

## Overview

Perparim Abdullahu, here are your top recommended actions

All recommended actions →

<b>Turn on auditing</b> <input type="radio"/> Start recording user and admin activity to the audit log.	Required	⌚ 2 min	
<b>Turn on analytics to scan for potential risks</b> <input type="radio"/> Scans run daily and provide real-time insights to help detect activity that matters most.	Optional	⌚ 48 hours	Includes video tutorial
<b>Get to know insider risk management</b> <input type="radio"/> Learn about the solution...what it is, best practices, common terms, and more.	Optional	⌚ 10 min	
<b>Configure insider risk settings</b> <input type="radio"/> Define settings that apply to all insider risk features and workflows.	Required	⌚ 10 min	Includes video tutorial
<b>Create your first policy</b> <input type="radio"/> Use predefined templates to detect risk activities, such as data theft.	Required	⌚ 5 min	
<b>Make sure your team can get their jobs done</b> <input type="radio"/> Assign permissions by adding other admins to insider risk management role groups.	Required	⌚ 10 min	Includes video tutorial

Microsoft 365

Insider Risk Management



⌚ 4 min

## Summary

No policy data found

No data available at this moment



# Deep Dive: Insider Risk Management in Microsoft Purview

Detect → Investigate → Act on insider threats

#PerparimLabs #MicrosoftPurview #InsiderRisk  
#MicrosoftSecurity #Compliance #ZeroTrust



## Maximize productivity with Security Copilot in Microsoft Purview

Use the power of AI to accelerate data discovery, analysis, and policy improvements

Get started

Learn more

Data Security Posture Management

Get centralized visibility into data security risks

Ask for insights into your current posture and recommended policy controls.

Learn more

Data Loss Prevention

Dive into incidents with ease

New enhanced hunting prompts go deep into incident data and users involved.

Learn more

Insider Risk Management

Identify risky user behavior, faster

Quickly understand user intent, activity timing, and top risk factors.

Learn more

Having trouble finding specific features or solutions?

Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features



Data Security Investigations  
(preview)



Data Catalog



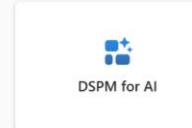
Information Protection



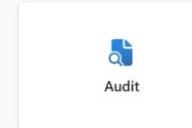
Data Loss Prevention



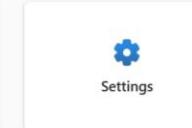
Insider Risk Management



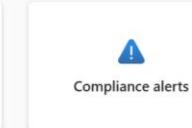
DSPM for AI



Audit



Settings



Compliance alerts



View all solutions →

# Why Insider Risk Matters

- Insider risks are **accidental or malicious**.
- Pain points:
  - Data spillage
  - Confidentiality violations
  - IP theft, fraud, insider trading
  - Compliance violations (HIPAA, GDPR, PCI)

Example: employee accidentally shares a financial spreadsheet with hidden customer data.

#PerparimLabs #MicrosoftPurview #InsiderRisk  
#MicrosoftSecurity #Compliance #ZeroTrust



Home



Solutions



Agents



Learn



Settings



Insider Risk Management

## Insider Risk Management

Overview

Recommendations

Policies

Reports

Forensic Evidence

Adaptive Protection

### Related solutions

Communication

Compliance

Data Security

# Policies

**⚠ Attention:** You currently aren't assigned to a role group that allows you to view alerts. Consider assigning somebody to this role [Learn which role groups are needed to review alerts](#)

Policy warnings

0

Policy recommendations

0

Healthy policies

0

*(i) Scan for potential risks in your org. Turn on analytics to scan user activity daily. You'll get real-time, pseudonymized insights to help you set up and refine policies so you're detecting the most relevant activity. [Learn more](#)*

*(i) **Review collection policies.** Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they're set up to detect the device activities you want to monitor. [Learn more](#)*

+ Create policy

Start scoring activity for users

Refresh

Filter

Users in scope

Active alerts

Confirmed alerts

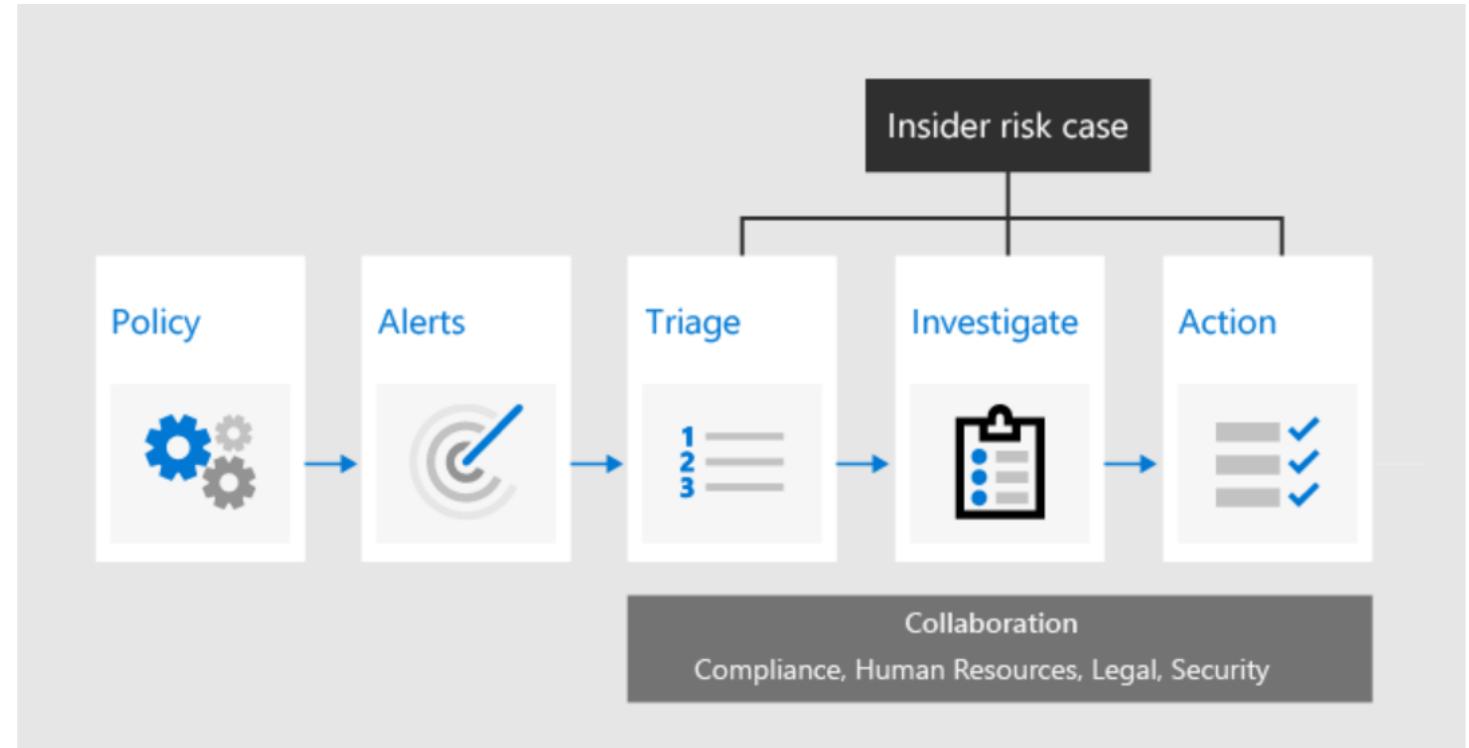
# Core Principles of Insider Risk Management

- Transparency (privacy + protection balance)
- Configurable policies
- Integration with M365/Purview
- Actionable insights + alerts

Example: masking usernames keeps investigations privacy-friendly.

# The Workflow

- Policy → Alerts → Triage → Investigate → Action



Example: departing user copies 500 files → alert → HR + Legal investigation.

Home

Solutions

Agents

Learn

Settings

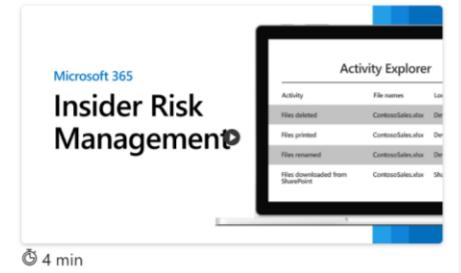
Insider Risk Management

## Overview

Perparim Abdullahu, here are your top recommended actions

All recommended actions →

<b>Turn on auditing</b> <input type="radio"/> Start recording user and admin activity to the audit log.	Required	⌚ 2 min	
<b>Turn on analytics to scan for potential risks</b> <input type="radio"/> Scans run daily and provide real-time insights to help detect activity that matters most.	Optional	⌚ 48 hours	Includes video tutorial
<b>Get to know insider risk management</b> <input type="radio"/> Learn about the solution...what it is, best practices, common terms, and more.	Optional	⌚ 10 min	
<b>Configure insider risk settings</b> <input type="radio"/> Define settings that apply to all insider risk features and workflows.	Required	⌚ 10 min	Includes video tutorial
<b>Create your first policy</b> <input type="radio"/> Use predefined templates to detect risk activities, such as data theft.	Required	⌚ 5 min	
<b>Make sure your team can get their jobs done</b> <input type="radio"/> Assign permissions by adding other admins to insider risk management role groups.	Required	⌚ 10 min	Includes video tutorial



## Summary

# Microsoft Purview in Action

- Wrap-up: Helps organizations detect, investigate, and act on insider risks while maintaining compliance.