# Insider risk management

MS Purview Insider Risk Management is a solution that helps minimise internal risks allowing you to detect, investigate, and act on risky or malicious activities:

- Leaks of sensitive data and data spillage

- Confidentiality violations

- IP theft

- Fraud

- Insider trading

- Regulatory compliance violations

Insider Risk Management centers around 4 principles:

- Transparency

- Configurable

- Integrated

- Actionable

Workflow
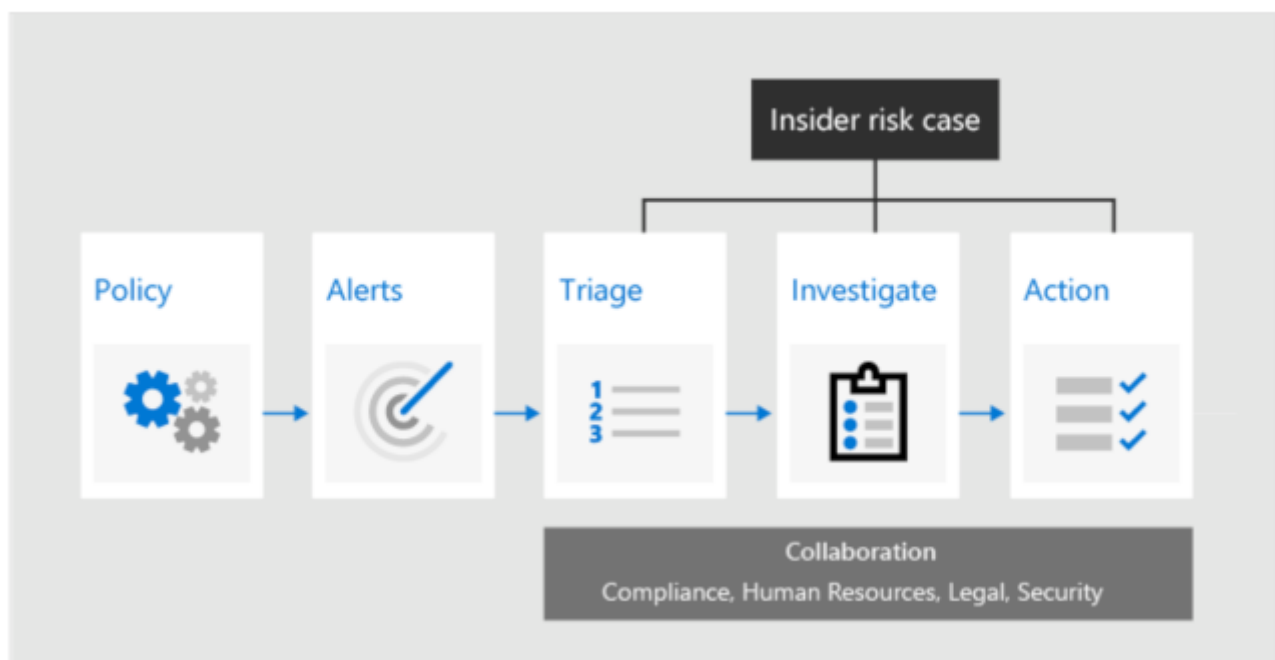
Policies - created using predefined templates and conditions defining what risk indicators are examined.

Alerts - automatically generated by risk indicators matching policy conditions

Triage - New activities that need investigation are surfaced here and resolved by opening a new case

Investigate - Cases are created for alerts that require deeper review

Action - After cases are investigated reviewers can act quickly to resolve it

Communication Compliance

Helps minimise communication risks by enabling orgs to detect, capture and take actions for inappropriate messages-

- Configure - admins identify compliance requirements and configure policies

- Investigate - admins look deeper at issue detected

- Remediate - tag a message, notify user, escalate to another reviewer, mark as false positive, or remove message from teams.

- Monitor - keep track of and manage compliance issues identified by policies ongoing.

Cases where communication compliance is useful

- Corporate policies

- Risk Management

- Regulatory compliance

Information Barriers

A way to restrict communciations between certain groups/departments. It is suppoted in Teams, SharePoint Online, OneDrive for Business.

Examples are: Education (students in one school can't look up details for another), Legal (confidentiality of data obtained by lawyer of one client accessed by lawyer from same firm representing a different client), Profesional services (group of people in company only able to chat with a client or specific customer)