



Starting an insider risk management program



March 2022
pwc.com/us/microsoftcybersecurity



Table of contents

2	Executive summary
4	Insider risk fundamentals
6 - 10	Managing insider risk <ul style="list-style-type: none">• Getting started with a program• Accelerating time to action
11 - 15	Mitigating common insider risks within Microsoft 365 <ul style="list-style-type: none">• Workplace harassment• Misuse of patient data in healthcare industries• Data theft by priority users• Satisfying regulatory compliance obligations
16	Future considerations

Executive summary

High profile insider risk incidents continue to occur across industries, ranging from data theft to corporate code of conduct violations. Recent examples have included the theft of confidential documents related to COVID-19 vaccines in the pharmaceutical industry to threats and harassment made towards employees in the workplace. These incidents continue to raise awareness of insider risk at organizations, driving many to establish insider risk programs.

How employees and contractors interact with data has changed significantly, with an all in-person workplace no longer the norm. A third of executives (33%) will have a mixed model¹, with some in-person full-time, some hybrid and some fully remote. This hybrid approach can bring challenges to managing insider risk; communication and collaboration no longer sits within the traditional confines of offices buildings, resulting in potentially less relevant on-premise security controls.

Organizations with existing insider risk programs should consider the effectiveness of their program when users are operating outside the organization's offices and network. These factors, combined with increases in cloud adoption have resulted in an increased possibility of accidental or intentional misuse of data that requires an effective approach to insider risk.

An insider risk program does not need to be highly sophisticated to be effective. At their core, successful insider risk programs help identify and investigate risks, quickly take actions against those risks and mature the program through

progressive iterations. This paper aims to encourage organizations to get started with building an insider risk program, outlining the practical steps to kick off the program – while enabling organizations to maintain end user privacy.



¹ Source: [PwC US Pulse Survey, August 19, 2021](#).

Starting out with insider risk has never been easier. Advances in technology and increases in security investment have resulted in many organizations having the components required to get started with building an insider program. One of the most common blockers for organizations in starting a program is understanding what potential insider risks exist and should be prioritized.

PwC and Microsoft advocate for an enterprise-wide approach to insider risk. This approach allows organizations to leverage key stakeholders to identify areas of potential insider risks, which in turn are used to tailor technical controls to address those risks.

This approach consists of three key components:



A Program Sponsor with the authority and accountability to bring together the required areas of the organization.



An understanding of the assets the program needs to protect and the associated risks.



Technology to support risk identification and trigger the investigation process.

Insider risk fundamentals

Insider risk definition

Insiders are commonly defined as current or former members of the workforce with authorized access to, or knowledge of, an organization's assets, facilities, information, or people.

Insiders become a risk when they willingly, knowingly, or inadvertently use or exceed that access to harm the organization or other employees. One of the most common insider risk scenarios is when an employee leaving an organization seeks to take files and data with them to their future employer. This may include trade secrets, pricing data or sales and opportunity information that could negatively impact the organization to which the data belongs.



69%

of practitioners experienced over 5 malicious insider risk incidents







84%

of practitioners experienced over 5 non-malicious insider risk incidents²

² [Source: Insider Risk Management Program Building: Summary of Insights from Practitioners, May 2021](#)

Common types of insider risks

Insider risks commonly span six broad categories:

					
Data leakage	Data theft	Workplace harassment	Sabotage	Internal fraud	Espionage

When determining the insider risks relevant to your organization, consider which of the insider risk categories are most relevant to your industry. For example, technology organizations often wish to protect intellectual property, healthcare organizations often seek to protect patient data and financial services look to protect against insider trading.

What is an insider risk program?

Throughout this paper, we refer to an insider risk program as a mechanism of managing insider risk. Insider risk programs help to manage the risks posed by insiders through specific prevention, detection, and response practices and technologies.

Effective insider risk management programs identify critical assets and potential insider risks that put those assets at risk. These programs typically establish high-risk insider scenarios and identify additional risks as they evolve. They are designed to proactively identify insider activity, achieve early intervention, and help reduce negative impacts, while balancing end user privacy

Building an insider risk program is the first step in achieving early intervention.

Managing insider risk

Engage across the organization

PwC and Microsoft advocate for an enterprise-wide approach to insider risk; leveraging key stakeholders to help identify insider risks and implement technical policies to address them.



When starting an insider risk program, consider consulting with Security, Compliance, Technology, Human Resources, Legal/Privacy and business representatives to understand the right approach for the organization, based on local regulations, business critical assets, employee culture and workplace policies.

One of the most critical factors in starting an insider risk program is gaining support of these stakeholders to allow for insider risks to be identified, technical and non-technical policies to be implemented and a defined response for when risks are realized. As the program grows, additional formalization will be required to scale the program and can help its consistent application.

Getting started with a program

Managing insider risk often requires a formalized, codified program to be effective. A program does not need to be complex and should scale based on the size of the organization and the insider risks faced.

Organizations typically need the following three things to get started:



A Program Sponsor with the authority and accountability to bring together the required areas of the organization; Security, Compliance, Technology, Human Resources, Legal/Privacy and business representatives. The sponsor should drive the implementation of relevant policies and technology, and advocate for relevant training and awareness opportunities.



An understanding of the assets and associated risks across the organization that the program needs to protect. Identifying risk can be as informal as a brief conversation with a colleague through to a formal insider risk investigation.



Technology to support the risk identification and trigger the investigation process.

Program sponsor

A sponsor will help provide decision making oversight and set the direction and the “tone at the top” of the program. The sponsor will support the development of the program while also aligning the program to the broader organizational culture. Depending on the size of your organization, you may have several potential sponsors. We often see the Chief Information Security Officer, Chief Risk Officer, General Counsel, Chief Operating Officer or Chief Security Officer as the sponsor. The sponsor can help bring in additional stakeholders relevant to the program; for example, Human Resources are often engaged for code of conduct violations and Security for data leak investigations.

Identifying insider risks

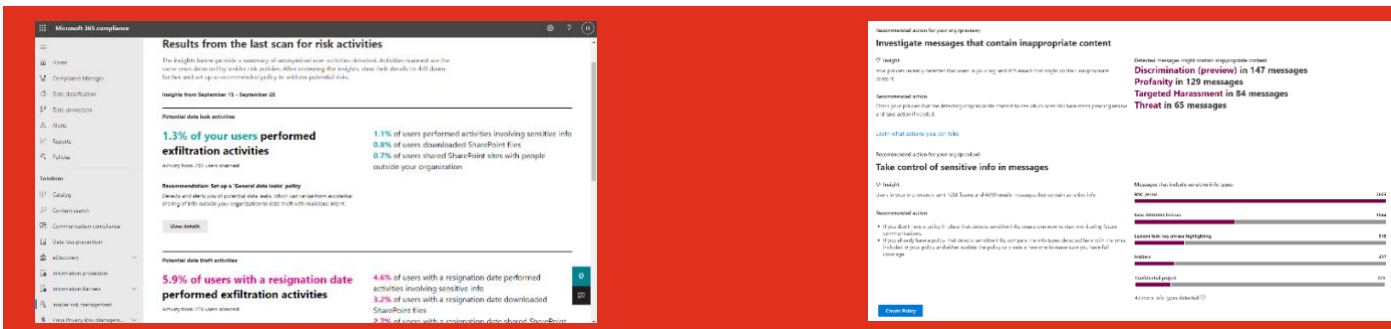
Identifying sensitive information assets and the potential insider risks associated with the information is a key aspect of any insider risk program. The risk identification process should be repeated often to help inform the technical and non-technical policies required.

Identifying risk can be as informal as a brief conversation with a colleague through to a formal insider risk investigation. Both approaches are valid mechanisms for helping identify insider risk, however as the insider risk program matures, formal mechanisms such as insider risk workshops, and risk registers will likely allow for the effective on-going management of the insider risk program. Other insider risk stakeholders may have documents that outline risky behaviors, for example, consult with HR on requirements within the organization’s anti-discrimination, anti-harassment, or code of conduct policies.

Existing sensitivity labels or data classification frameworks can support the identification of sensitive information in an organization. Once identified, the program can begin to identify potential risks associated with that information. For example, could documents describing a manufacturing process provide an advantage to a competitor? If so, this intellectual property data loss scenario may be a risk the program should seek to mitigate.

Technology policies

Technology is at the heart of every insider risk program. Microsoft 365 Insider Risk Management can be used to identify, triage, and act on risky user activity. Integrations with other sources such as HR data can help identify risky behavior, for example data theft by a departing employee.



Microsoft Communication Compliance helps discover communication risks such as sharing of adult content, harassing or threatening language, or sharing of sensitive information.

Built with privacy by design, usernames are pseudonymized by default, and role-based access controls and audit logs are in place to help organizations provide user-level privacy in both solutions. When implemented, these technologies can provide a broader view of risky behavior across the organization while allowing an organization to take immediate action.

As an initial step of starting an insider program, consider enabling the Microsoft 365 Insider Risk Management Analytics and Microsoft 365 Communication Compliance [Recommended Policy Actions](#) features. When enabled, these features can provide aggregated insights into the trends that are occurring in your organization while maintaining employee privacy. For example, you can see the amount of sensitive information that is commonly shared over email or Microsoft Teams chats or the percentage of departing employees downloading sensitive or proprietary information to a USB drive.

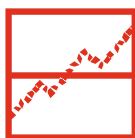
Consider discussing these trends with the Program Sponsor on what policy templates could be enabled based on the identified risky behavior. These trends combined with your organization's employee culture and privacy requirements can help to determine what technology policies and privacy controls are appropriate for your organization. Employee culture and privacy is a critical component to the success of insider risk programs and mechanisms can be put in place to help protect employee privacy. For example, many organizations choose to implement pseudo-anonymity during the initial alerting stage, masking employee names to maintain privacy. Consider the scope of the policies that are being implemented, many can be applied to higher risk areas of the organization rather than the broader organization. Additionally, designated admins can scope policy investigators to specific policies, based on their area of

expertise. We often see organizations looking to data loss prevention (DLP) as a way of managing insider risk. While these technologies differ in how they operate, they are often complimentary and can work together as part of a defense in depth strategy to managing insider risk. An insider risk program differs from a DLP program or strategy by focusing on medium to long-term behavioral indicators of risk, rather than individual transactions made by users. Where DLP excels at blocking egregious actions and preventing known risks, contextual behaviors surfaced through insider risk technologies like Microsoft 365 Insider Risk Management, can highlight threats that fall outside that scope or that may not have initially triggered an alert. DLP and insider risk technologies can work better together to enable your insider risk program to provide a more comprehensive view of behavioral risk.

Key Questions to explore



What insider risk areas warrant most attention in your organization?



Have trends in previous insider incidents been observed?



Do specific areas of the organization have an elevated risk?

Accelerating time to action

Established insider risk programs often look at ways of accelerating the time to action when risky behavior has been identified.

Investigations can be time consuming, especially when analyzing multiple data sources. Mature organizations improve the triage process to enable teams to quickly identify and act on potentially harmful activity. Organizations utilizing Microsoft Insider Risk Management can review the alert context during the triage phase. For example, this could highlight whether the user has a resignation date, along with a summary of the activity that was detected that led to an alert being created. This helps focus their detailed review on the riskiest activities and prioritize the alert and triage efforts. Organizations utilizing privacy centric controls such as pseudonymity can proceed with an initial triage while maintaining privacy. Thresholds can also be utilized to enable security teams to

customize their policies and triggers, which can help in management of potential alerts and with prioritizing those activities that are considered higher-risk.

There are several methods for triaging alerts. Microsoft Insider Risk Management integrates with Microsoft Sentinel, allowing organizations to collect, detect and investigate insider risk activities. This allows a single pane of glass to review alerts for insider risk in a broader organizational context. In Communication Compliance, events are tracked within Microsoft 365 Audit (also known as "unified audit log") and can be imported into Microsoft Sentinel.



Finally, the discovery and search components of eDiscovery can be the most costly and time consuming phase of an investigation. Both Microsoft Insider Risk Management and Communication Compliance are integrated with Advanced eDiscovery, allowing an investigator to escalate directly to Advanced eDiscovery to kick off a legal investigation.

Mitigating common insider risks within Microsoft 365

PwC and Microsoft consider data exfiltration by a departing employee to be a common scenario and a good starting point for all insider risk programs, regardless of industry. This basic scenario requires correlation between various log sources, including employee data, however this can be quickly enabled within Microsoft 365 Insider Risk Management through the data theft by departing users policy template.

Once this policy template has been enabled, the insider risk program is ready to identify additional insider risks applicable to the organization.

Data exfiltration by a departing employee is one of many insider risk scenarios. Consider how the risk scenarios below may be relevant to your organization with the following case studies



Workplace harassment

With more and more communication and collaboration taking place outside the traditional confines of offices buildings, organizations need to manage risk in communications. Using Communication Compliance, PwC and Microsoft have supported organizations in detecting code of conduct violations such as sharing of adult imagery or using threatening language in the workplace.

Once a policy is configured and policy alerts are triggered, the alerts are reviewed by a policy investigator, who is explicitly granted permission to review policy alerts by the Communication Compliance admin role. The investigator can respond in several ways,

including notifying the employee that a workplace policy has been violated, removing the message from a Microsoft Teams chat or channel, or escalating to a team for further action.

When considering if this [policy template](#) is appropriate for your insider risk program, consider what type of communication is appropriate within your organization. Does an employee handbook exist within the organization that outlines the types of communication appropriate in the organization?

Microsoft 365 compliance

Communication compliance > New policy

1 Name
2 Users and reviewers
3 Locations
4 Conditions and percentage
5 Finish

Choose conditions and review percentage

Communication direction *

- ☒ **Inbound.**
Detects communications sent to supervised users from external and internal senders, including other supervised users.
- ☒ **Outbound.**
Detects communications sent from supervised users to external and internal recipients, including other supervised users.
- ☒ **Internal.**
Detects communications between the supervised users or groups in this policy.

Conditions

By default, we'll monitor all communications from the users and groups you specified. To refine the scope of this policy, we limit the results to communications matching specific criteria. [Learn more about these conditions.](#)

Content matches any of these classifiers

[Add](#)

[Trainable classifiers](#)

Optical character recognition(OCR)

OCR extracts printed and handwritten text from embedded or attached images in email and Teams chat messages so you can search for keywords.

☐ Use OCR to extract text from images.
OCR can only be used for policies that detect keywords, trainable classifiers, or sensitive info types.

Review percentage

If you want to reduce the amount of content to review, specify a percentage. We'll randomly select this amount of content from the conditions you chose.

[Back](#) [Next](#)

Trainable classifiers

4 selected

Name	Supported Languages
Source code	English
<input checked="" type="checkbox"/> Targeted Harassment	English, French, German, Italian, Japanese...
<input checked="" type="checkbox"/> Profanity	English, French, German, Italian, Japanese...
<input checked="" type="checkbox"/> Threat	English, French, German, Italian, Japanese...
Resume	English
<input checked="" type="checkbox"/> Discrimination	English
Finance	English
IT	English
Healthcare	English
Legal Affairs	English
Agreements	English
HR	English
IP	English
<input checked="" type="checkbox"/> Adult images	
<input checked="" type="checkbox"/> Racy images	
<input checked="" type="checkbox"/> Gory images	

[Add](#) [Cancel](#)

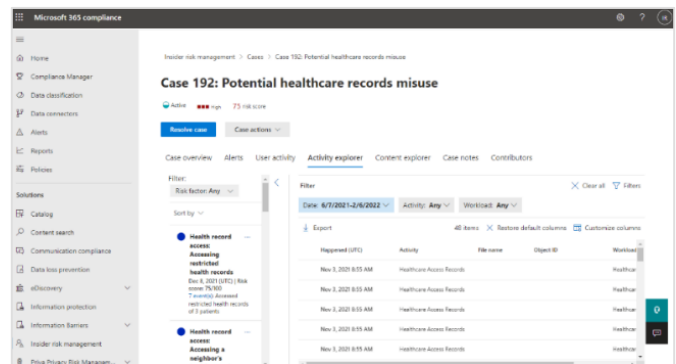
Misuse of patient data in healthcare industries

Healthcare organizations have historically suffered from a very high rate of insider-related data breaches. Data in healthcare is often sensitive and misuse of data is a common insider risk requiring mitigation by insider risk programs in the Healthcare industry.

The challenge of managing data misuse stems from the fact that Healthcare users often deal with a vast amount of highly sensitive data that must be kept current and accessible in a very timely manner as life and death decisions can depend on it.

By implementing a [healthcare policy template](#) within Microsoft 365 Insider Risk Management, many healthcare organizations have been able to identify potential data misuse scenarios. For example, identifying users who are viewing data relating to a patient who lives on the same street.

Microsoft 365 Insider Risk Management has built-in indicators and detections that leverage data from Epic and other electronic medical records (EMR) solutions to help organizations identify potential insider risks related to patient data misuse



Data theft by priority users

Not all users in an organization have access to sensitive information assets. With limited resources, organizations often attempt to identify priority users. The intent of identifying the high-risk roles is to enable additional prevention and detection policies to be applied in accordance with the increased risk.

A user's priority may depend on their role, level of access to sensitive information, or risk history. For example, in Financial Services, priority users may include individuals within Wealth Management with access to sensitive financial and contact information of key clients. In pharmaceutical organizations, it may include users with access to data relating to the manufacturing processes.

By implementing a [data leaks by priority users template](#), organizations can start identifying risky behavior ranging from data theft to the installation of malware or other potentially harmful applications or disabling security features on their devices.

When considering if this policy template is appropriate for your insider risk program, consider which user groups may be priority users. Are there specific roles in the organization which could increase insider risks? Could certain access levels increase the potential impact of a malicious event? Are there any behavioral indicators that may increase the priority of a user?

Microsoft 365 compliance

Insider risk management > New insider risk policy

Choose a policy template

These templates are made up of conditions and indicators that define the risk activities you want to detect and investigate. All templates rely on a triggering event to occur before the policy will begin assigning risk scores to user activity. Triggering events are different depending on the template you choose, and prerequisites are required for some policies to work. [Learn more about templates](#)

To bypass triggering event requirements, you can temporarily assign risk scores to users based on activity detected in this policy. [Learn how to do this](#)

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)

Data leaks by priority users (preview)

Detects data leaks by users included in a priority user group. Data leaks can range from accidental oversharing of information outside your organization to data theft with malicious intent. [Learn more about this template](#)

Prerequisites

- A priority user group is created in insider risk settings
- (Optional) Data loss prevention (DLP) policy configured to

Next **Cancel**

Satisfying regulatory compliance obligations

Insider Risk Management and Communication Compliance can be used to align to industry regulations. Each industry's regulatory compliance obligations are different; for example, the financial services industry is subject to FINRA and SEC regulations to show proof of supervision, the food and pharmaceuticals industry is subject to FDA regulations to detect and triage customer complaints on products or services, and the oil and gas industry is subject to NERC SIP regulations around maintaining an efficient flow of power to a power grid.

The [regulatory compliance template](#) in Communication Compliance can help financial services organizations meet supervision requirements such as FINRA Rule 3110 and SEC Rule 17a-4.

Microsoft 365 compliance

Communication compliance

Policies Alerts Reports

+ Create policy Export policy updates Refresh

8 items Search Customize

Policy name	Items pending review	Resolved items	Status	Last modified	Last policy scan
Sabotage	59	8	Active	Oct 29, 2021 12:50 PM	Feb 21, 2022 6:43 AM
New CC Policy from Lexicon Custom Dictio	21	0	Active	Aug 10, 2021 9:37 AM	Feb 21, 2022 5:42 AM
Yammer ONLY	11	0	Active	Mar 11, 2021 2:07 PM	Feb 20, 2022 9:02 PM
Conflict of interest - Sales and Finance	8	0	Active	Jun 10, 2021 7:35 PM	Feb 21, 2022 6:36 AM
Insiders	1642	133	Active	May 4, 2021 6:26 PM	Feb 21, 2022 4:05 AM
Teams ONLY	492	25	Active	Jul 7, 2021 1:27 PM	Feb 21, 2022 2:24 AM
Catch ALL	1741	1751	Active	Oct 6, 2021 10:20 PM	Feb 21, 2022 8:28 AM
Offensive or threatening language	19	15	Active	Oct 28, 2021 8:27 AM	Feb 20, 2022 10:03 PM

Recommended action for your org (preview)

Investigate messages that contain inappropriate content

Insight

Your policies recently detected that users in your org sent 11 emails that might contain inappropriate content.

Recommended action

Check your policies that are detecting inappropriate content to see which ones still have items pending review and take action if needed.

Detected messages might contain inappropriate content

- Threat in 5 messages
- Profanity in 3 messages
- Targeted Harassment in 3 messages

Monitor communications for info related to financial regulatory compliance

About this template

Set up a policy to monitor communications that might contain info that might be related to insider trading, such as messages containing credit card numbers. To detect this info, you can choose from built-in or custom sensitive info types or upload a new keyword dictionary.

Settings we need from you

Policy name *

Regulatory compliance

Users or groups to supervise *

☒ All users ☐ Select users

Start typing to find users or groups

Reviewers *

Start typing to find users

Sensitive info to monitor *

None selected. You can choose sensitive info types or an existing keyword dictionary.

[Add sensitive info](#)

Settings we've filled in for you

[Create policy](#) [Customize policy](#)

Organizations in highly regulated industries, such as financial services, pharmaceuticals and food, are mandated by law to track and address customer complaints made on their product or services. By configuring Communication Compliance's customer complaint classifier, organizations can detect possible complaints filed by customers and surface matches for appropriate customer complaint management to investigators.

Future considerations

As with all security initiatives, program maturity will come through with investments in people, process, and technology. Many organizations can mature their insider risk programs by focusing on identifying insider risks relevant to their critical assets. This helps drive the technology requirements and informs the technology policy configurations required to successfully identify risky behavior.

Identifying risky behavior in the organization and intervening early is a goal for many mature programs. By intervening early, organizations can avoid the expense of long investigations and impact of insider risks. Common early intervention techniques include proactive messaging, awareness of an insider risk program and implementing preventative controls to priority user groups.

Interested in learning more?

The Microsoft 365 compliance solutions trial is the easiest way to try all the capabilities of Microsoft compliance solutions. After the trial setup is complete, all features of the Microsoft E5 license package are available for you to use for up to 90 days. Learn more about easy trials [here](#).

Learn more about Insider Risk Management, how to get started, and configure policies in your tenant in this [supporting documentation](#).

Learn more about what's new with Communication Compliance and how to get started and configure policies in your tenant in this [supporting documentation](#).

For a further conversation on insider risk management with PwC, please reach out to the authors below.



Contacts

John Boles

Principal, PwC Cybersecurity Risk and Regulatory,
PwC US

John.boles@pwc.com

Sloane Menkes

Principal, PwC Cybersecurity Risk and Regulatory,
PwC US

Sloane.menkes@pwc.com

Matt Gregson

Director, PwC Cybersecurity Risk and Regulatory,
PwC US

gregson.d.matthew@pwc.com

Raman Kalyan

Director of Product Marketing

Raman.kalyan@microsoft.com

Katie Anderson

Senior Product Marketing Manager

Katherine.anderson@microsoft.com

Liz Willets

Product Marketing Manager

Liz.walker@microsoft.com

Thank you

pwc.com

© 2022 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2022 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

