6 Tips to Get Started with Compliance in Microsoft 365

Microsoft provides a host of tools for managing risks, governing sensitive data, and maintaining regulatory compliance. When properly set up, the Microsoft Purview compliance portal provides powerful insights and solutions. The tips in this article will help your organization get the most out of and get started with compliance in Microsoft 365.

1. Know Your Starting Point

To outline a roadmap for achieving compliance, you first need to determine the current state of compliance in the organization. Conducting a proactive compliance audit can provide a starting point by highlighting risks and identifying areas for improvement.

Additionally, the Microsoft Purview Compliance Manager helps by providing a centralized dashboard that tracks risk level and measures progress on compliance tasks.

2. Get Expert Advice with Guided Setup for Purview

Microsoft offers setup guides to help organizations configure Microsoft 365 productivity tools and security policies and set up device management. The library of setup guides now includes a guide specific to the Microsoft Purview Compliance Manager.

To access the Compliance Manager setup guide, go to the Microsoft 365 Admin Center. Then, on the Setup card or the Training & Guides card, select Advanced Deployment Guides and filter by security and

compliance. In addition to guided steps, the guide includes product information, links to related Microsoft documents and access links for premium assessment templates.

3. Configure Alerts for Potential Compliance Issues

The Compliance Manager dashboard displays a summary of active alerts. By default, Microsoft includes built-in alert policies for malware activity, possible admin permissions abuse, data lifecycle management problems and potential threats. Additionally, you can define custom alerts specific to your organization.

Alerts can be applied to actions by all users or by a list of specific users. And you can indicate how many times an action has to occur before it triggers the alert. For example, you might set an alert to trigger after a user tries to delete more than a certain number of files in 30 minutes. Another alert might trigger when anyone tries to share files from a specified folder externally.

4. Protect Critical Data with Sensitivity Labels

A key aspect of Microsoft 365 compliance allows the organization to apply sensitivity labels to protected data. Administrators can then create policies to monitor and govern that data. For instance, by applying a sensitivity label to protected health information, the organization can ensure against improper sharing or deletion.

Data users and administrators can apply sensitivity labels manually when necessary. Additionally, the system can automatically tag data by identifying patterns such as credit card numbers or keywords. Further, by using machine learning, the system can learn to identify and tag certain types of content based on examples the organization provides.

5. Define Retention Policies

Microsoft 365 promotes compliance by allowing organizations to define retention at both the file level and the folder level. For example, the organization can apply retention labels to specific documents or emails, regardless of where they travel. Then, if a user edits or deletes protected content, the system automatically retains a copy of the content.

The organization can also apply retention policies to an entire folder. In this case, the policy applies to everything within that folder.

6. Cover Security Basics for Remote Work

Regulatory compliance of necessity includes many aspects of data security. Companies must demonstrate adherence to best practices around information access, data loss prevention and threat protection. For companies that include remote work, some essential security tasks include the following:

- Enable multi-factor authentication (MFA)
- Deploy endpoint detection and response
- Implement a zero-trust approach to network security
- Upgrade end user security awareness training programs
- Set up 24/7 threat monitoring
- Review patch management policies to ensure timely installation of security patches

Get Started with Compliance in Microsoft 365

It's sometimes difficult for organizations to get started with compliance. Take a proactive approach to compliance and data governance by joining forces with Messaging Architects. With a detailed understanding of the controls and options available, we will help you take compliance to the next level.