Microsoft Security

A guide to recognizing and mitigating insider risk with Microsoft Purview

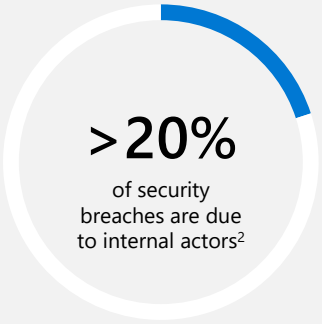
Not all threats come from the outside

Security challenges due to bad actors on the outside, such as representatives of nation states or hackers seeking to profit from proprietary or personally identifiable information (PII), can be devastating to companies. However, the popularity of remote and flexible work has spawned increased risk—often inadvertently, by internal employees.

Such risk can translate into substantial cost to the organization, requiring reactive recovery efforts to protect business operations, reputation, or brand value. This is insider risk.

Insider risk is defined as the potential for a person to use authorized access—either maliciously or unintentionally—in a way that negatively affects the organization. Vulnerabilities can extend to physical and virtual access to information, processes, systems, and facilities-related assets.

Inside risks are a universal and growing concern



$15.4

million total average annual cost of activities to resolve insider threats[3]

However, the real cost of insider risks extends beyond financial. In a recent Microsoft Security survey, respondents highlighted the top five risks with loss of customer data and damage to brand or reputation topping the list.[4]

Theft or loss of customer data	84%
Brand or reputational damage	82%
Theft or loss of employee personal data	81%
Theft or loss of mission critical data or intellectual property	81%
Legal & regulatory impact, including litigation defense cost	80%

The potential monetary cost associated with these insider risks is staggering. It is estimated that at least 20% of insider risk events will cost organizations more than $750,000.[4]

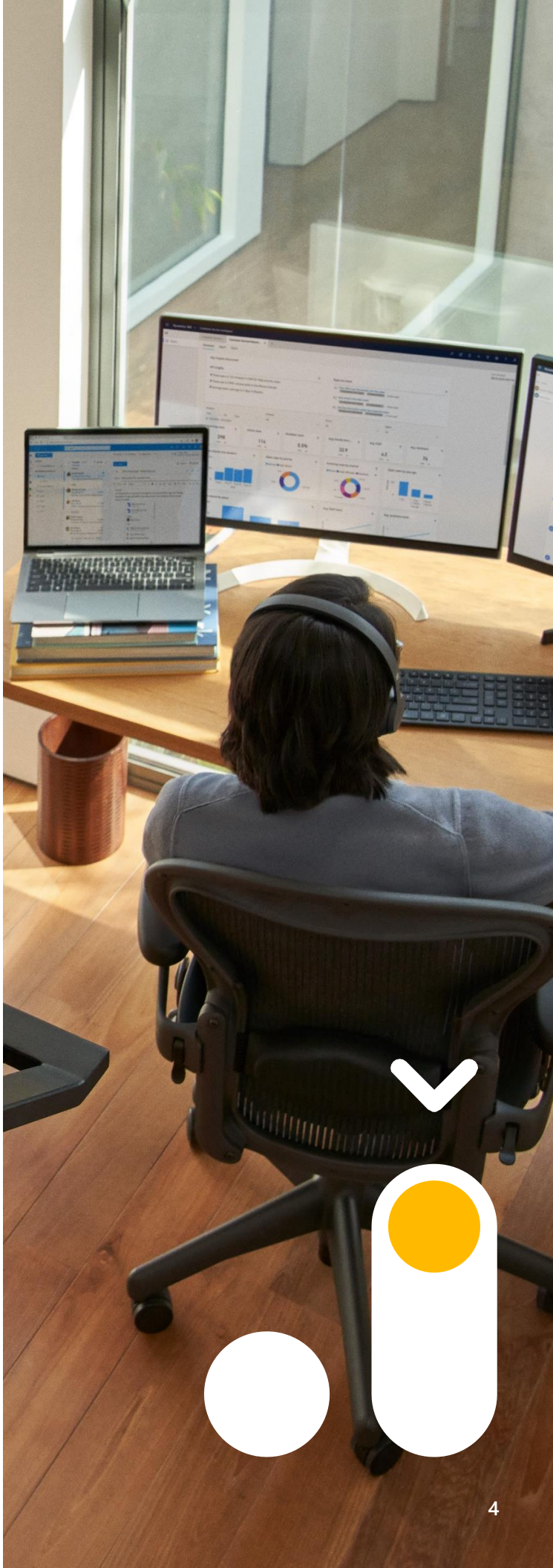
Managing insider risks

How does an organization protect itself against threats when the risk originates from individuals trusted with access to resources, files, and other critical business assets? One way is to build a holistic insider risk management program that uses tools to support:

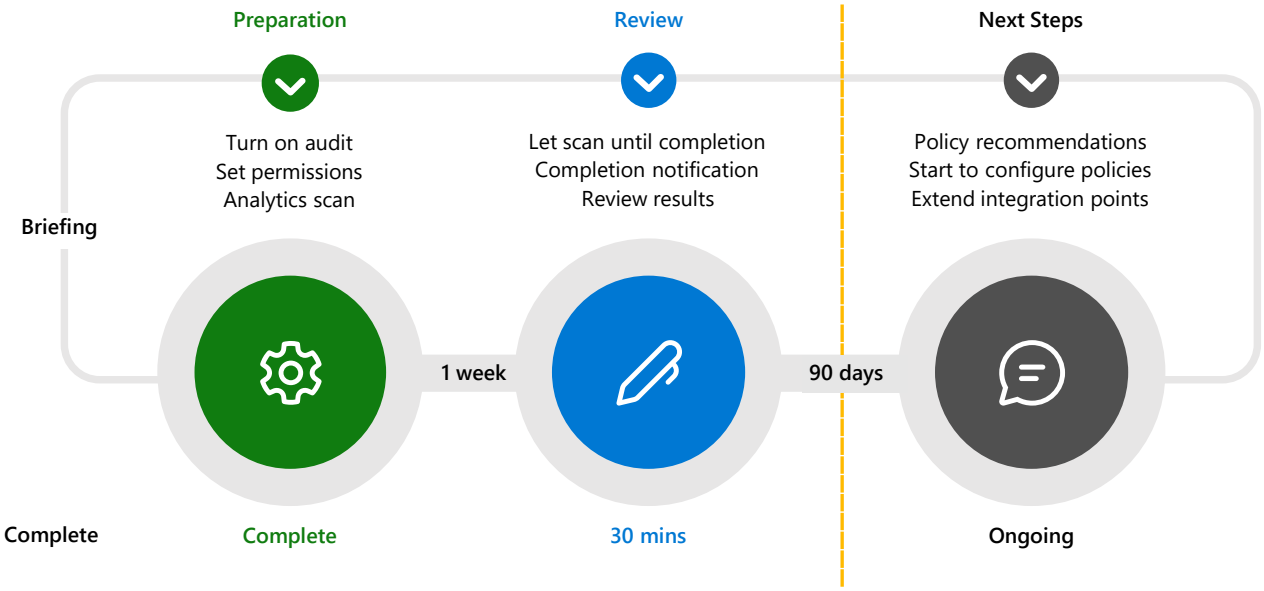
1. Prioritizing employee trust, productivity, and privacy controls.
2. Attaining program buy-in and involvement across the organization—including the offices of CISO, CIO, and Risk.
3. Effective training and education of employees.
4. Proactive use of positive deterrents.
5. Integration with other key tools that help expedite detection and management of insider risk.

Robust insider risk management programs can be achieved with Microsoft Purview's insider risk management and analytics. Microsoft Purview provides a unified data governance solution to help manage and protect your data estate.

See for yourself by following the simple step-by-step instructions outlined below to run your own insider risk assessment (IRA) and learn where your organization is most at risk from insider threats.



Get started with an Insider Risk Assessment Trial



License requirements

To get started, you will need a valid Microsoft 365 E3 subscription, and endpoints under management with Microsoft Defender for Endpoint.

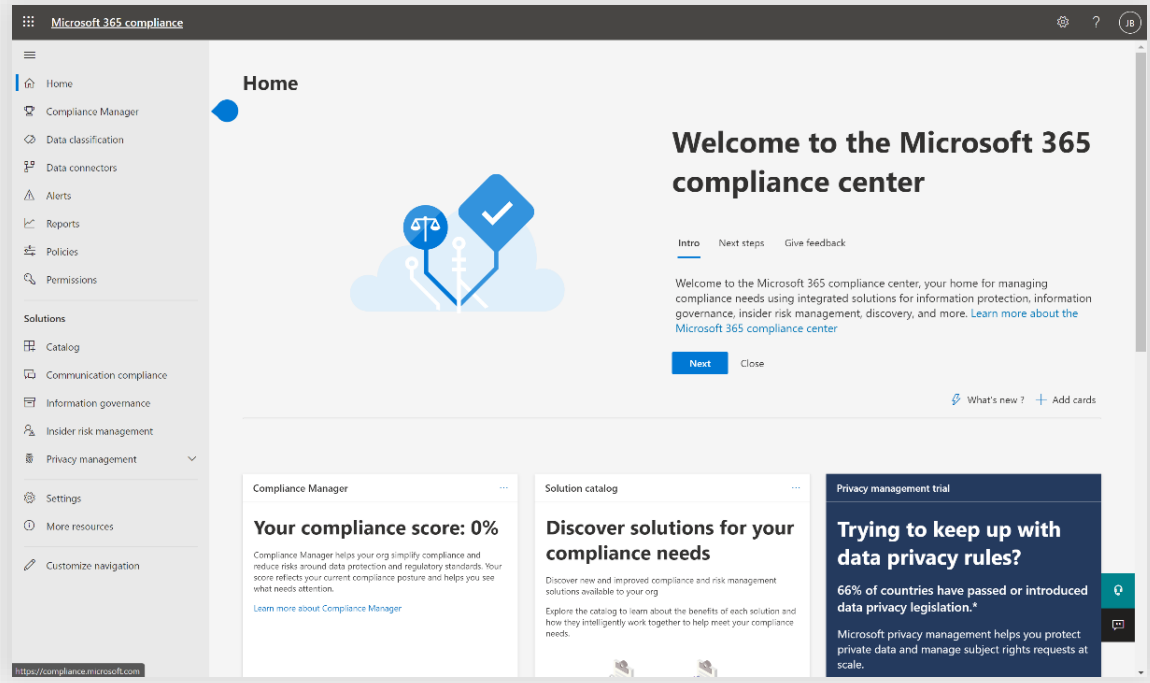
Getting started with IRM

Contact a Microsoft authorized partner for help configuring additional Microsoft solution integrations or advanced policies.

Step 1: Connect to the Microsoft Compliance Portal

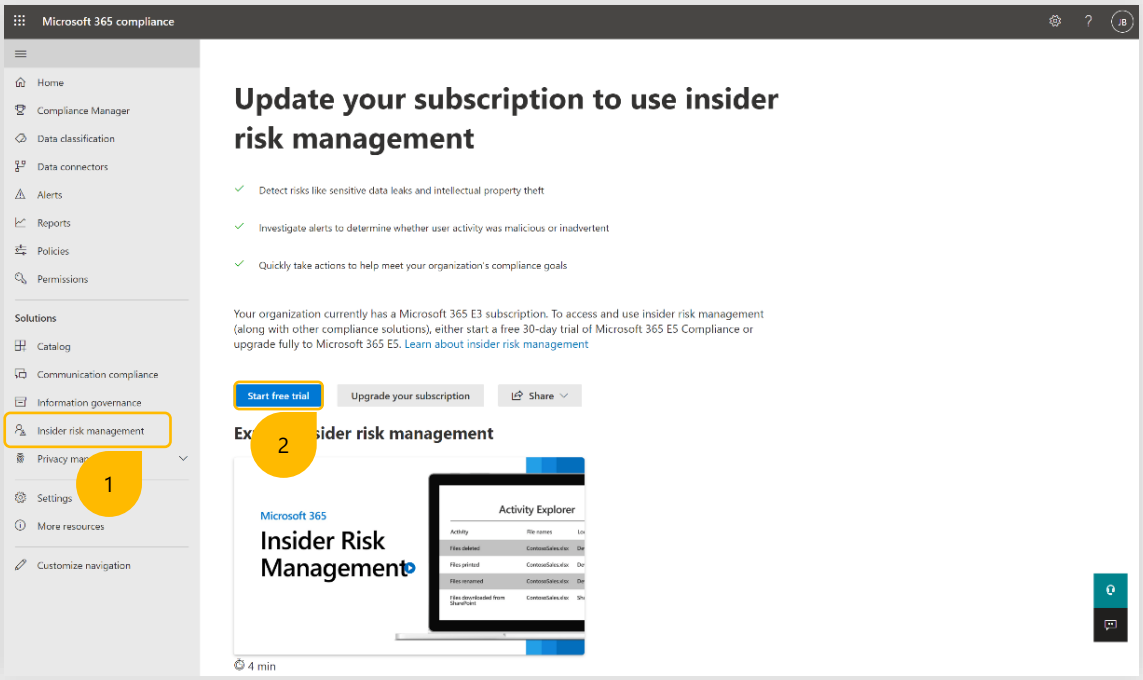
Note: You must belong to either the **Organization Management** role group or the **Compliance Administration** role group to configure settings within the Microsoft Purview Portal.

Go to https://compliance.microsoft.com

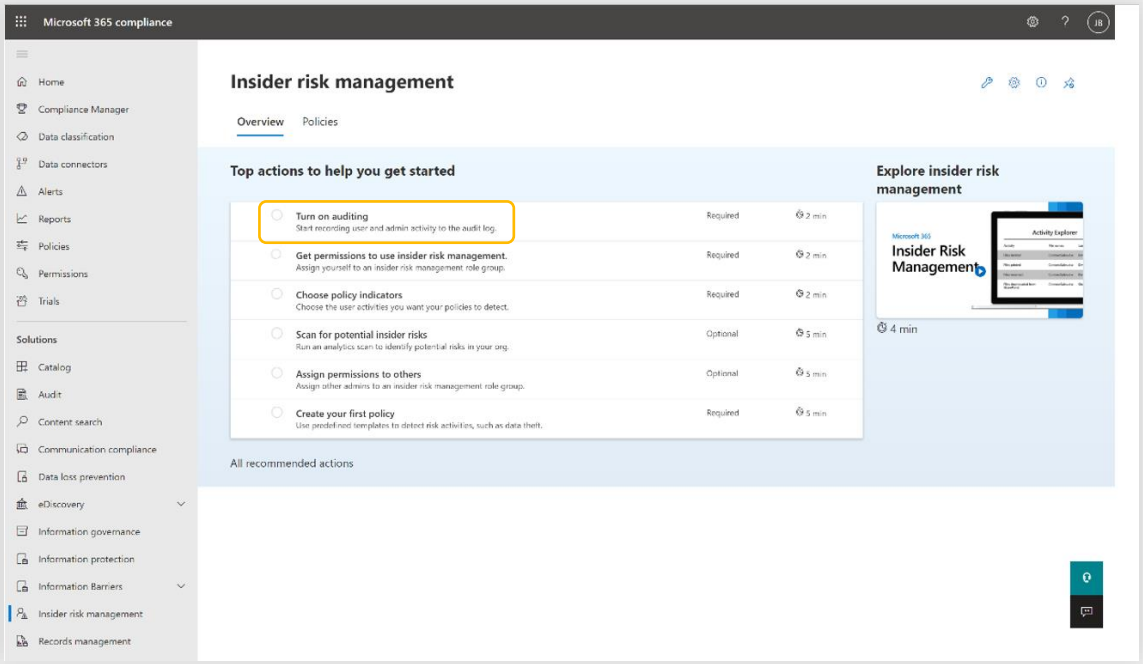


Step 2: Activate the IRM trial

Navigate to Insider risk management menu and select **Start free trial** to activate insider risk management.

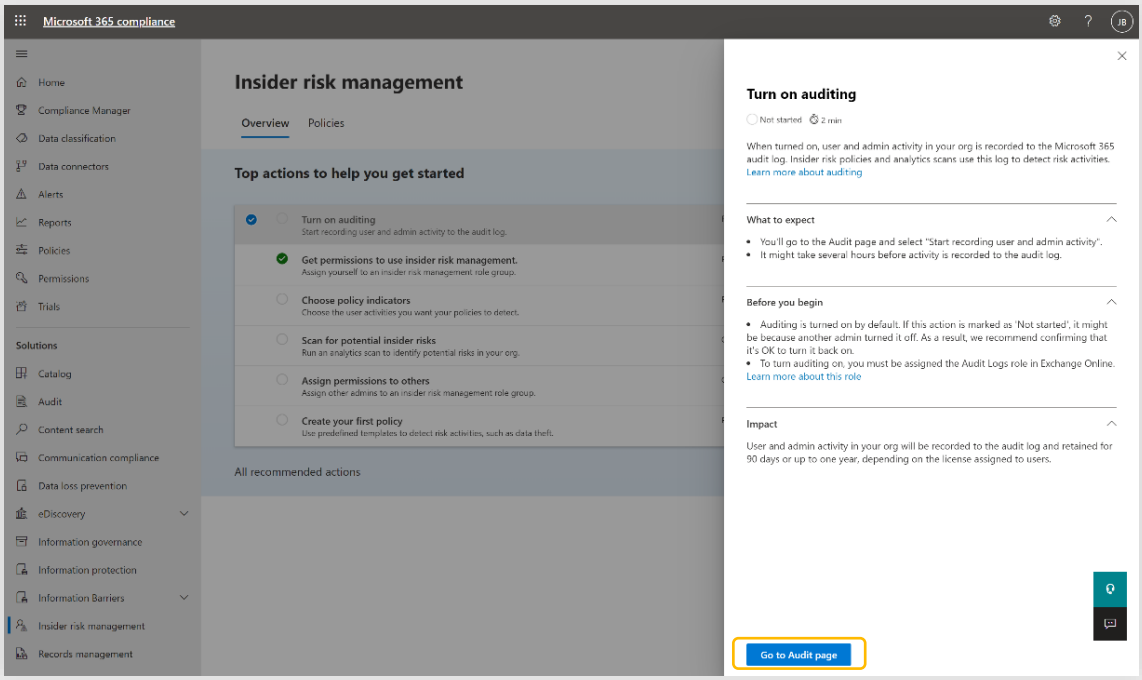


Once activated, a collection of wizards will help you activate and quickly configure IRM.

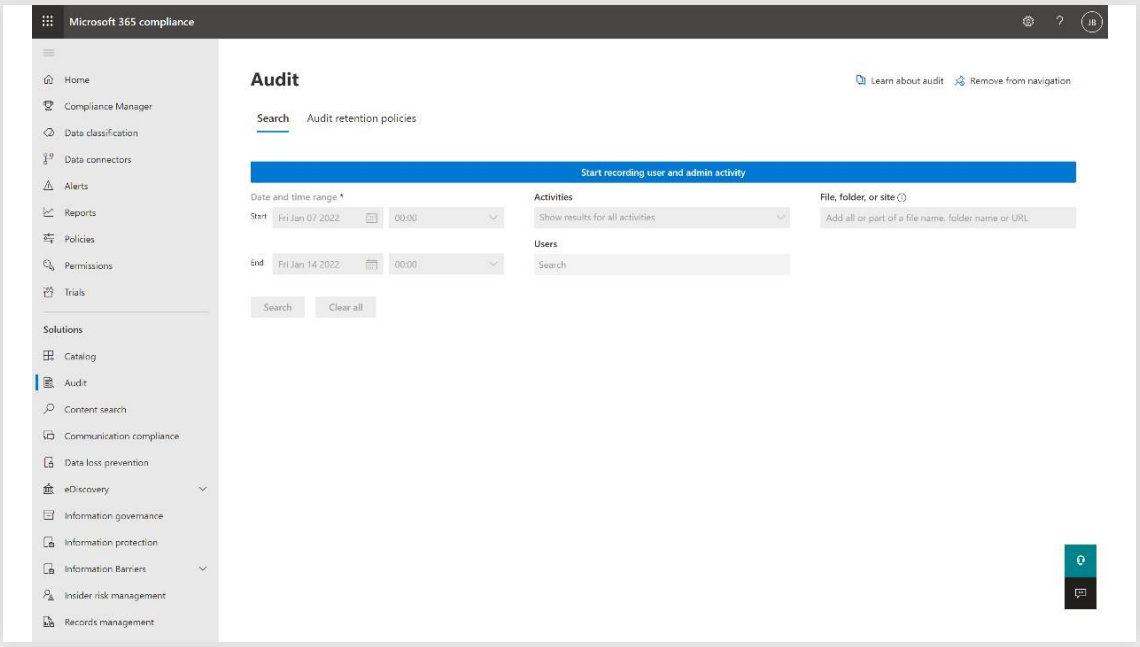


Step 3: Confirm auditing is active

Auditing is required to collect data for insider risk management. This feature is activated by default and is typically left active by administrators.

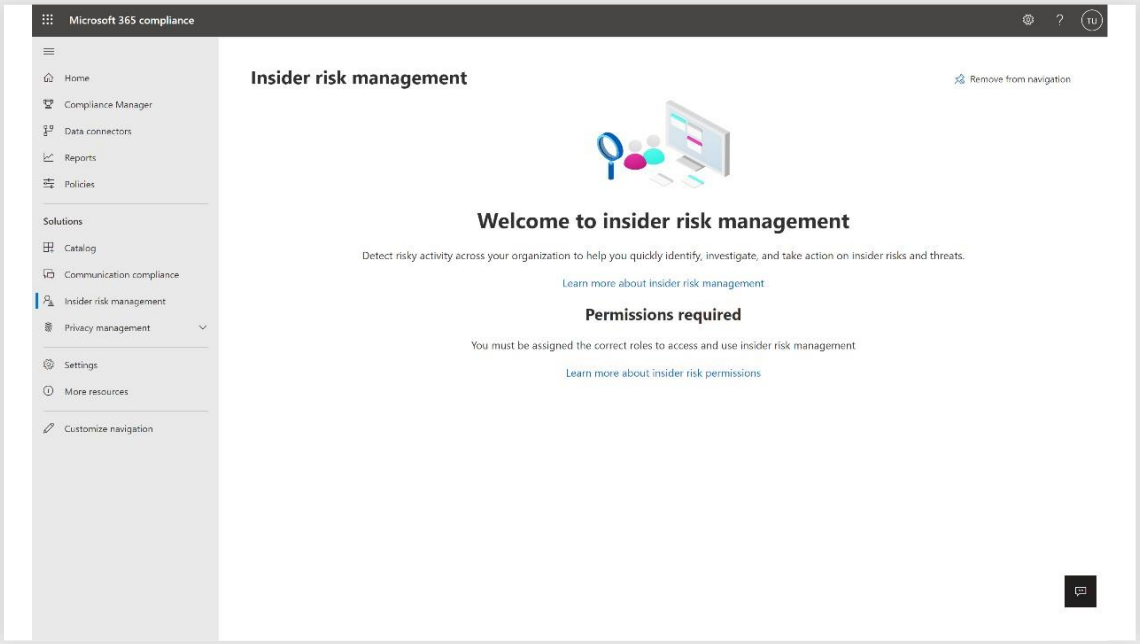


Click the blue **Go to Audit** page button at the bottom of the screen. On the next page, confirm that auditing is activated. If auditing is not activated, reach out to your Microsoft 365 Administrator team or the group with Microsoft 365 Global administrator roles.

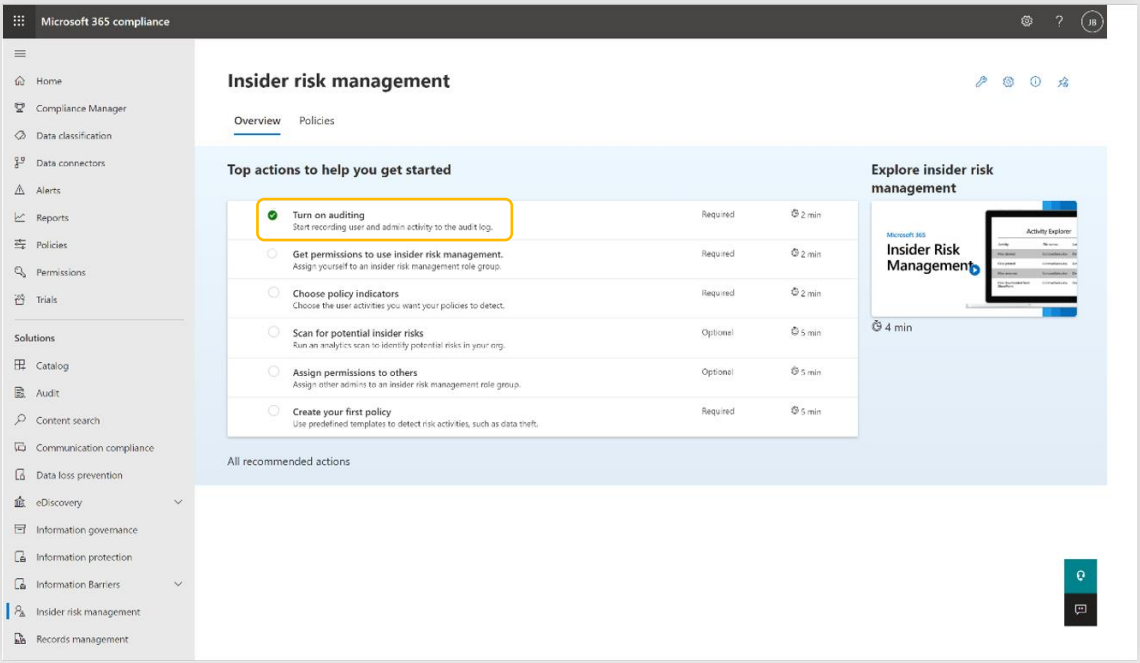


Step 4: Configure IRM permissions

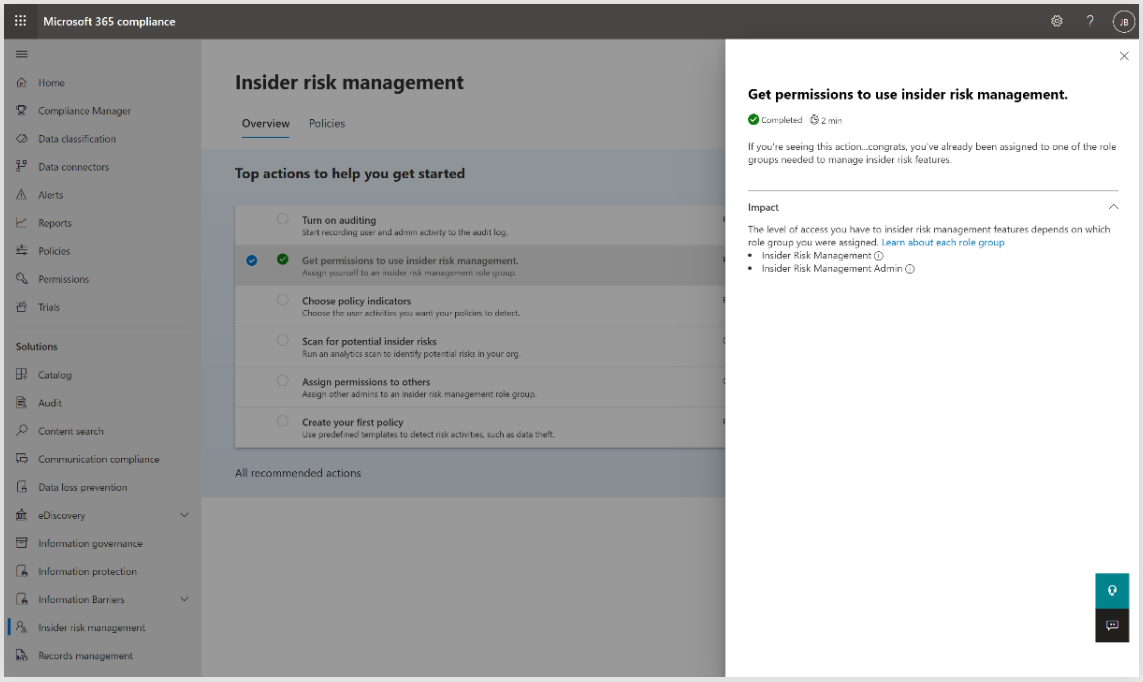
Click the **Insider risk management** tab on the left navigation bar. If you already have permission to access IRM, you will see the confirmation screen below.

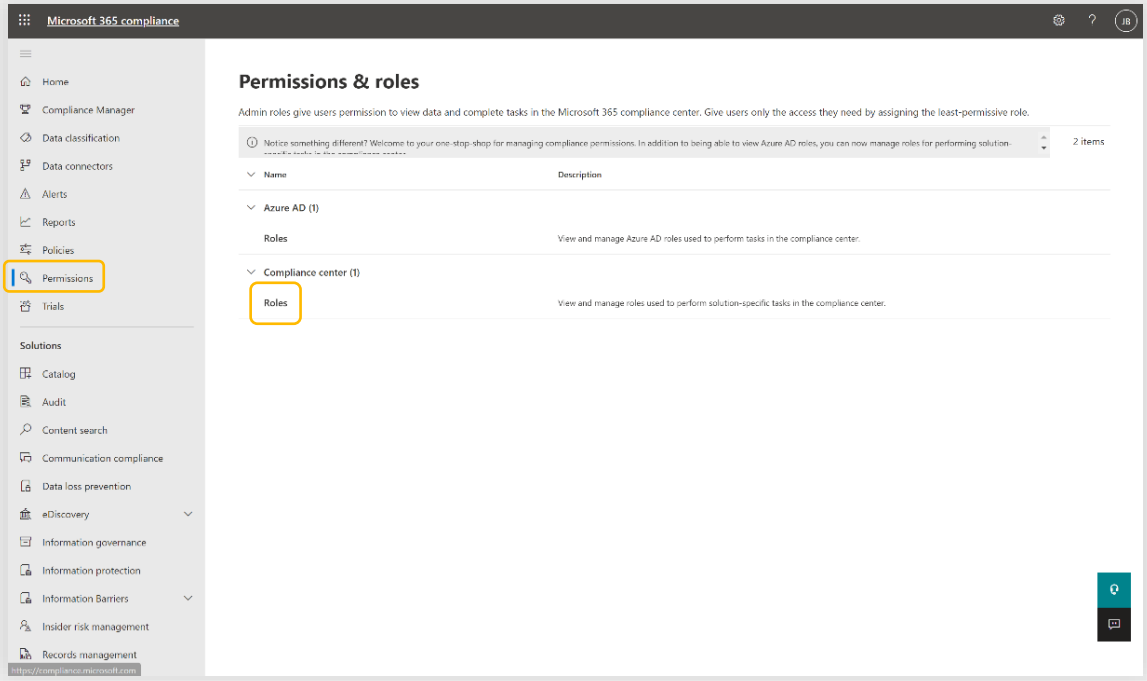


Going back to the Insider risk management menu, you can also confirm Auditing is activated.



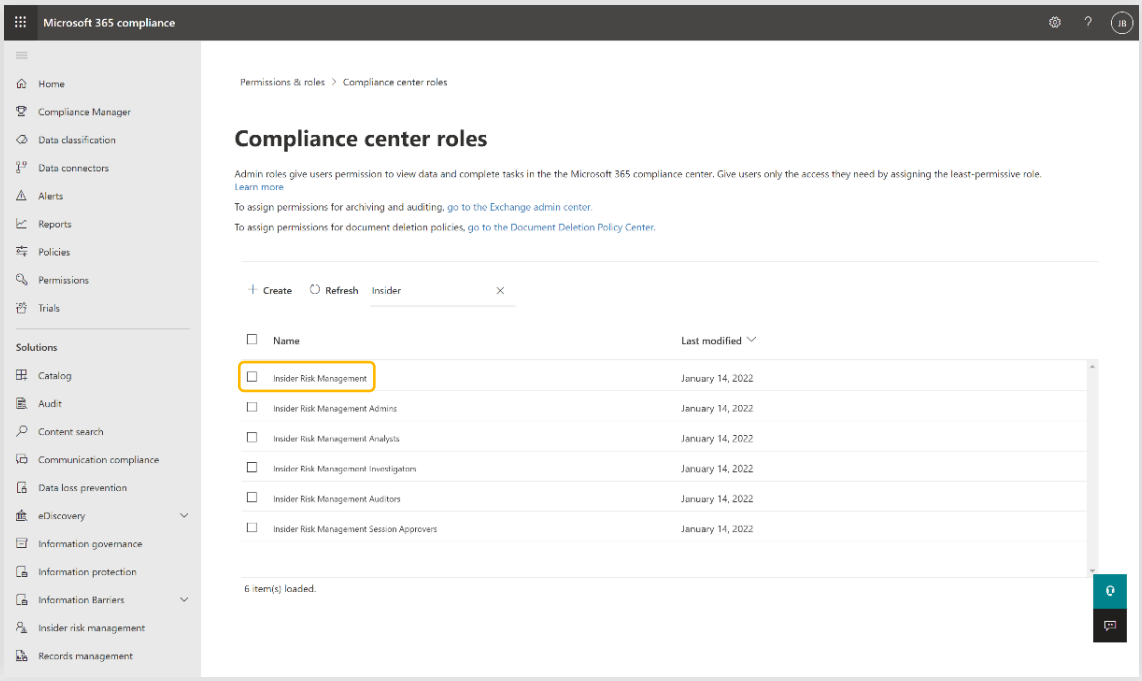
If you do not already have the appropriate permissions, select **Get permissions to use insider risk management** from the menu and follow the steps below.



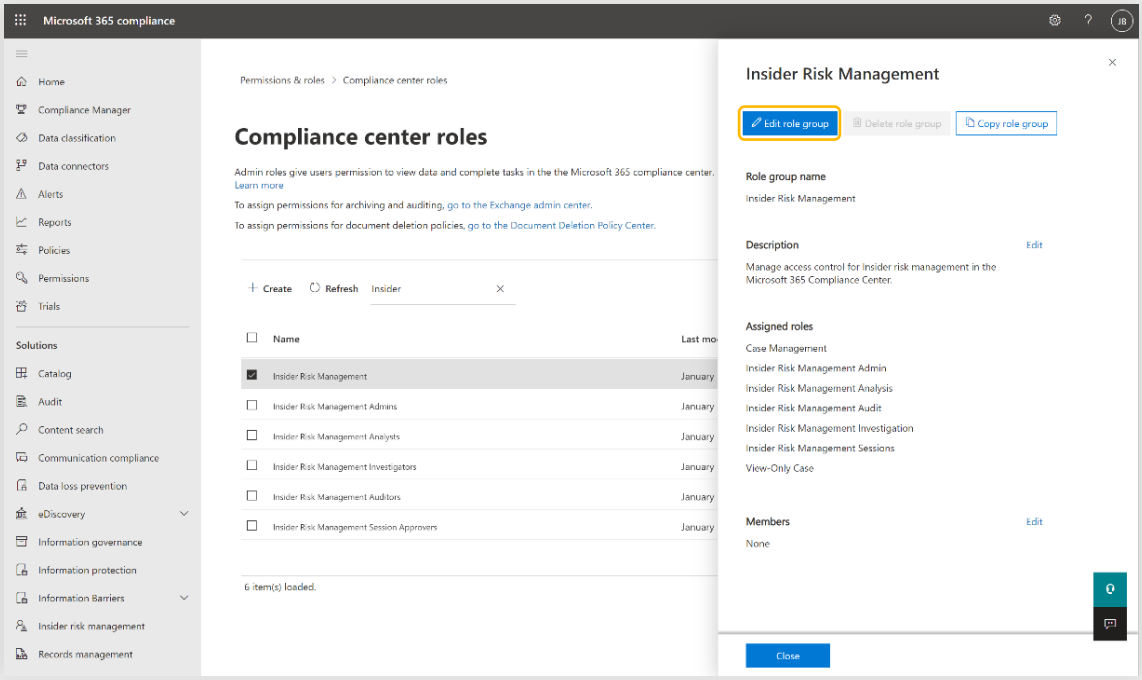


Select **Permissions**, then **Compliance center**. You will see a list of roles configured for the compliance environment, as shown below.

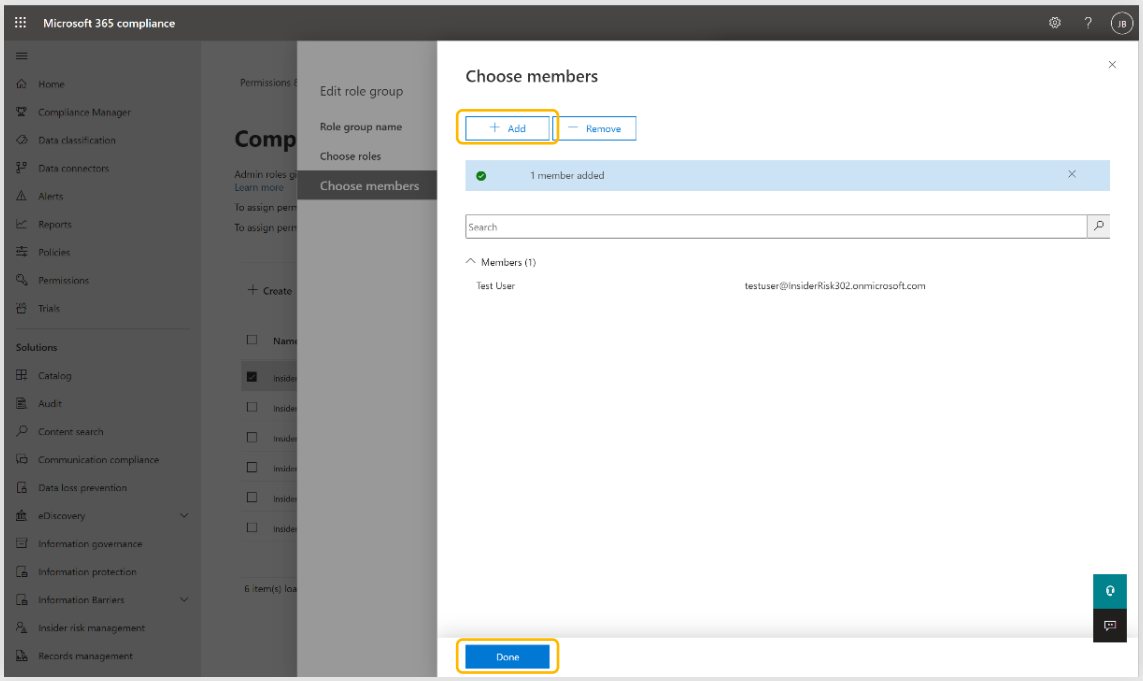
If you are unable to access this menu reach out to your Microsoft 365 Administrator team or the group with Microsoft 365 Global administrator roles.



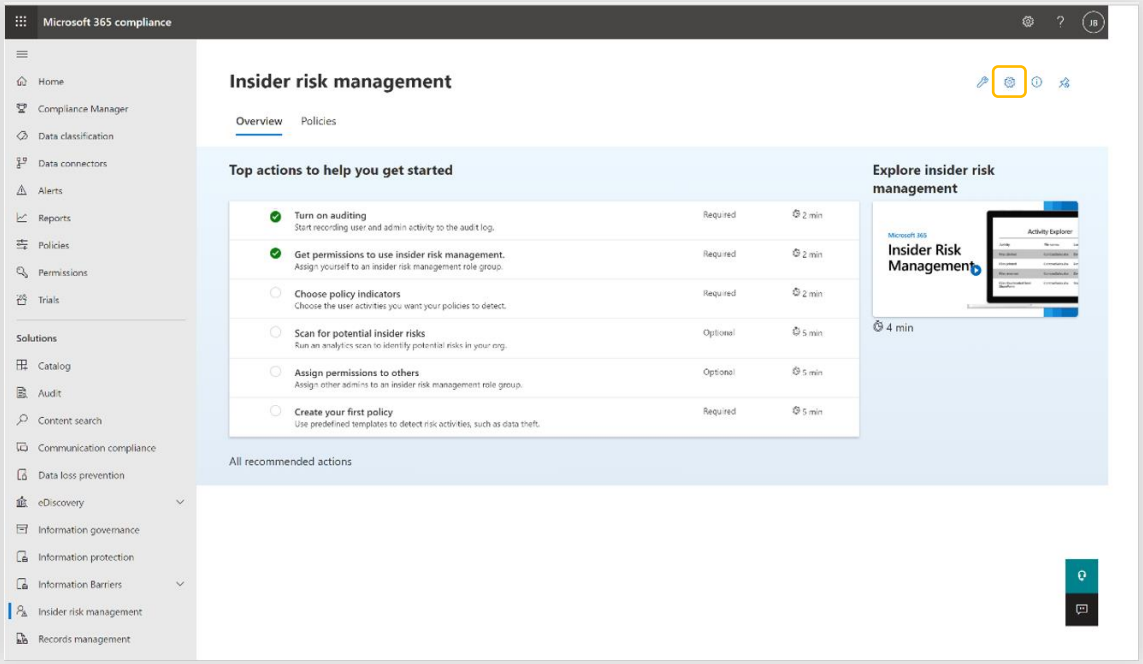
Select **Insider Risk Management**.



Then click **Edit**.



Add your account and click **Done**.

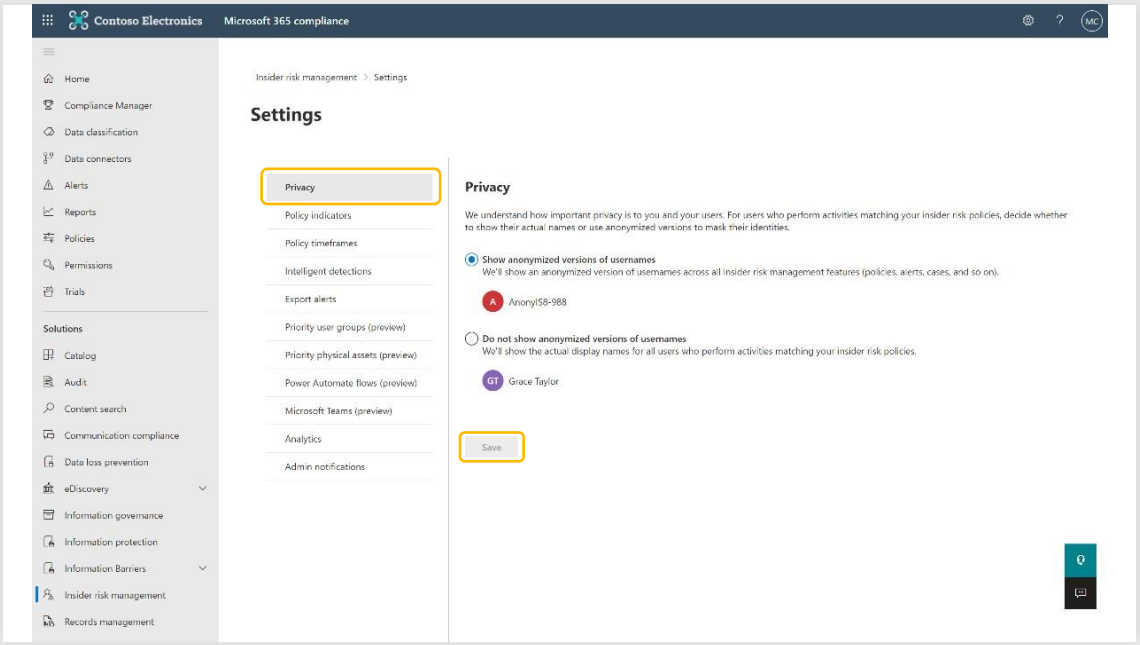


You now have access to IRM.

Step 5: Anonymization of user data

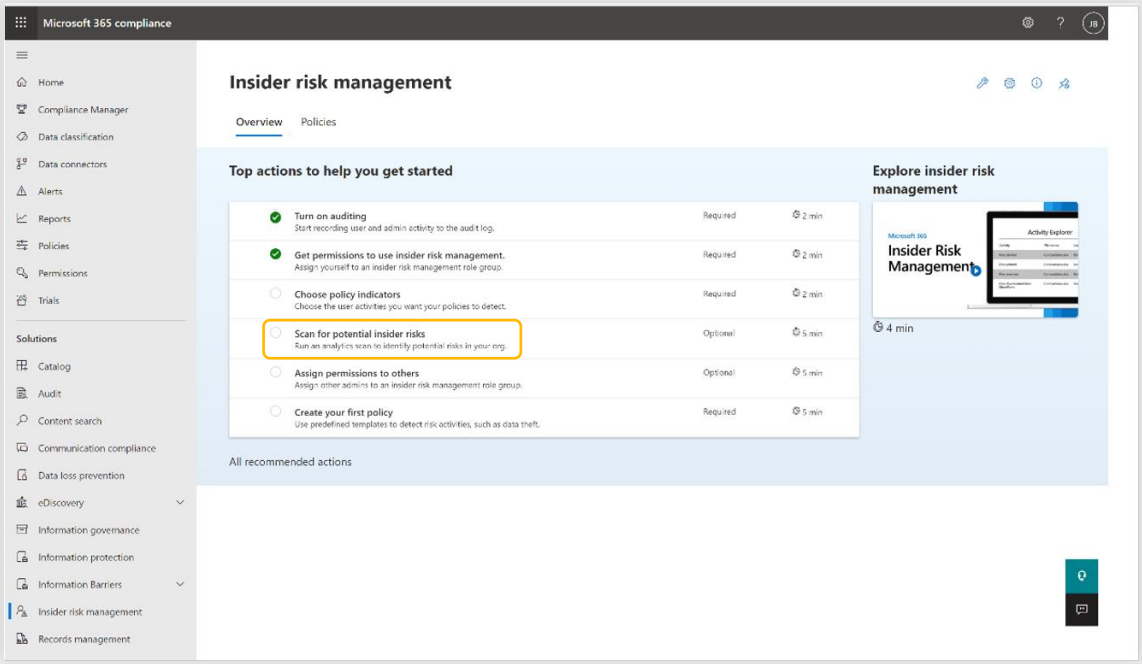
The next step in the configuration of IRM is to determine whether to anonymize usernames to prevent the identification of individuals for which insider risk activities are detected. Anonymization may be preferred, based on your organization's data privacy requirements.

Click on the settings icon at the top right corner of the screen, then choose the **Privacy** tab and define your choice. Click **Save** to retain your selection.

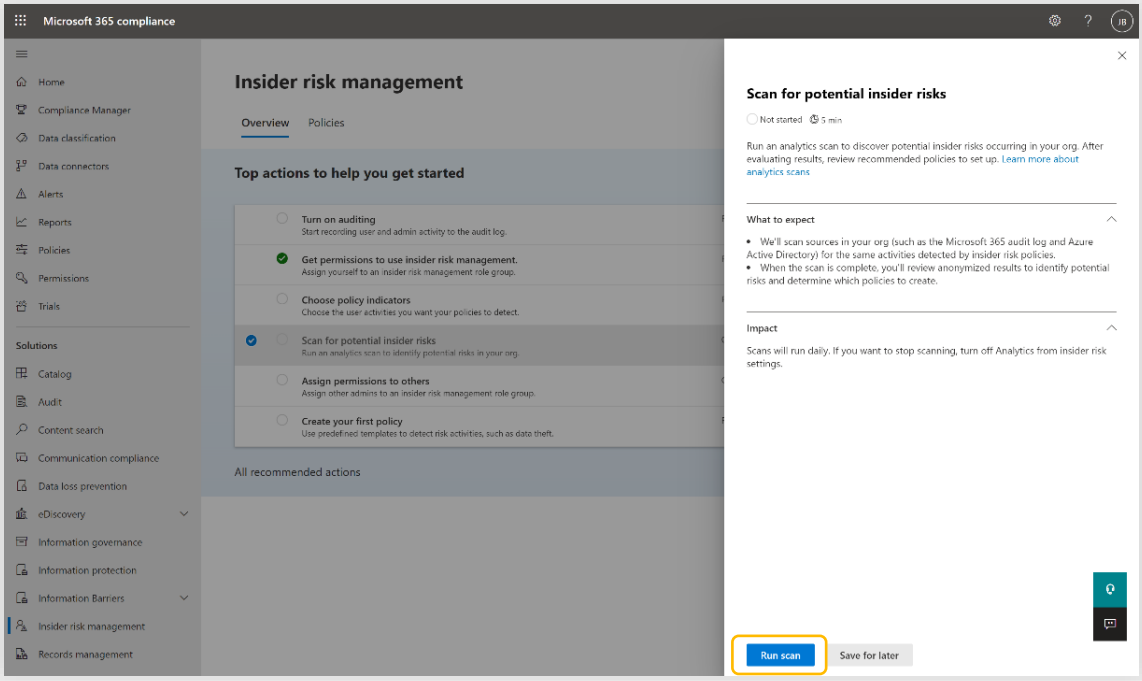


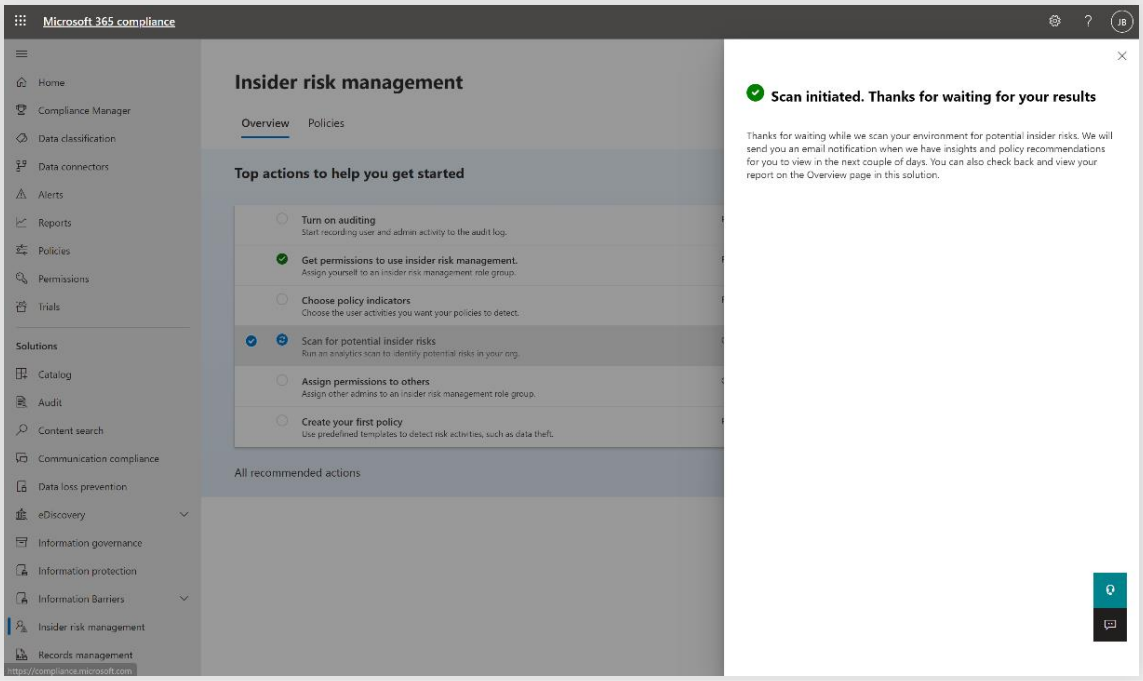
Step 6: Run your first scan

Navigate to the **Insider risk management** menu and choose **Scan for potential insider risks**.



Click **Run scan** to begin.





Congratulations, you have successfully activated insider risk management. Once the scan is complete, insights relating to endpoints under management with Microsoft Defender for Endpoint will be available.

How long does it take?

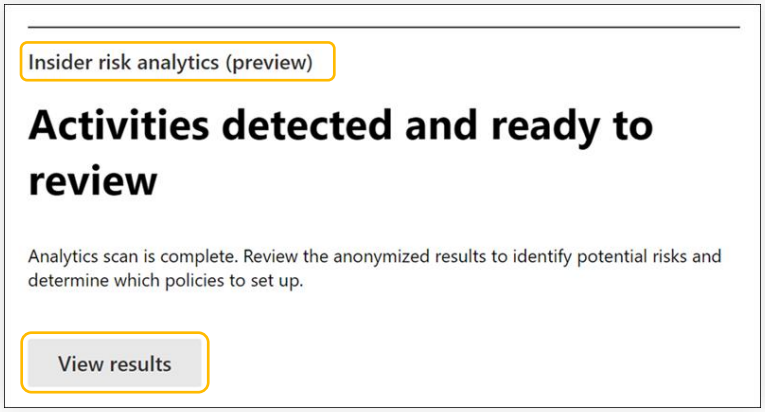
Collected data begins to display after 48 hours. It is recommended the results be checked five days after enabling the analytics to get a complete view of the various data sources.

Accessing analytics insights or reports

After the first analytics scan is complete, members of the "insider risk management admin" role group will automatically receive an email notification and can view the initial insights and recommendations. Scans run daily unless analytics are turned off.

Email notifications contain information about each of the three analytics categories—data leaks, theft, and exfiltration.

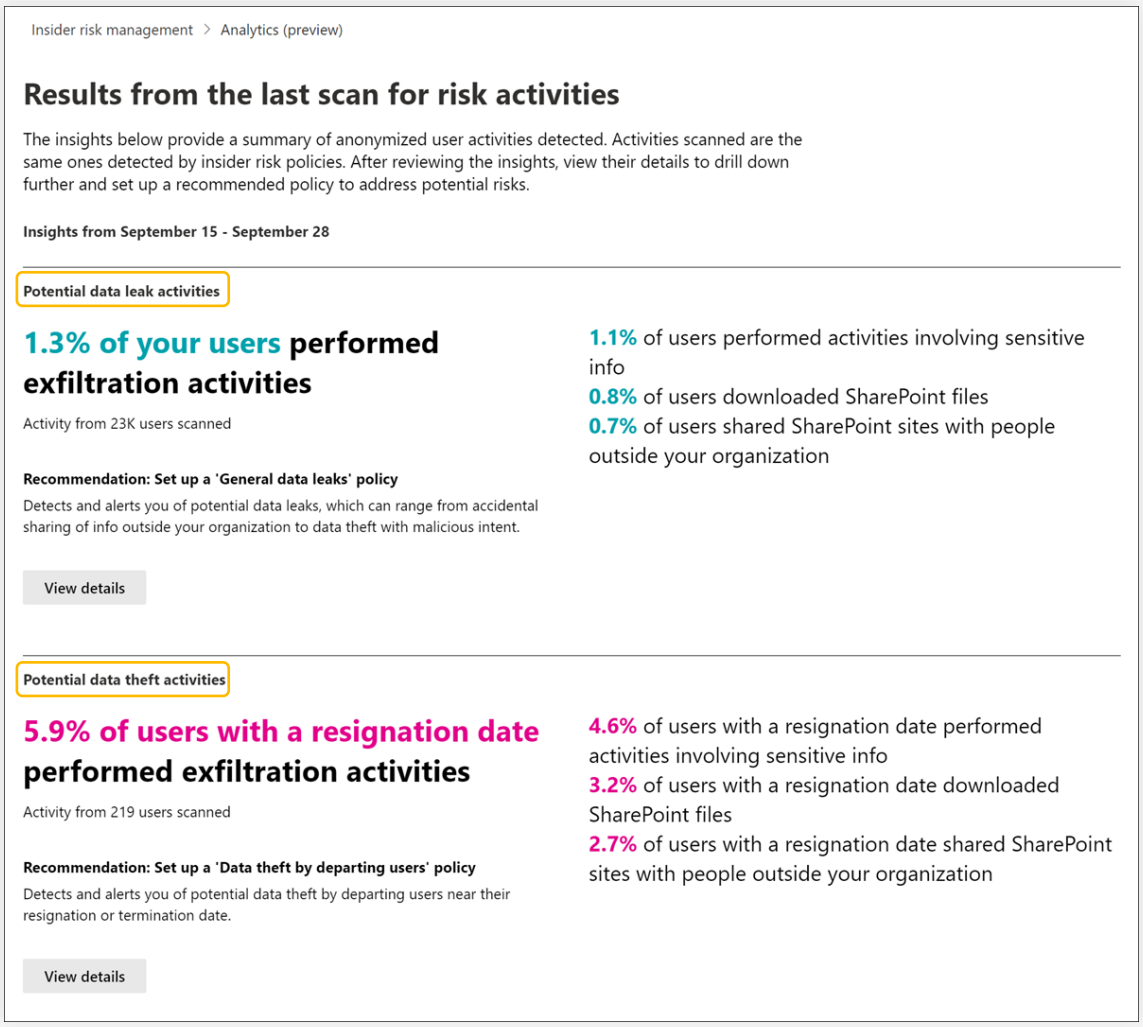
To view the results of the analytics, navigate to the **Overview** tab and select **View results** under the **Insider risk analytics** card.

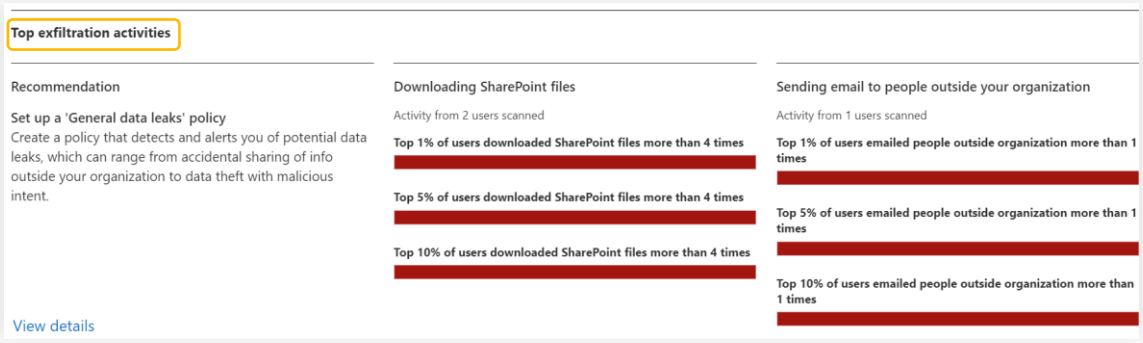


For completed scans, you'll see the potential risks discovered in your organization and recommendations for addressing the risks. Identified risks and specific insights are included in reports grouped by area, the total number of users with identified risks, the percentage of users with potentially risky activities, and a recommended insider risk policy to help mitigate the risks.

The reports include:

- **Data leak insights:** Activities for all users that may include accidental oversharing of information outside your organization or data leaks by users with malicious intent.
- **Data theft insights:** Activities for departing users or users with deleted Azure Active Directory accounts that may include risky sharing of information outside your organization or data theft by users with malicious intent.
- **Top exfiltration insights:** Activities by all users that may include sharing data outside of your organization.



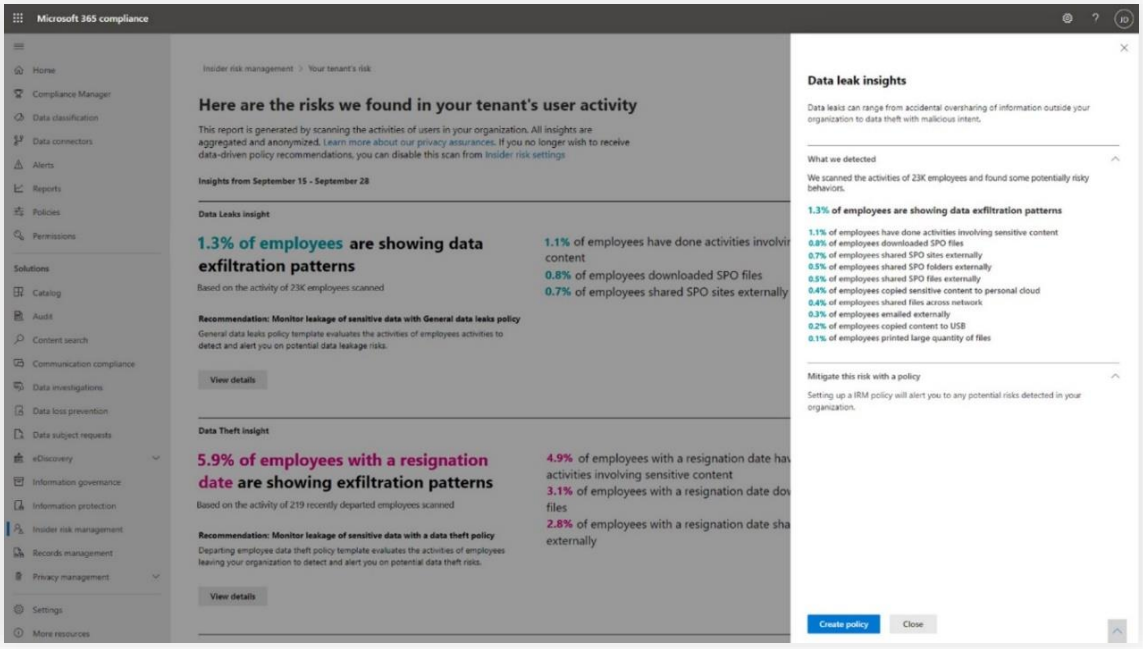


Three individual reports on the **Results from the last scan for risk activities** page displays the top 3 items from each area of the analytics and the high-level recommendations for next steps.

For each of the three reports, additional details can be accessed to display all the metrics collected, as well as next steps or recommendations.

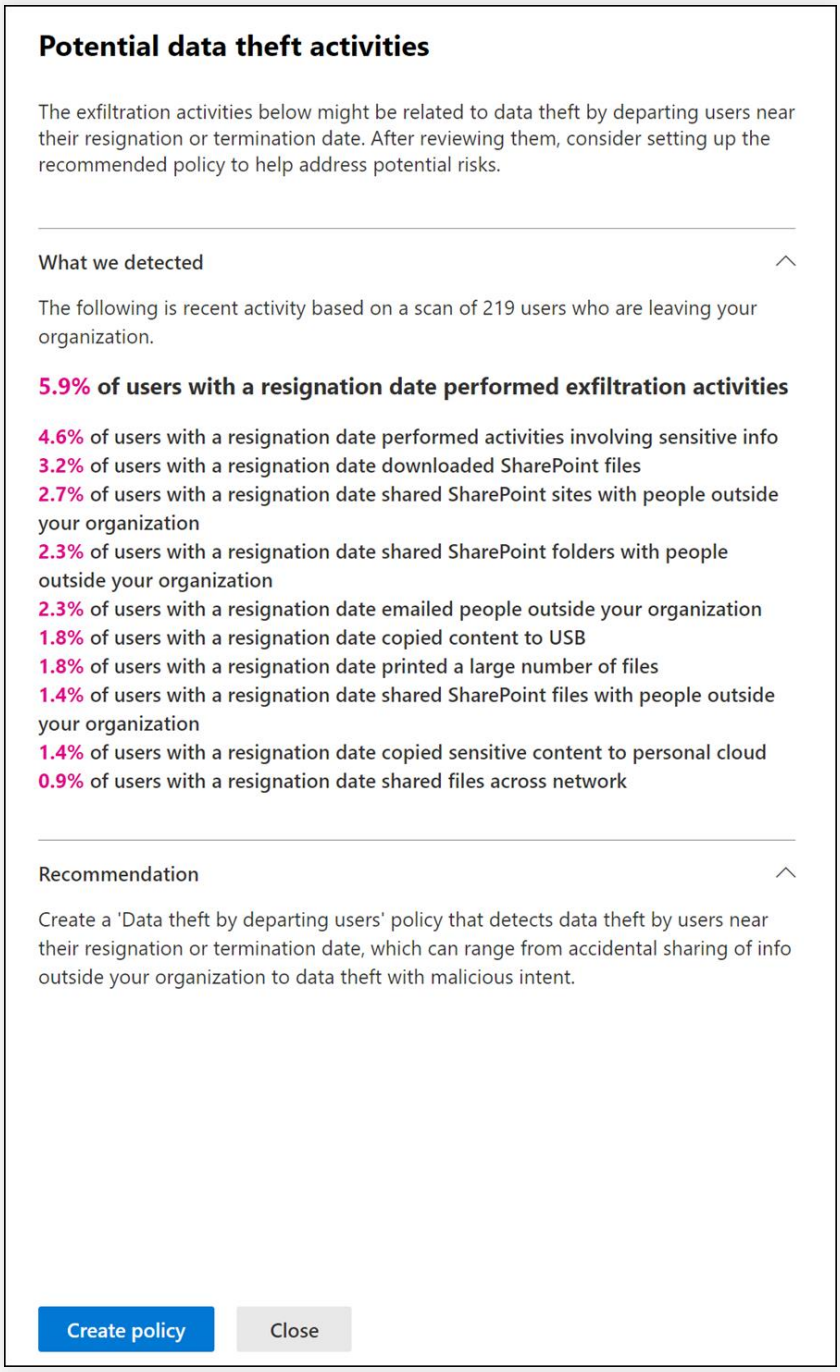
Data leak insights

The Data leak insights report displays the percentage of employees' activities identified as at risk for data breaches including external sharing activities, copying of sensitive data to personal clouds, and content copied to USB. Policies can be set up to protect against the continued threat of insider data leaks.



Potential data theft activities report

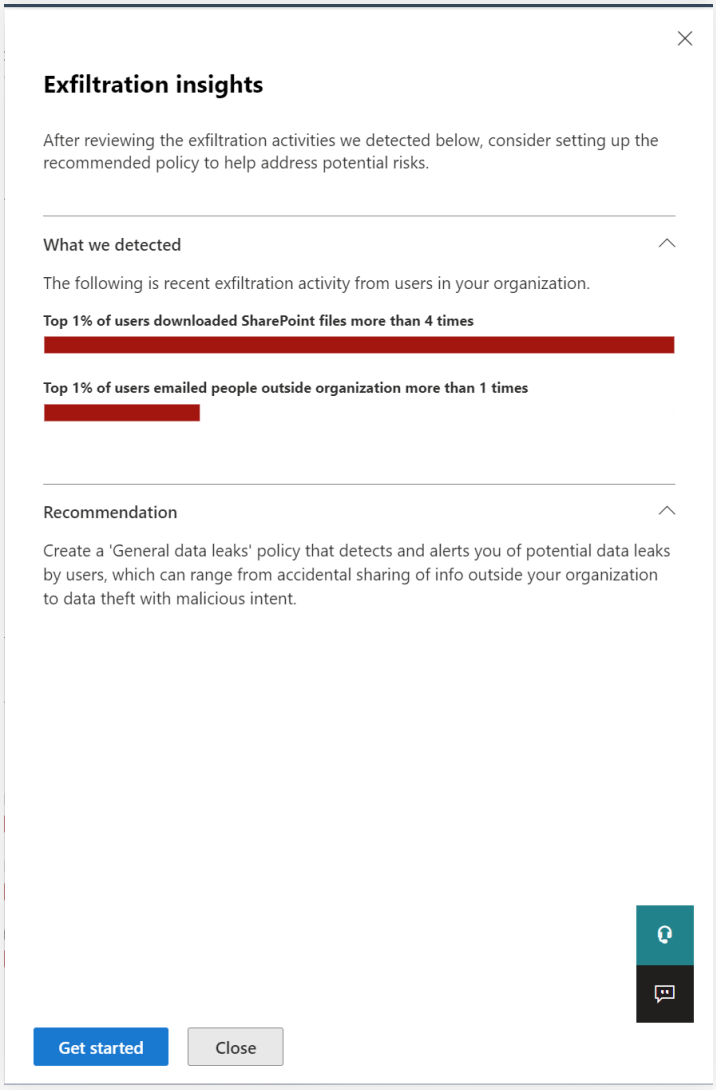
Insights for data theft activities are typically triggered for employees who are scheduled for departure or termination.



Top exfiltration activities report

Any exfiltration activities performed by users will be displayed here. The indicators used for exfiltration are:

- Sharing Microsoft SharePoint files, folders, or sites with people outside the organization.
- Downloading content from Microsoft SharePoint or Microsoft Teams.
- Sending emails with attachments to recipients outside the organization.
- Detect when a user's exfiltration activities exceed organizational norms.



Learn More

Getting insights on insider risk is simple with IRM in Microsoft Purview. Participate in a partner-led, Protect and Govern Sensitive Data workshop to learn more.

Microsoft Security

Sources

[1]Microsoft, Insider Risk Management Market Research, 2021.

[2]Verizon, 2021 Data Breach Investigations Report, 2021.

[3]Ponemon, 2022 Cost of Insider Threats Global Report, 2022.

[4]Microsoft, Building a Holistic Insider Risk Management Program: 5 elements that help companies have stronger data protection and security while protecting user trust, 2022.