Microsoft 365 Insider Risk Management by VENZO

01

Microsoft 365
Insider Risk Management

Manage risks posed by insiders through Insider Risk Management

Our approach enables you to effectively manage risks stemming from the behavior of you employees and other insiders. We help you configure and adopt the insider risk management solution and policies that make your organization capable of detecting, investigating and controlling insider risks.

Microsoft 365 Insider Risk Management by VENZO_

Detect Risky User Activity

VENZO leverages Microsoft 365 Insider Risk Management to enable your organization to detect risky user behavior such as data theft and data leak by insiders.

Insider risk management policies are configured to detect risky behavior undertaken by employees. Employees can be specified as high-risk based on a triggering event, e.g., dismissal or if they are high-priority users, e.g., they have access to critical information assets.

Compliant Communication

Communication between employees and certain groups of employees might pose risks and violate compliance requirements. VENZO assists you in configuring an effective solutions for managing communication risks.

Communication compliance monitors communication for inappropriate content, sensitive information, possible compliance breaches, and information barriers restrict defined employee groups from communicating with each other.

Investigate and Act

Effectively managing insiders' risky behavior is important to prevent harmful consequences. This is possible through the integrated solutions for investigating and acting on insider risks.

Potential violations of policies are raised as alerts for your compliance team to triage and investigate. If investigation of user activity reveals inappropriate behavior, actions can be taken by notifying the user or escalating the case for further review and actions.

Educate Employees

Equally important to the technical implementation of protection features is educating employees to avoid inappropriate behavior and communication as well as creating a culture of compliance.

VENZO provides your organization with educational resources you can use to drive adoption and foster a culture that proactively prevent risks.

VENZO will train owners, administrators, and reviewers to successfully service and operate the implemented solution.

02

Microsoft 365 Insider Risk Management – Presentation

How can you leverage Microsoft 365 Insider Risk Management to manage risk, achieve compliance, and protect information?

Our Approach

Our end-to-end approach to Insider Risk Management supports your organization on the entire journey from identifying the relevant compliance requirements, operationalizing these for solution configurations and educating users, admins, and reviewers to drive adoption.

Identifying Requirements

- Through workshops we work closely with relevant stakeholders in your organization to identify requirements for insider risk management such as regulatory compliance obligations and company policies.
- We thoroughly document the requirements for operationalization.

Configuring the Solution

- We collaborate with you to transform the identified requirements to operational insider risk management policies and configure the solution in close collaboration with internal owners to ensure knowledge and ownership.
- We test the solution in your environment to confirm that it works as intended.

Driving Adoption

- We equip your organization with dedicated materials to drive adoption of the solution and educate relevant users on how to leverage the solution.
- We support your organization to educate your employees on appropriate behavior and communication to proactively prevent insider risks from materializing.

Preparing for Operation

- We train your solution owners, admins, and case reviewers to operate the insider risk management functions.
- Owners and admins will be able to continuously monitor and configure the solutions in light of changed requirements.
- Case reviewers will be able to use the functions to investigate risky behavior and take action.

Identifying Requirements

The first part of the process we identify the relevant requirements related to insider risks for your organizations. The requirements might have their source in regulatory obligations or company policy. We conduct workshops with the relevant stakeholders such as the compliance department or legal affairs.

The identification of requirements is the essential first step towards compliance and managing insider risks.

Identifying Requirements

Identification workshops

- Conduct workshops with key stakeholders to identify relevant requirements for insider risk management.
- Conduct workshops to understand business needs for insider risk management and get input for configuration.
- Identify owner, admins and case reviewers to plan the insider risk management operating procedures.

Operationalize requirements

- Turning the identified requirements and business needs into operational specifications to be used as configurations in the insider risk management policies.
- Defining operating procedures for insider risk management and inviting identified stakeholders to participate in the process to ensure ownership and adoption.

Configuring the Solution

When requirements have been identified and operationalized, the next step is to technically configure the solution through insider risk management policies, information barriers, and communication compliance policies.

In collaboration with stakeholders in your organization VENZO plans the configuration, how it is to be performed, and how testing will be undertaken.

Configuring the Solution

Configuration

- Operationalized requirements are translated into usable configuration.
- Insider risk management policies, communication compliance, and information barriers are configured in the administration center.
- The configuration is conducted in collaboration with stakeholders to transfer knowledge of the solution.

Operationalize requirements

- Turning the identified requirements and business needs into operational specifications to be used as configurations in the insider risk management policies.
- Defining operating procedures for insider risk management and inviting identified stakeholders to participate in the process to ensure ownership and adoption.

Driving Adoption

Identification of requirements and configuration of the solution is the first part of a successful implementation. The second and crucial part is to drive adoption and preparing for operation.

Effective adoption is supported by insightful material that helps to educate employees, users, and admins on how to use the insider risk management solution and on appropriate behavior to proactively prevent insider risks from materializing.

Driving Adoption

Adopting the Solution

- Dedicated educational material informs your employees and users about the solution and how to properly interact with it with the aim of driving adoption.
- Adoption initiatives give users an understanding of the impact of the insider risk management and communication compliance solution as well as how it impact their ways of working.

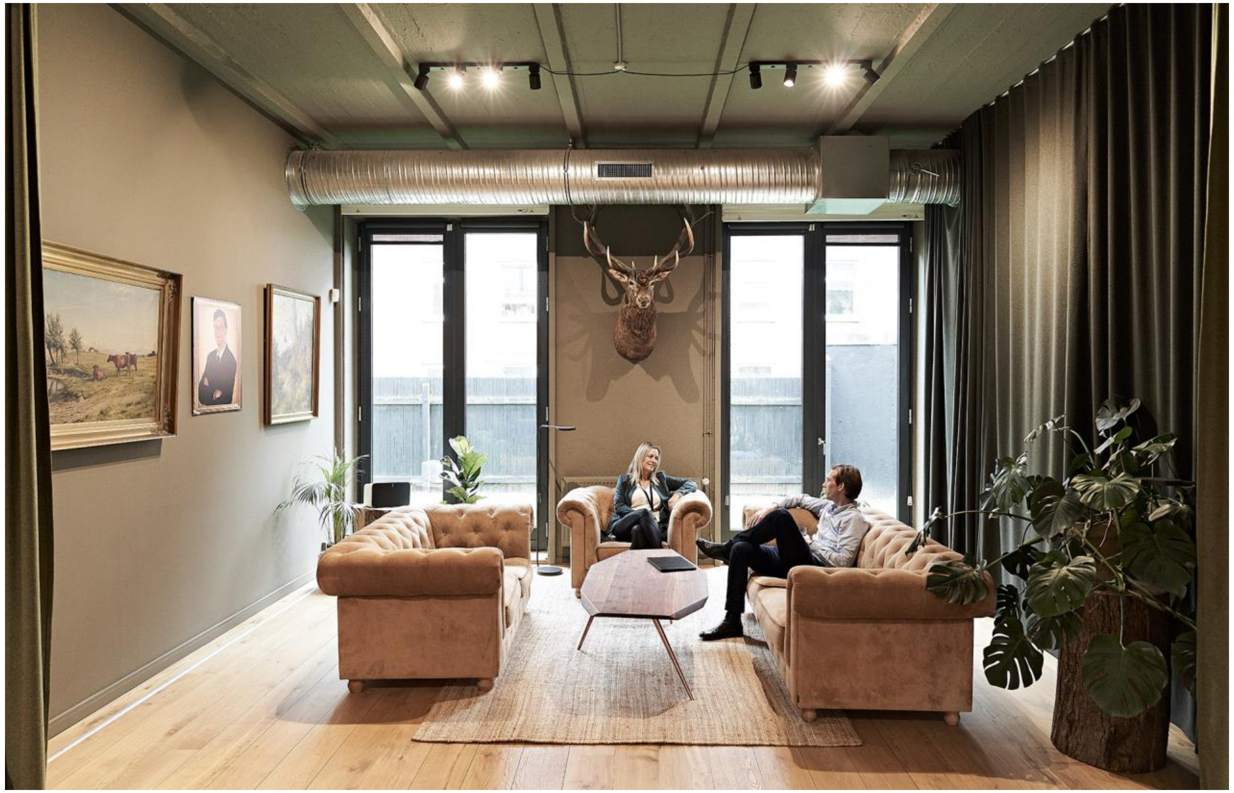
Informing to Prevent Risks

- In line with informing users of the impact of the solution, employees are educated on appropriate behavior as insiders and on compliant communication.
- Educating users aims to proactively prevent insider risks by seeking to avoid risky behavior and non-compliant communication.

Preparing for Operation

Preparing your organization and appointed operators for operation is the last crucial step ensuring that the solution lives, and that insider risks are effectively managed to protect your organization.

VENZO produces material, procedures, and training for employees. Owners and admins are trained on how to service the solution. Case handlers are trained to investigate and act on behavior posing insider risks.



Preparing for Operation

Servicing the Solution

- Owners and administrators of the insider risk management solution are provided training and procedures on how to service the solution.
- Training on monitoring of the solution and how it’s functioning.
- Training on configuring the solution and changing configurations in light of changing requirements.

Operating the Solution

- Insider risk management and communication compliance reviewers are trained in operating the solution.
- Training in monitoring risky user behavior through reports and alerts.
- Training in using the investigation functions.
- Training in using the functions for taking further action if warranted by investigation.

02

Create value through Risk Management and Compliance

Insider Risk Management and Compliance

Implementing insider risk management and communication compliance solution provides value to your organization by enabling you to better and more efficiently manage risks, achieving compliance, and protecting your valuable information.

Create Value with Risk Management and Compliance

Efficiently Manage Your Risks

The insider risk management solution strengthens your objective of efficient managing risks by providing a technical solution for detecting risky behavior and preventing adverse effects from risks materializing.

The monitoring implemented through insider risk management policies detects and flags potential harmful actions and enables taking action to remediate risks. Communication compliance policies can identify and prevent inappropriate communication between employees.

Support Your Compliance Efforts

Compliance is a major objective for organization in order to prevent breaches of regulatory obligations. Insider risk management and communication compliance gives your organization the tools to achieving compliance.

Preventing conflict of interest and misuse of insider information are regulatory requirements for many organizations. The solution helps you prevent these by detecting inappropriate communication and creating information barriers between groups of users.

Create Value with Risk management and Compliance

Protect Your Valuable Information

Information is among the most valuable assets for organizations. Therefore, resources applied to protect it should be optimized. Insider risk management is an important complementary function to protect information from illegal, inappropriate, unauthorized, or unethical behavior and actions by users in your organization.

Insider risk management policies protect information by detecting issues such as leaks of sensitive data and theft of intellectual property (IP).

Creating a Culture of Compliance

Technical solutions are important for detecting and acting on insider risks and incompliant communication, but equally important is creating a culture of compliance and appropriate behavior.

By complementing technical implementation with adoption driving efforts and educating users on appropriate behavior and communication, the risks can be proactively prevented.

Thank you.

We are looking forward to next meeting!

For questions about our services or approach, please reach out to hello@venzo.com or your Microsoft Account Manager.

VEN
ZO_