

Microsoft 365 Governance Tips to Balance Productivity, Control, and Security



For millions of users worldwide, Microsoft 365 powers collaboration and supports workloads in the cloud. Its ever-evolving technology drives productivity and creates opportunities. At the same time, increasing complexity requires [effective Microsoft 365 governance](#). Hence, our Microsoft 365 Governance tips to balance productivity, control, and security.

Plan for Governance Success

The [Goldilocks zone](#) of good governance looks different for each organization. Ideally, Microsoft 365 assists companies with solving business problems and meeting organizational objectives. To that end, administrators need to take a proactive approach to designing and implementing an information governance strategy.

First and foremost, this will involve clarifying business needs and goals and then building a governance plan around those goals. Additionally, organizations need to understand applicable regulations and gain an understanding of existing security and compliance risks.

Organizations should also understand that eGovernance in Microsoft Cloud is dependent on licensing levels. For example, the features set available vary between the different licensing packages.

Define Retention, Email, and Data Security Policies

A key tool for governing information to reach business goals and achieve compliance involves policies. In the case of data retention, for instance, Microsoft 365 Records Management allows organizations to define data retention at both the folder level and the file level.

For example, administrators can create a retention policy to apply to all items in a SharePoint site or all messages on a channel. On a more granular level, they can apply retention labels to specific items, such as single documents or emails. Likewise, [email policies](#) discourage data pack rats and streamline eDiscovery.

Policies also provide protections for sensitive data. For instance, the organization can create policies to ensure that users do not accidentally share financial data or personally identifiable information.



Balance Productivity with Control and Security

In addition to increasingly complex tools, administrators must balance the need for productivity with a constantly evolving threat landscape and regulatory pressures. Microsoft 365 governance allows administrators to strictly control user access and automate policies for data sharing and retention.

These controls aid security and compliance. However, too much structure can lead to reduced productivity when users must deal with multiple logins and strict controls over sharing. This frustration may spark a rise in shadow IT as employees find ways to collaborate outside the approved applications.

Likewise, retention policies help to ensure regulatory compliance and protect vital information assets. But retaining too much data eats up storage space and creates chaos. Effective governance finds a sweet spot that protects the organization while driving efficiency.

Back Up Critical Business Data

Microsoft 365 includes a host of tools for collaboration, which store data in a variety of locations. For instance, users keep and share documents through SharePoint and OneDrive. Outlook mailboxes contain thousands of emails and appointments. And Teams stores chats and voicemails for future reference.

Microsoft 365 enables administrators to implement retention and destruction policies on specific data or locations. However, data not governed by such policies is subject to manual destruction and Microsoft does not maintain backups of data.

Therefore, organizations should look to third party backup solutions and determine how much of this data requires backup and how often to run backups. This varies, depending on business needs, industry regulations and applicable legislation, such as HIPAA. [Data archive solutions](#) should also be considered to provide long term compliance options.



Preserve Data Organization and Configuration

If businesses simply back up the data, without consideration for the way the data is organized, restoring from the backup would cause chaos. For instance, users often depend on a system of folders and subfolders in SharePoint to group like documents together and make them easy to locate. Backups should take that organization into account to allow for seamless restoration.

2015 | 2013 | 2012 Microsoft
Partner of the Year



Inc. 500 || 5000
2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010



ShoreTel Sky
Partner of the Year

When backups also include configuration settings, it further eases the process of restoration. This is particularly true in the case an organization needs to rebuild much of the system after a ransomware attack. Configuration includes access management settings, library settings, sharing permissions and so forth.

Get More Microsoft 365 Governance Tips

Microsoft 365 offers powerful tools to empower collaboration, protect data assets, and support innovation. But powerful tools require fine-tuning and careful management. Understanding and properly configuring the options available requires training and experience.

The [information governance consultants](#) at eGovernance bring extensive experience in Microsoft 365. Along with powerful [archiving, eDiscovery and Compliance solutions](#), they provide the Microsoft 365 governance tips and expertise organizations crave for success.

2015 | 2013 | 2012 Microsoft
Partner of the Year



Inc. 500 ||| **5000**
2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010



ShoreTel Sky
Partner of the Year