Insider Risk Management

examlabpractice.com

REFERENCE: https://learn.microsoft.com/en-us/purview/insider-risk-management

What is insider risk management used for?

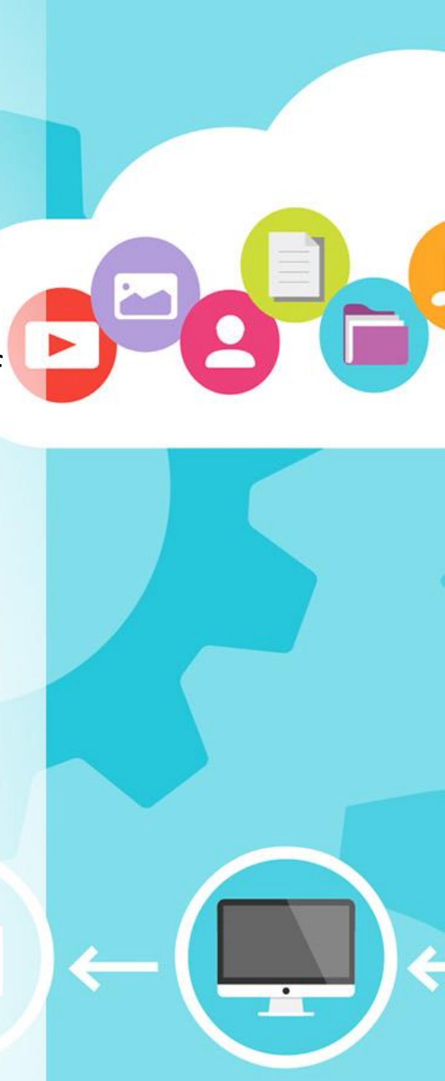
- Microsoft Purview Insider Risk Management is a compliance solution that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization.
- Insider risk policies allow you to define the types of risks to identify and detect in your organization, including acting on cases and escalating cases to Microsoft eDiscovery (Premium) if needed.
- Risk analysts in your organization can quickly take appropriate actions to make sure users are compliant with your organization's compliance standards.

Modern Risk Pain Points

Managing and minimizing risk in your organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external events and factors that are outside of direct control. Other risks are driven by internal events and user actions that can be minimized and avoided. Some examples are risks from illegal, inappropriate, unauthorized, or unethical behavior and actions by users in your organization. These behaviors include a broad range of internal risks from users:

- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

Users in the modern workplace have access to create, manage, and share data across a broad spectrum of platforms and services. In most cases, organizations have limited resources and tools to identify and mitigate organization-wide risks while also meeting user privacy standards.



Principles of Insider Risk Management

Transparency: Balance user privacy versus organization risk with privacy-by-design architecture.

Configurable: Configurable policies based on industry, geographical, and business groups.

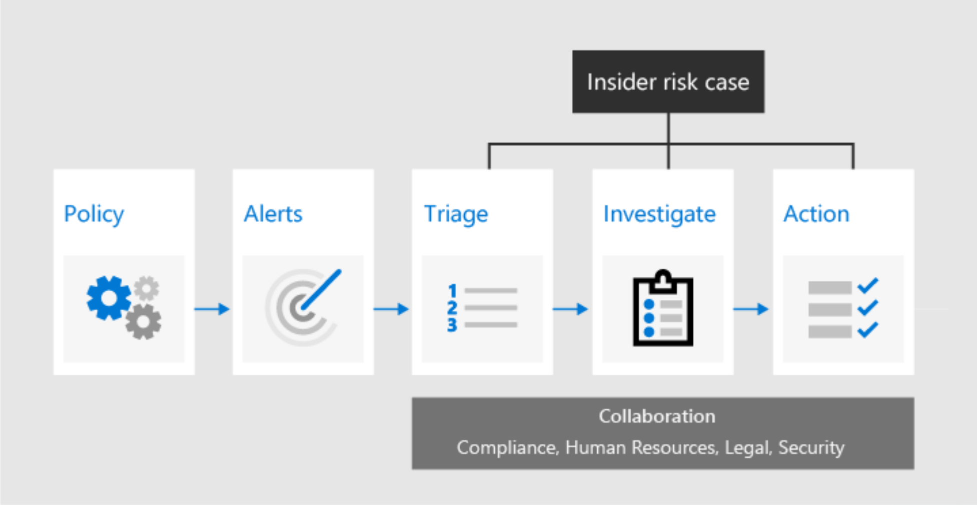
Integrated: Integrated workflow across Microsoft Purview solutions.

Actionable: Provides insights to enable reviewer notifications, data investigations, and user investigations.

Workflow

The insider risk management workflow helps you identify, investigate, and take action to address internal risks in your organization. With focused policy templates, comprehensive activity signaling across the Microsoft 365 service, and alert and case management tools, you can use actionable insights to quickly identify and act on risky behavior.

Identifying and resolving internal risk activities and compliance issues with insider risk management uses the following workflow:



Policies

Insider risk management policies are created using pre-defined templates and policy conditions that define what triggering events and risk indicators are examined in your organization. These conditions include how risk indicators are used for alerts, what users are included in the policy, which services are prioritized, and the detection time period.

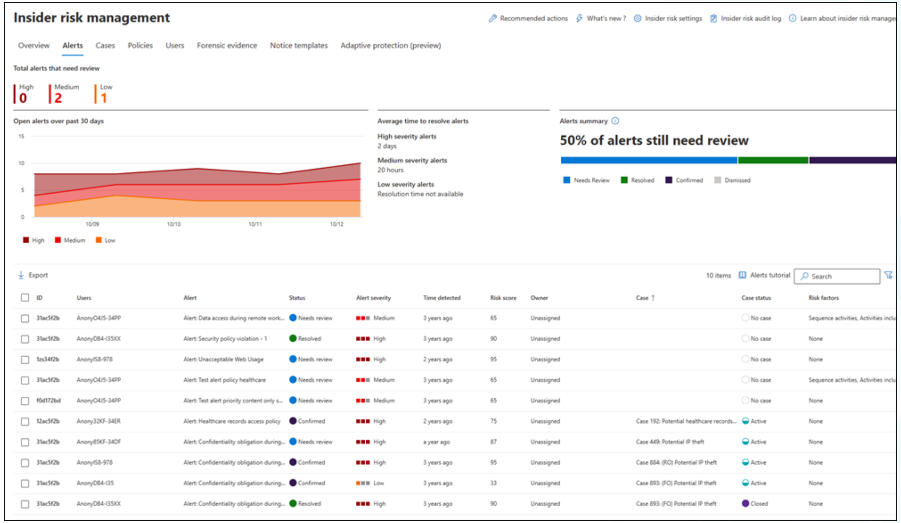
You can select from the following policy templates to quickly get started with insider risk management:

- Data theft by departing users
- Data leaks
- Data leaks by priority users
- Data leaks by risky users
- Security policy violations
- Security policy violations by departing users
- Security policy violations by risky users
- Security policy violations by priority users
- Patient data misuse
- Risky browser usage

Alerts

Alerts are automatically generated by risk indicators that match policy conditions and are displayed in the Alerts dashboard. This dashboard enables a quick view of all alerts needing review, open alerts over time, and alert statistics for your organization. All policy alerts are displayed with the following information to help you quickly identify the status of existing alerts and new alerts that need action:

- ID
- Users
- Alert
- Status
- Alert severity
- Time detected
- Case
- Case status
- Risk factors



Insider risk management

Total alerts that need review

High 0 | Medium 2 | Low 1

Open alerts over past 30 days

Average time to resolve alerts

High severity alerts
2 days

Medium severity alerts
20 hours

Low severity alerts
Resolution time not available

Alerts summary

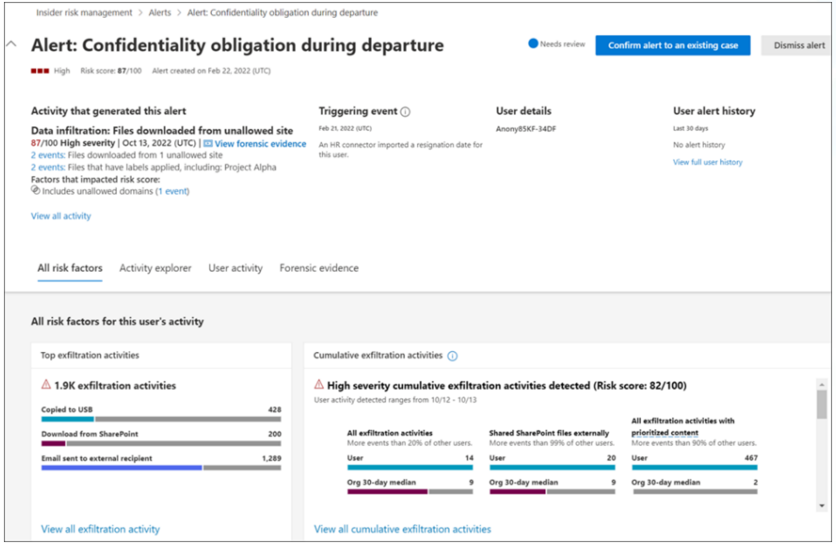
50% of alerts still need review

ID	Users	Alert	Status	Alert severity	Time detected	Risk score	Owner	Case ↑	Case status	Risk factors
31ac5f2b	AnonyO4J5-34PP	Alert: Data access during remote work...	● Needs review	Medium	3 years ago	65	Unassigned		○ No case	Sequence activities, Activities inclu
31ac5f2b	AnonyDB4-I35XX	Alert: Security policy violation - 1	● Resolved	High	3 years ago	90	Unassigned		○ No case	None
1zs34f2b	AnonyIS8-978	Alert: Unacceptable Web Usage	● Needs review	High	2 years ago	95	Unassigned		○ No case	None
31ac5f2b	AnonyO4J5-34PP	Alert: Test alert policy healthcare	● Needs review	Medium	3 years ago	65	Unassigned		○ No case	Sequence activities, Activities inclu
f0d172bd	AnonyO4J5-34PP	Alert: Test alert priority content only s...	● Needs review	Medium	3 years ago	65	Unassigned		○ No case	None
12ac5f2b	Anony32KF-34ER	Alert: Healthcare records access policy	● Confirmed	High	2 years ago	75	Unassigned	Case 192: Potential healthcare records...	◐ Active	None
31ac5f2b	Anony85KF-34DF	Alert: Confidentiality obligation during...	● Needs review	High	a year ago	87	Unassigned	Case 449: Potential IP theft	◐ Active	None
31ac5f2b	AnonyIS8-978	Alert: Confidentiality obligation during...	● Confirmed	High	3 years ago	95	Unassigned	Case 884: (RO) Potential IP theft	◐ Active	None
31ac5f2b	AnonyDB4-I35	Alert: Confidentiality obligation during...	● Confirmed	Low	3 years ago	33	Unassigned	Case 893: (FO) Potential IP theft	◐ Active	None
31ac5f2b	AnonyDB4-I35XX	Alert: Confidentiality obligation during...	● Resolved	High	3 years ago	90	Unassigned	Case 893: (FO) Potential IP theft	● Closed	None

Triage

New user activities that need investigation automatically generate alerts that are assigned a Needs review status. Reviewers can quickly identify and review, evaluate, and triage these alerts.

Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert. Using alert filters, it's easy to quickly identify alerts by status, severity, or time detected. As part of the triage process, reviewers can view alert details for the activities identified by the policy, view user activity associated with the policy match, see the severity of the alert, and review user profile information.


Insider risk management > Alerts > Alert: Confidentiality obligation during departure
Needs review
Confirm alert to an existing case
Dismiss alert
All risk factors
Activity explorer
User activity
Forensic evidence

Alert: Confidentiality obligation during departure

■■■ High   Risk score: **87**/100   Alert created on Feb 22, 2022 (UTC)

Activity that generated this alert

Data infiltration: Files downloaded from unallowed site
87/100 **High severity** | Oct 13, 2022 (UTC) | View forensic evidence
2 events: Files downloaded from 1 unallowed site
2 events: Files that have labels applied, including: Project Alpha
Factors that impacted risk score:
Includes unallowed domains (1 event)

View all activity

Triggering event

Feb 21, 2022 (UTC)

An HR connector imported a resignation date for this user.

User details

Anony85KF-34DF

User alert history

Last 30 days

No alert history

View full user history

All risk factors for this user's activity

Top exfiltration activities

⚠ **1.9K exfiltration activities**

Copied to USB	428
Download from SharePoint	200
Email sent to external recipient	1,289

View all exfiltration activity

Cumulative exfiltration activities

⚠ **High severity cumulative exfiltration activities detected (Risk score: 82/100)**

User activity detected ranges from 10/12 - 10/13

	All exfiltration activities More events than 20% of other users.	Shared SharePoint files externally More events than 99% of other users.	All exfiltration activities with prioritized content More events than 90% of other users.
User	14	20	467
Org 30-day median	9	9	2

View all cumulative exfiltration activities

Investigate

Selecting a case on the case dashboard opens the case for investigation and review. This step is the heart of the insider risk management workflow. This area is where risk activities, policy conditions, alerts details, and user details are synthesized into an integrated view for reviewers. The primary investigation tools in this area are:

- **User activity:** User risk activity is automatically displayed in an interactive chart that plots activities over time and by risk level for current or past risk activities. Reviewers can quickly filter and view the entire risk history for the user and drill into specific activities for more details.
- **Content explorer:** All data files and email messages associated with alert activities are automatically captured and displayed in the Content explorer. Reviewers can filter and view files and messages by data source, file type, tags, conversation, and many more attributes.
- **Case notes:** Reviewers can provide notes for a case in the Case Notes section. This list consolidates all notes in a central view and includes reviewer and date submitted information.

Action

In more serious situations, you may need to share the insider risk management case information with other reviewers or services in your organization. Insider risk management is tightly integrated with other Microsoft Purview solutions to help you with end-to-end risk resolution.

- **eDiscovery (Premium):** Escalating a case for investigation allows you to transfer data and management of the case to Microsoft Purview eDiscovery (Premium). eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations. It allows legal teams to manage the entire legal hold notification workflow. To learn more about eDiscovery (Premium) cases, see Overview of Microsoft Purview eDiscovery (Premium).
- **Office 365 Management APIs integration (preview):** Insider risk management supports exporting alert information to security information and event management (SIEM) services via the Office 365 Management APIs. Having access to alert information in the platform the best fits your organization's risk processes gives you more flexibility in how to act on risk activities.