- User matches a data loss prevention (DLP) policy**
Policy will start assigning risk scores when a user performs an activity matching the 'High' severity incident reports. [Learn more about DLP policy requirements.](#)

- User performs an exfiltration activity**
Policy will start assigning risk scores when specific thresholds are detected for activities.

Select which activities will trigger this policy

- Downloading content from SharePoint
- Sending email with attachments to recipients outside the organization
- Printing files
- Copying files to USB
- Using Microsoft Edge to copy files to cloud storage
- Sharing SharePoint files with people outside the organization

8. Now you will choose which events will trigger an Insider Risk Management (IRM) alert. This is found in the **Triggering thresholds for this policy**.
 - a. When it comes to your thresholds, for testing purposes, I recommend you decrease the numbers as low as you are comfortable. This will guarantee a quicker trigger of the IRM alert during your testing. I like to use a 3/2/1 set of thresholds as it keeps the triggers to no more than 3 during a given day of testing.
 - b. The 3 thresholds I recommend you focus on for this blog are:
 - Sending email with attachments to recipients outside the organization**

- **Copying files to USB**
 - **Using Microsoft Edge to copy files to a cloud storage.**
- c. Here is an example of these thresholds with **Copying files to USB**.

Copying files to USB


- Total number of activities
 per day
- Number of activities for files containing sensitive info types
 per day
- Number of activities for files matching priority content
 per day

[Reset to defaults](#)

9. You will be taken to the Policy Indicators. Accept the defaults (all should be check marked) and click **Next**.

Policy indicators

This policy will use the selected indicators below to detect user activity.

 If an indicator isn't selected below, you won't receive any alerts for that activity.

Office indicators

- Select all
- Sharing SharePoint files with people outside the organization
- Sharing SharePoint folders with people outside the organization
- Sharing SharePoint sites with people outside the organization
- Downloading content from SharePoint
- Adding people outside organization to priority SharePoint sites

10. Again, you can either accept the default thresholds or apply reduced numbers to speed up your testing. Once again, I recommend you find the criteria you want to test and reduce the thresholds to 1/2/3. Here is an example.

Use default thresholds for all indicators

Specify custom thresholds

Sharing SharePoint files with people outside the organization

1 to 2 events per day generates low severity alerts

2 to 3 events per day generates medium severity alerts

3 to 10000 events per day generates high severity alerts

[Reset to defaults](#)

11. Click Next and perform your Review and **Submit** and **Done**.

Review settings and finish

Review the settings for your insider risk policy. The policy will 1 generating alerts. We recommend letting your users know how

① 1 suggestion below for improving your policy.

Policy template

LeakOfInformation

[Edit policy type](#)

12. We are not done with the basics of Insider Risk Management (IRM) configuration. The next part of the blog (part 6a) will cover the alerts cases. That data will be more fully populated after the 7 days of testing AFTER your IRM license has been enabled.

Appendix and Links

[Learn about insider risk management - Microsoft 365 Compliance | Microsoft Docs](#)

[Investigate insider risk management activities - Microsoft 365 Compliance | Microsoft Docs](#)

[Insider risk management cases - Microsoft 365 Compliance | Microsoft Docs](#)

[Insider risk management policies - Microsoft 365 Compliance | Microsoft Docs](#)

[Insider risk management notice templates - Microsoft 365 Compliance | Microsoft Docs](#)

[Insider risk management settings - Microsoft 365 Compliance | Microsoft Docs](#)

Note: This solution is a sample and may be used with Microsoft Compliance tools for dissemination of reference information only. This solution is not intended or made available for use as a replacement for professional and individualized technical advice from Microsoft or a Microsoft certified partner when it comes to the implementation of a compliance and/or advanced eDiscovery solution and no license or right is granted by Microsoft to use this solution for such purposes. This solution is not designed or intended to be a substitute for professional technical advice from Microsoft or a Microsoft certified partner when it comes to the design or implementation of a compliance and/or advanced eDiscovery solution and should not be used as such. Customer bears the sole risk and responsibility for any use. Microsoft does not warrant that the solution or any materials provided in connection therewith will be sufficient for any business purposes or meet the business requirements of any person or organization.