Microsoft Purview

Communication Compliance

01

Introduction to Communication Compliance

Definition and Purpose

Understanding Communication Compliance

- Refers to the adherence to laws, regulations, and organizational policies governing communication practices
- Ensures that all communications are legitimate, ethical, and secure
- Includes the ability to manage sensitive info (using an alternative method) and protect against harassing, threatening, or inappropriate language used in communications.

Importance in Organizations

Effective communication compliance is crucial for organizations to mitigate legal risks, maintain trust, and uphold a positive reputation. It is essential for safeguarding sensitive information and ensuring regulatory adherence.

Key Components of Compliance

Policies and Regulations

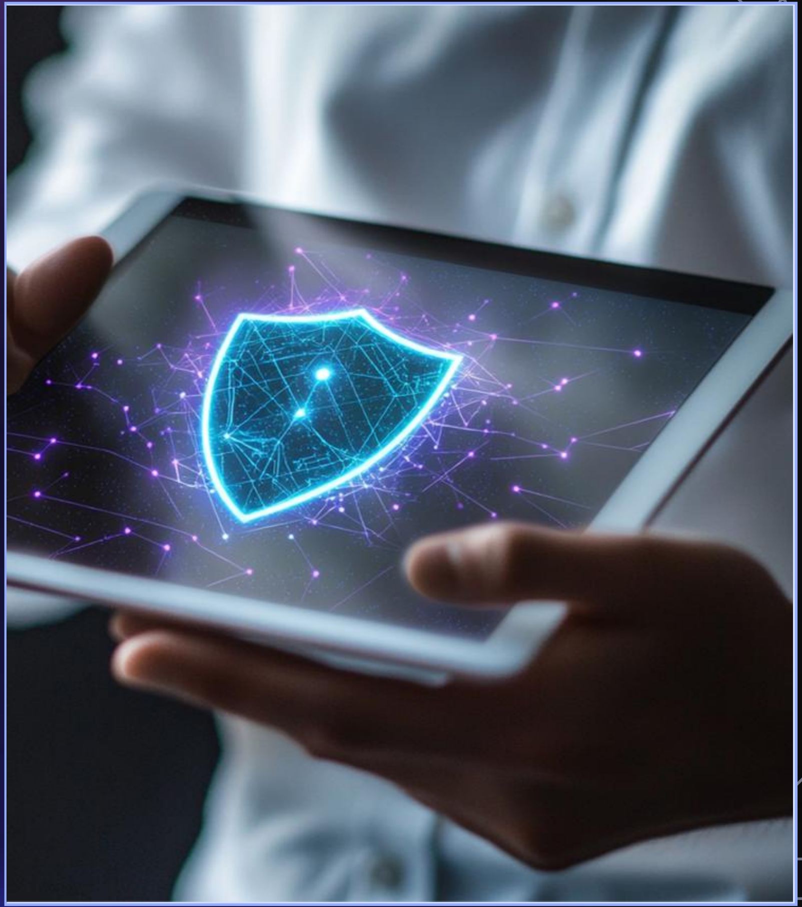
Policies and regulations provide a framework for communication practices within organizations, setting standards that employees must follow to maintain compliance with legal and ethical norms.

Risk Management Strategies

Effective risk management strategies involve identifying potential communication risks and implementing measures to minimize their impact, safeguarding the organization’s interests and compliance standing.

02

Communication Monitoring Strategies



Policy Creation Process

Identifying Compliance Needs

In this stage, organizations assess regulatory requirements and internal standards to determine specific communication compliance needs that must be addressed in policy formulation.

What is considered threatening, etc.?
Is there a built-in policy or do we need to build something specific to our organization?

Drafting Policies

This step involves creating clear and comprehensive policies that articulate compliance requirements, outlining procedures, responsibilities, and consequences for violations to ensure understanding and adherence.

As previously discussed, Purview provides a way to centrally codify and enforce those policy definitions.

Implementing Policies in Microsoft Purview

Configuring Settings

Here, the focus is on setting up the necessary configurations within Microsoft Purview to align technical settings with the established compliance policies, ensuring they are actively enforced.

The who, the what, the how…

Training Staff and Stakeholders

This component emphasizes the importance of conducting training sessions for employees and relevant stakeholders, fostering awareness and understanding of compliance policies and their implications in daily operations.

Yet another dimension to governance, risk, and compliance.

Techniques for Effective Monitoring

- **Automated Alerts and Reporting**

  Automated alerts and reporting systems enhance monitoring efficiency by providing “real-time” notifications about communication anomalies, thereby facilitating prompt intervention and management of potential issues.

- **Manual Review Processes**

  Manual review processes involve a systematic examination of communications by human analysts, ensuring nuanced understanding and the ability to assess context, tone, and intention behind messages.

Analyzing Communication Patterns

Identifying Risks and Violations

Identifying risks and violations involves scrutinizing communication patterns for compliance breaches or inappropriate behavior, which is essential for maintaining organizational integrity and regulatory adherence.

▶ PART 01

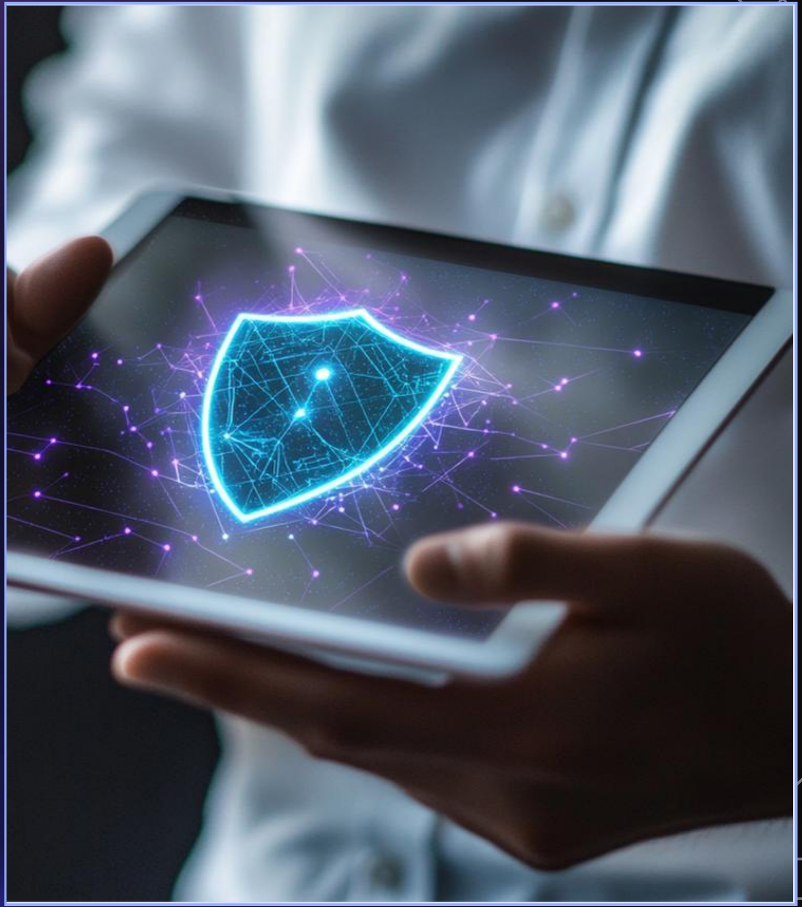
Leveraging AI and Machine Learning

Leveraging AI and machine learning technologies allows organizations to analyze vast amounts of communication data efficiently, uncovering trends, and improving the accuracy of risk assessments through predictive analytics.

▶ PART 02

03

Monitoring & Investigating Policy Matches



Definition of Policy Matches

Types of Policies

Policy matches can include regulatory policies, internal corporate policies, or compliance policies, each serving distinct purposes in governance and operational frameworks.

Criteria for Matches

Criteria for policy matches involve alignment with legal requirements, consistency with organizational objectives, and coherence with best practices to ensure effective implementation.

Functionality of Policy Matches in Purview

01

Automated Policy Matching

Automated policy matching employs algorithms to identify and apply relevant policies quickly, enhancing efficiency and reducing human error in the compliance process.

02

Manual Policy Review Process

The manual policy review process involves systematic evaluation by stakeholders to ensure policies are appropriately matched and adhered to, fostering accountability and thorough oversight.

Tools for Investigation of Policy Matches

01

Dashboard Overview

The dashboard provides a comprehensive visual representation of data, allowing users to monitor key performance indicators and assess policy adherence efficiently.

02

Analytics and Reporting Tools

These tools facilitate data analysis through various metrics and generate reports, enabling organizations to identify trends, anomalies, and areas for improvement in policy implementation.

Process of Investigation

Steps in the Investigation

The investigation process involves several systematic steps, including initial data collection, analysis, verification of findings, and documentation for transparency and accountability.

Role of Compliance Officers

Compliance officers play a crucial role by ensuring that all investigations are conducted fairly and in alignment with legal standards, while also providing guidance on regulatory requirements.

Regular Review Processes

Frequency of Reviews

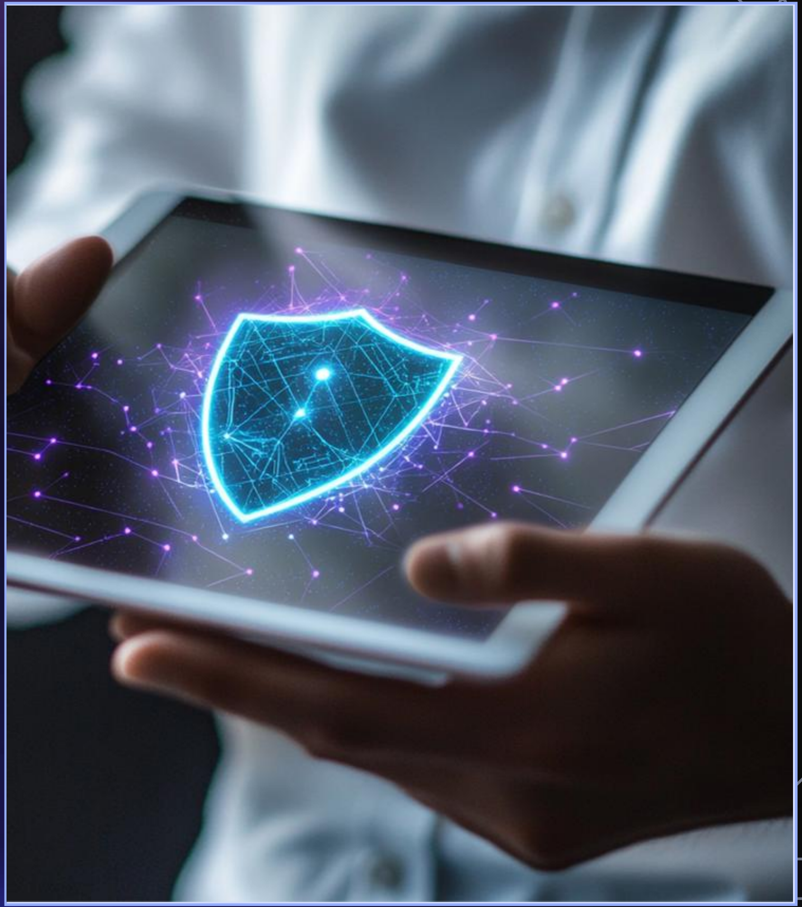
Establishing a consistent frequency for reviews, whether weekly, monthly, or quarterly, helps maintain oversight and fosters an environment of continual assessment and improvement.

Documentation and Record Keeping

Proper documentation and record keeping are essential for tracking the outcomes of monitoring activities. This practice facilitates accountability and provides valuable historical data for future reference.

04

Role of Reviewers in Communication Compliance



Responsibilities of Reviewers

Data Assessment

Reviewers are tasked with evaluating the quality and integrity of data (communications) and its alignment with established communication compliance policies, ensuring that it meets organizational standards and compliance requirements.

Risk Evaluation

Reviewers analyze potential risks associated with specific types of communication, identifying vulnerabilities that could impact data security and regulatory compliance.

Types of Reviewers

Internal Reviewers

Internal reviewers are employees within the organization responsible for conducting regular assessments of data management practices and adherence to company policies.

01

External Stakeholders

External stakeholders include third-party auditors and consultants who provide an independent review of data practices, ensuring objectivity and compliance with industry regulations. In the case of harassing communications, for example, there may be external legal impacts.

02

Assigning Reviewers

Criteria for Selection

The selection criteria for reviewers should encompass relevant experience, subject matter expertise, and the ability to provide constructive feedback, ensuring a comprehensive review process.

Role Permissions

Defining role permissions is essential for safeguarding the review process, allowing specific access levels for reviewers to edit, comment, or approve submissions based on their designated roles.

Definition of Escalations

Reasons for Escalation

Escalation occurs when issues cannot be resolved at the current level of authority, necessitating intervention from higher management to ensure timely resolution.

Types of Escalations

Escalations can be categorized into operational, strategic, and financial types, each addressing different aspects of an organization’s performance and decision- making processes.

Escalation Pathways

01

Standard Operating Procedures

Standard Operating Procedures (SOPs) outline the step-by-step processes for managing escalations, ensuring consistency and clarity in response across the organization.

02

Communication Channels

Effective communication channels are vital during escalations, providing clear paths for information exchange, updates, and feedback among involved parties and management.

05

Challenges in Communication Compliance

Common Challenges in Compliance

Data Privacy Concerns

Data privacy concerns arise from the need to protect sensitive information while ensuring compliance with regulations, leading to potential legal risks for organizations.

Ensuring Employee Awareness

Ensuring employee awareness is crucial, as many employees may not fully understand compliance requirements, which can lead to unintentional violations and increased organizational risk.

Common Compliance Issues

Misinterpretation of Policies

Misinterpretation of policies often arises from unclear language or ambiguous guidelines, leading to inconsistent application of compliance measures across the organization.

Inconsistent Monitoring

Inconsistent monitoring can result from a lack of standardized procedures or insufficient resources, allowing compliance breaches to go unnoticed and unaddressed.

Organizational Resistance

01

Change Management Issues

Implementing new compliance measures often encounters resistance from employees accustomed to existing processes, hindering organizational adaptability and creating friction in communication efforts.

02

Overcoming Resistance to Compliance

Addressing and mitigating the reluctance among staff to embrace compliance initiatives requires effective leadership, transparent communication, and ongoing training to foster a culture of compliance.

Maintaining Updated Policies

01

Keeping Up with Regulatory Changes

Organizations must continuously monitor and adapt to evolving regulations, which can be a daunting task that strains resources and complicates compliance communication efforts.

02

Addressing Emerging Threats

Proactively identifying and responding to new threats in the compliance landscape is essential, as failure to do so can lead to significant vulnerabilities and communication breakdowns in compliance strategies.

Mitigation Strategies

Training and Resources

Providing comprehensive training and readily available resources ensures that employees fully understand compliance requirements and can apply them effectively in their roles.

Engaging Stakeholders

Engaging stakeholders fosters a collaborative environment where all parties contribute to compliance efforts, enhancing accountability and adherence to established communication protocols.

Thanks