Summary

Overview: Insider risk management is a compliance solution in Microsoft 365 that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Insider risk policies allow you to define the types of risks to identify and detect in your organization, including acting on cases and escalating cases to Microsoft Advanced eDiscovery if needed.

This lab is designed to give you an experience of Insider Risk Management capabilities and act as a demo. There are several items that need to be setup within an M365 for Insider Risk to work, monitor, alert, and trigger. These labs have been preconfigured, so you should be able to see some sample information in there. In the event that you have a lab with no information it can take up to 8 hours for activities to be detected and triggered This is due to how the platform works and parameters that are set up within any environment.

At no means should you use this guide to configure your production environment without further understanding and implications to end-users.

Lab steps

Insider risk management

What is it	Where is it and what to do
Insider risk management uniquely positions Microsoft 365 to help organizations quickly identify and remediate insider risks. Whether you have concerns around possible data risks from departing or disgruntled users, the items that we setup in the previous labs all monitor and work with each other. For example, the custom and built-in sensitive information types created we can reuse as part of our monitoring. Insider risk management doesn't block or stop staff members from doing their work, but monitors the behaviors patterns and data that they are handling. Using different signals the platform uses machine learning to identify and apply risk scores to each	No clickable steps here but sets the scene for what Insider risk management is.

What is it	Where is it and what to do
alert. This helps with ensuring there's a balance between productivity, security, and compliance. Remember that activities can be both intentional or unintentional as we empower our workforce to work from anywhere to get the job done. To ensure this isn't just a big brother tool, privacy is built-in as default, meaning the reviews of this tool aren't able to identify individuals and concentrate on the evidence within the review tools. This protects against bias as well as privacy.	
In this lab you're acting as a Security analyst for Contoso. When you navigate to the Insider Risk Management Portal, you will see the insider risk management dashboard, which displays an overview of the alerts to review, active cases, users, and the policies with the most activity. There are tabs for Alerts, Cases, Policies, Users, and Notices. We'll start by creating different policy templates that are built into the solution. You will see the policy page for insider risk management. You see that one policy has already been created, but first lets create a new policy. Click on Create policy then you are taken through the first page of a wizard where you can define a name and provide a description. You also see several policy templates. This is where the solution makes it easier for you to try to focus in on the types of risks that you want to build policies around. The built-in templates help you focus on confidentiality issues like data theft and data leak, and sabotage issues like security policy violations. The data theft by departing users policy template leverages an HR connector that ingests employees'	Navigate to https://compliance.microsoft.com/ logged in as the administrator of your given lab tenant. Login with the credentials you have been provided for your lab tenant 1. In the left navigation pane of the Microsoft 365 compliance center, click **Show all…**, then click **Insider risk management**. 2. On **Overview** tab, hover over each of the following: • **Alerts to review** • **Active cases** • **Users** • **Policies with most activity** 3. Click the **Policies** tab. 4. Click **Create policy.**

What is it	Where is it and what to do
resignation and termination dates from an HR system that enables the policy to detect potential data theft by departing users, such as downloading files from SharePoint or Teams, or copying files to portable devices. The Data leaks policy templates can be associated with a DLP policy to help detect when users accidentally or intentionally share sensitive information outside your organization or in violation of your information protection policies. You also can associate a data theft policy with an HR connector to detect when a disgruntled employee may be intentionally leaking or sharing sensitive and confidential information with malicious intent or for potential personal gain. Leading indicators of someone being disgruntled include someone being demoted or being put on a performance improvement plan. If you have deployed Microsoft Defender for Endpoint, you also can create policies to help detect for security violations such as installing malicious software or disabling multi-factor authentication. Let's choose the Data theft by departing users template and you'll give the policy a number such as Data leak by disgruntled employee (x) as the name of the policy. Because privacy is an important aspect to this solution, you have control over what is happening. You can choose to select this one checkbox and have everybody in your organization be in policy or you can scope it to specific users. As part of this lab, you're just going to select everyone just to keep it simple. Next thing is the ability to choose any content that you want to prioritize. Let's say you're creating a policy for your research and development team	5. Click on **Data theft > Data theft by departing users** to review the template settings. 6. Click on **Data Leaks > General data leaks** to review the template settings. 7. Click on **Data Leaks > Data leaks by disgruntled users** to review the template settings. 8. Click **Next**. 9. Type **Data theft by departing users** in the **Name** field, then click **Next**. 10. Select Include **all users and groups**, then click **Next**. 11. On the **Specify what content to prioritize** page, review the options and select the **I <u>don't</u> want to specify…** option selected.

What is it	Where is it and what to do
that's working on a super-secret project where those project files include specific labels or sensitive information types or maybe they reside on a very specific set of SharePoint sites. Here is where you can define what those are and automatically treat those as higher priority. A higher priority increases the risk score associated with any activity related to those sites, information types, or labels. For now, let's leave any custom settings and not specify any content right now. The next piece is a set of indicators you can choose. Rather than having to rely on setting up complicated feeds to bring in data from your cloud services into a central User and entity behaviour analytics, security analytics platform, or security, information and event management solution (SIEM), all you need to do here is check a box for the types of activities you want to monitor. Whether you want to see activity from SharePoint or Teams, download activity or sharing activity, it is all done with a simple click of a box. Furthermore, when you are talking about Windows 10/11 devices, there are no endpoint agents you must deploy because it's built into the product itself. If your organization is managing those Windows devices, you just navigatehere and select the signals that you want. Because each company is unique, you can customize the thresholds for each of these indicators. You can either use the recommended thresholds or, if you choose, you can turn that	**Note**: This review of the policy wizard will there's quite a few settings that we'd setup within a production environment, however for the lab we will walk through the basics. Feel free to click on each of the options to familiarize yourself with what's possible. The platform is forever changing so new options or features in preview happen regularly. Click **Next** to advance to the **Triggers for this policy.** 12. **Triggers for this policy**, review the different options that are available for this template. If we setup the HR connector to sync resignation or performance employee data we can also use this metric as a risk score booster. 13. Click **Next** to advance to the **Indicators and policy indicators page**. 14. Scroll through **Office indicators**. 15. Scroll through **Device indicators** and **others**. **Note**: There are other indicators on this page and new indicators are added frequently. Feel free to discuss any of these indicators that might be of interest. 16. Click **Next**. 17. Click on **Specify custom thresholds** and scroll through the list to review the granular settings that are available. 18. Click **Next** to review all the policy settings.

What is it	Where is it and what to do
toggle off and customize it to what you consider to be a low, medium, or high impact risk score based on your custom thresholds. At the end of the wizard, you can review your policy settings. Because we have already set up some policies, we will Cancel this policy without submitting it. Now let's take a look at Insider risk analytics to see if there are any potential risks that exist that additional policies could help. Insider risk analytics enables you to conduct an evaluation of potential insider risks in your organization without configuring any insider risk policies. We can see from the scan results that there has been some activity including things like users downloading SharePoint files and sending emails to users outside the organization. Analytics will recommend policies that can be created to help detect and prevent activity such as accidental oversharing of information outside of the organization or data theft by users with malicious intent. (Within the lab it's difficult to create a lot of traffic like a production environment would do.) You can launch the create policy wizard right from the recommendation panel with the recommended policy template selected. Now that we have seen how easy it is to create a policy, let's walk through the investigation and remediation capabilities of the insider Risk Management solution in Microsoft 365. So here we have a case that needs to be reviewed. This is a macro view of the user's activity. In this case, you can see where you would have the ability to go back to review the user's activity for several	19. Click **Cancel**. **Note**: The policies needed for the investigation is already set up for you so you can cancel this wizard without saving. 20. Click on the **Overview** tab 21. Scroll down to the **Insider risk analytics** section and click **View Results.** 22. In the **Potential data leak activities section**, click on **View details**. 23. Review the activity and recommendations offered by Analytics in the fly out window. **Note:** The results of analytics recommendations will vary as this isn't a production environment. 24. Click **Close**. 25. In the **Top exfiltration activities section, review the activities and click View details**. 26. Review the activity and recommendations offered by Analytics in the fly out window. 27. Click **Cancel.** 28. Return to the Insider risk management **Overview** page and click the **Cases** tab, then click on the case that has already been created, **Case 032: Potential data leak.** 29. Click the **User activity** tab. (click on **1 Month** to get a closer look at the more recent events that are displayed represented as bubbles.) 30. Click on the bubbles to show the types of events and details.

What is it	Where is it and what to do
months and view activity around things like data exfiltration and email activity. The context you need for the review is included in that view and as you scroll down, and can get a chronological view as well. Not only is this macro exploration available, *Activity explorer* also gives me a micro view into the user's activities which literally spans seconds or a sequence of seconds. This lets us dig in and get specific logs one line at a time on what the user was up to and relate it to the different events where there's data exfiltration and other activities that have taken place. We can look at different types of events, and of course, dig into specific events to get more details.	31. Click the **Activity explorer** tab. 32. Click on the **Activity filter** to see a summary of the types and counts of each activity for that user. 33. Hover over the various line items in the right panel. 34. Click on one of the line items to display the details flyout page. 35. Scroll down to the **Exfiltration** event that shows you how many email, data types where automatically found. 36. Click **Close** or the **X** in the upper right corner to close the details page.
On the *Content explorer* tab, you can see a list of any emails and files captured in the case and view a preview of the document directly in the Content explorer. This allows you to evaluate the content that is matching the policies.	37. Click on the **Content Explorer** tab 38. Review the list of documents and **click on a document** to see the preview of the document in the Source window.
As you review this case, there are notes you might want to add to associate them with the case. You can call out things in the Activity and content explorer views or add external information that will be helpful in the resolution of the case. Another feature of the insider risk management solution is the ability to bring in different collaborators and contributors into the solution who can create case notes and help review cases. You can also associate each case with a different Teams team in order to collaborate and have a workspace for managing documents, managing	39. Click on the **Case notes** tab 40. Click **+ Add case note** 41. **Type a note** and click **Save.** 42. Click the **Contributors** tab to briefly display the contributors that have been added. 43. At the top of the Contributor's tab, click the **Case Actions** dropdown and review each of the elements. 44. Notice that you can also copy a link to the case and collaborate within MS Teams.

What is it	Where is it and what to do
notes, and creating secure communication channels to communicate with my collaborators across other departments.	
The insider risk management solution in Microsoft 365 is also integrated with the Power Automate platform which can help drive efficiency by automating different tasks. Oftentimes you will find yourself having to manually execute a task over and over; whether it's going into Outlook, sending an email summarizing what's happening, get the response back, track the response, all that stuff. Or maybe you are required to notify specific users on certain actions or check with a manager on whether or not the observed activity is in line with expected duties are not. These are examples of workflows. Well, with the integration into Power Automate, you can create these workflows in the tool which saves time and helps to move the investigation along. You also can escalate a case for further investigation. So not only does the insider risk solution help to identify risks and investigate them but escalate those cases to Advanced eDiscovery due to a litigation or law enforcement escalation right out of the box.	45. Hover over the **Case Actions > Automate > Manage Power Automate flows.** **Note:** It is not in the scope of this lab to run any of the flows at this time. Please view the built-in templates. Power Automate is very powerful and can be used to trigger a lot of different playbooks for automation. 46. Click on **Case Actions > Escalate for investigation** 47. Click **Cancel** 48. Click **Send Email Notice** 49. Review how the email is sent to the individual anonymized for privacy. The reviewer doesn't need to know who the individual is and click **Cancel**.
That is it for this lab, you've gone through the basics of how Insider risk management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Insider risk policies allow you to define the types of risks to identify	**Lab Complete**. If you are ahead of time go back and review the audit information for the reviewers. Navigate back to the main Insider Risk Management overview page. Click on the **Insider Risk Audit Log** (**Clipboard** icon),

What is it	Where is it and what to do
and detect in your organization, including acting on cases and escalating cases to Microsoft Advanced eDiscovery if needed. Security and compliance analysts in your organization can quickly take appropriate actions to help keep users in compliance with your organization's standards.	situated at the very top right of the overview page. Here you can see all the activities of the reviews of the cases, a full log of what was done is also captured.