

CoreView's Microsoft 365 Governance

BEST PRACTICES GUIDE



Executive summary

With Microsoft 365 housing so much sensitive data, governance has never been so important. Despite this, the data shows that M365 customers are overwhelmed with the task and struggling with the basics.

To turn the tide on governance, M365 customers must address two critical questions:

- 1 What are governance best practices for Microsoft 365?
- 2 What constitutes a best practice governance policy for Microsoft 365?

In defining governance best practices, Microsoft 365 customers should seek to establish mature processes for each of the 5 stages of the governance lifecycle—discovery, policy selection and implementation, policy violation detection, remediation, and reporting.

M365 organizations should not let the daunting task of writing a comprehensive companywide M365 governance framework bottleneck their initiative.

To avoid this from happening, it's wise to adopt a best practice M365 governance framework that addresses the biggest security, compliance, and operational risks that most M365 organizations face, and work outwards from there.

This guide lays out over **30 GOVERNANCE BEST PRACTICES** all organizations should implement across:



Security



License management



Identity



SharePoint & OneDrive



Teams governance



Exchange

Table of contents

01 Introduction

02 Security and identity

03 Microsoft Teams management

04 Microsoft 365 license management

05 SharePoint and OneDrive management

06 Exchange management

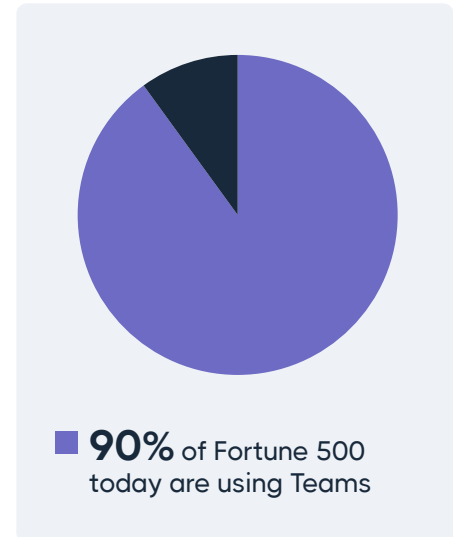
07 Conclusion

Introduction

Microsoft by the numbers

As we enter 2024, Microsoft's cloud organization continues to boom:

- Microsoft revenue has grown from \$93.6B in 2015 to more than \$211B in 2023.¹
- There are 345M M365 seats and 550M Entra ID users worldwide.²
- 90% of Fortune 500 today are using Teams.³
- There are over 300+ million monthly Teams users.⁴
- Over 200PBs are added to SharePoint monthly.⁵



With these levels of adoption, it's safe to say that Microsoft is probably powering almost all work that's happening in 2024. In fact, organizations are so reliant on M365 that an hour's downtime could cost a whopping 7 figures.⁶

This reliance on M365 has turned it into a goldmine of sensitive data. Research shows that 365 customers house 58% of their sensitive cloud data in Office 365 documents, highlighting the importance of robust security and governance.⁷

Despite this, the task of getting oversight and control of M365 is incredibly hard. The sheer scale of what Microsoft offers—18 admin portals, 40 data silos, and hundreds of APIs—makes the task at best an operational nightmare. At worst, unified control and governance is almost impossible.

Because of this complexity, organizations are struggling with the basics. Research shows that an astonishing 36% of all M365 admins are using Global Admin rights, 50% are not covered by default security policies, and 57% of admins have excessive permissions.⁸

Sources: ¹ [Microsoft Annual Report](#), 2015, [Microsoft Annual Report](#), 2023. ² [Microsoft Earnings Release FY22 Q3](#), 2022. ³ Morgan Stanley Research, CIO Survey Takeaways - Further Solidifying the Leadership Position, 2021. ⁴ [Microsoft Fiscal Year 2024 First Quarter Earnings Conference Call](#), 2023. ⁵ [SharePoint in the AI Era: Introducing Copilot in SharePoint & 10 more innovations for creators](#), 2023. ⁶ Gartner, [How to Mitigate the Impact of Microsoft 365 Downtime](#), 2021. ⁷ Gartner, [How to Protect Sensitive Data in Office 365 Using Microsoft Native Controls](#), 2021. ⁸ CoreView, [M365 Application Security, Data Governance and Shadow IT Report](#), 2021

For teams looking to turn the tide on M365 governance, it can be overwhelming to know how and where to start. That's where this guide comes in.

After 20+ years of working with M365 governance, the CoreView team has nearly seen it all. With this experience, we've learned what it takes to deliver best practice governance for M365. This guide distills our extensive exposure into over 50 best practices to use as a baseline for building your governance protocols and frameworks.

By establishing governance mechanisms, organizations can ensure that internal and external regulations are adhered to, mitigating the risk of compliance violations.

Implementing a full Microsoft governance lifecycle

For organizations trying to turn the tide on M365 governance, it's not enough to know what needs to be governed. It's also critical to work out the best practice process for how to govern it.

From our experience there are five steps to effectively maintaining governance within M365:



1. Discovery

You cannot manage what you cannot see, and for M365, the issue of visibility is critical. Although the 18 admin portals across M365 can provide you with the information you need, it's critical the organization establishes processes or tooling to automate the ongoing centralizing of this data into a single UI or report that gives you full visibility of policy across M365.

2. Policy Selection & Implementation

With visibility established, you are now ready to start the journey to security and governance enforcement in M365, and to achieve this, we must determine what policies you will enforce. In modern organizations this can be a mammoth task requiring consolidation of multiple internal and external security, compliance, and IT operations standards. This task so enormous that it can bottleneck a sincere initiative to get started with M365 Governance. Because of this, it's highly recommended that organizations that lack an existing M365 Governance Policy utilize a set of best practices, such as the ones that are contained in this guide.

3. Identify Policy Violations

Now it's time to identify policy violations. This can be an excruciating and error prone effort when undertaken manually. Therefore, it is highly recommended that organizations invest in tooling to assist with the policy violation detection process.

4. Remediation

With policy violations identified, it's now time to start remediation. Once again, this task can introduce large workloads and errors when performed manually. By leveraging automated tooling, M365 organizations will stay productive and make the M365 governance and security practical.

5. Reporting

Once the organization has successfully remediated all issues, they are ready to report on their success to the relevant internal and external stakeholders.

As should be abundantly clear, the M365 governance lifecycle is an extremely time intensive process that is impractical without proper tooling and automation. None of this is to mention the reality that the ongoing adoption of M365 services and onboarding of new users creates more and governance and security concerns that require organizations to repeat the lifecycle as often as they can, further highlighting the need for M365 governance automation to ensure best practice.

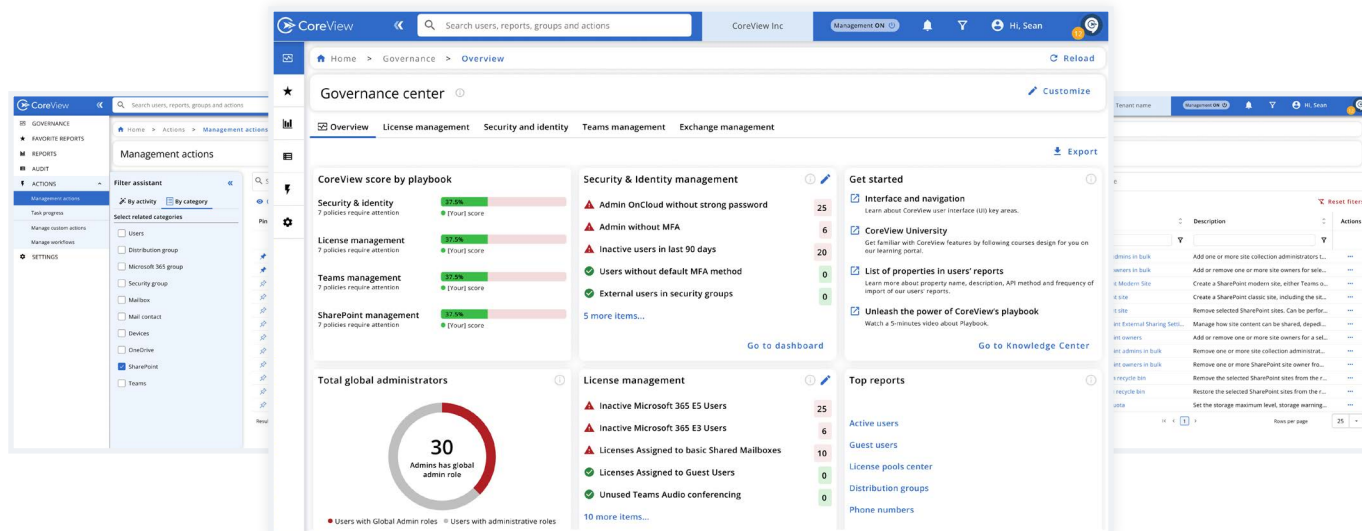
Defining best practices for Microsoft 365 governance

As mentioned in the previous section, M365 governance initiatives often slow dramatically when organizations are required to write up their own M365 governance standards. The task of working out exactly what M365 governance will mean for any organization is a highly personal journey, but this shouldn't stop all M365 customers from making a commonsense start.

That is what the rest of this guide is dedicated to.

From here our team of experts will talk you through five critical focus areas for M365 governance with detailed explanations of the biggest security, compliance, and operational issues every M365 customer should prioritize.

In the conclusion section you will find information on how to find out more about CoreView's automated M365 governance capabilities.



Security and identity

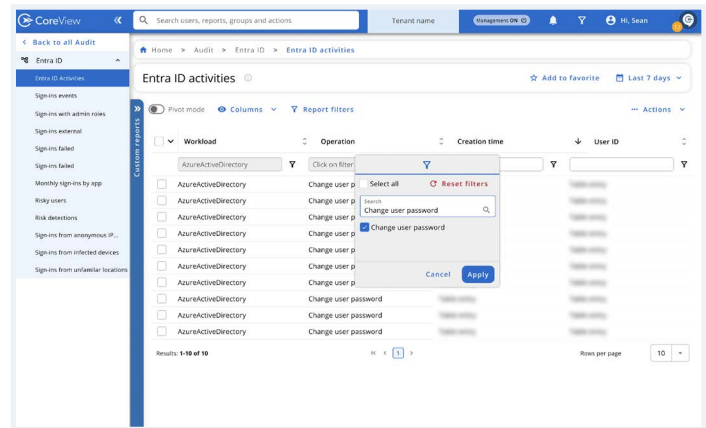
Security and identity best practices

It's clear that Security and Identity Management is crucial in the vast ecosystem of Microsoft 365. These best practices aren't just suggestions, they're essential for your immediate implementation to bolster your security and streamline identity management.

Moreover, each best practice comes packed with specific action items for ongoing remediation. Use these as building blocks for your PowerShell scripts or for optimizing your Microsoft 365 management solution.

Best practice #1: Enable multi-factor authentication (MFA) for all users

Microsoft 365's conditional access policy allows for custom MFA requirements under specific conditions. However, unconfigured default MFA methods leave organizations vulnerable. If a hacker gains access to a user's credentials and sets the MFA method, they obtain unauthorized access to Microsoft 365.



One of the most effective ways to secure your data is by implementing multi-factor authentication (MFA) for all users. MFA provides an additional layer of protection beyond the traditional username and password by requiring the user to provide a second form of verification, such as a fingerprint, facial recognition, or a one-time code sent via text message.

By implementing MFA for all users, organizations can protect sensitive information, prevent account takeovers, increase security for cloud-based services, meet regulatory requirements, and provide a simple and effective solution for enhancing security.

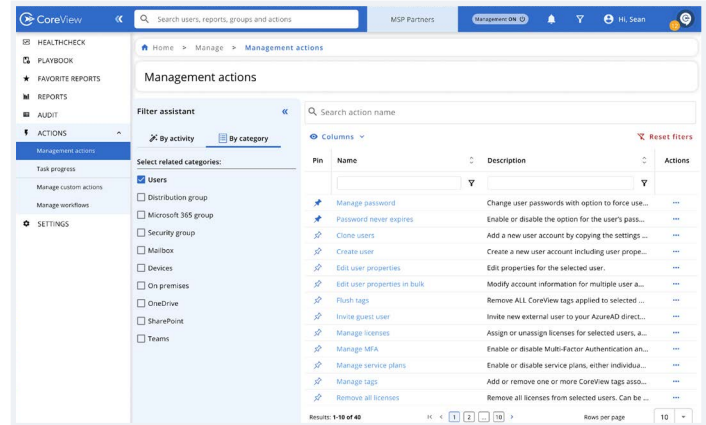
➔ ACTION PLAN:

- ☐ Run regular audits by generating a report that identifies users, including other M365 admins, without multi-factor authentication enabled.
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft admin responsible for MFA if the workflow fails.

Best practice #2: Ensure cloud administrators use strong passwords

Admin accounts with cloud identities in Microsoft 365 must be managed meticulously. Strong passwords are vital as administrators have access to sensitive information and control over crucial settings and configurations.

Weak passwords put this information at risk of compromise. Microsoft 365 admin accounts with cloud identities are entirely managed in the cloud, meaning on-premises identity policies are not applied to these admins, potentially increasing the risk of unauthorized access or a breach.



A compromised cloud identity admin account can lead to a significant security breach, as the attacker would have access to sensitive information and control over essential settings and configurations. In some cases, regulations may require additional security measures for cloud-based admin accounts, such as two-factor authentication or monitoring of administrative activity.

→ ACTION PLAN:

- ☐ Regularly run audits to identify admin accounts with weak passwords.
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft admin responsible for password security if the workflow fails.



[CoreView's] authorization model is easily manageable but allows at the same time a great granularity of the permissions assigned to a user."



– IT Manager, Retail | [Read full review here](#)

Best practice #3: Block credentials of users inactive after 60 days

Inactive user accounts with unblocked credentials pose a significant security risk to your Microsoft 365 environment. These accounts may still have access to sensitive information such as data and emails. If compromised, they could lead to data breaches, unauthorized access, and potential compliance violations.

By reducing the number of active user accounts, you decrease your system's attack surface, providing fewer opportunities for attackers. Blocking credentials of inactive users after 60 days minimizes the risk of security breaches and better protects your sensitive information.

→ ACTION PLAN:

- ☐ Set a time-out period for the inactive users (minimum: 1 day, maximum: 180 days).
- ☐ Regularly run audits to identify user accounts that have been inactive for more than 60 days.
- ☐ Upon identifying inactive users, send an attestation to the manager or a custom address, with the option to include an additional message.
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft admin responsible for user activity monitoring if the workflow fails.



[We] adopted CoreView due to its features for license assignment and O365 control without actual assigning of permission in O365 portal.”

– Senior MIS Engineer, Telecommunications | [Read full review here](#)

Best practice #4: Remove inactive guests after 90 Days

While no specific regulation mandates the removal of inactive external users, it is considered a best practice for security and privacy reasons. Cybersecurity standards, such as ISO 27001 and NIST SP 800-53, recommend regular reviews and removal of inactive user accounts to minimize the risk of unauthorized access and potential data breaches. Implementing access control and maintaining an accurate inventory of system users are also emphasized in these standards.

→ ACTION PLAN:

- ☐ Set a policy to identify and remove guest users who have been inactive for more than 90 days.
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft admin responsible for guest user activity monitoring if the workflow fails.

Best practice #5: Admin passwords should be changed every 90 days

While there are no specific regulations that mandate changing admin passwords on a regular basis, security guidelines from various authorities recommend doing so to maintain the security of an organization's information systems.

→ ACTION PLAN:

- ☐ Set a policy to change admin passwords every 90 days.
- ☐ Schedule the password change to recur every 90 days.
- ☐ Send attestation to the manager (or a custom address), with the option to include an additional message.
- ☐ Configure the workflow to alert the Microsoft admin responsible for password management if the workflow fails.

Best practice #6: Regularly review and manage external users in Microsoft 365 group

External users, especially those without proper training and security awareness, can increase the risk of a security breach or unauthorized access to your data. It's crucial to have proper policies and guidelines in place for external users and ensure ongoing monitoring and security training to minimize these risks.

→ ACTION PLAN:

- ☐ Regularly run audits to identify external users in the Microsoft 365 group.
- ☐ Remove external users who are no longer necessary from the Microsoft 365 group.
- ☐ Send attestation to the group owners or a custom address, with the option to include an additional message.
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft admin responsible for Microsoft 365 group management if the workflow fails.

Best practice #7: Regularly review and manage external users in security groups

Just like with Microsoft 365 groups, external users in security groups can pose a risk if not properly managed. Regular monitoring, training, and adequate access control measures need to be in place to minimize risks associated with external users in security groups.

→ ACTION PLAN:

- ☐ Regularly run audits to identify external users in the security groups.
- ☐ Remove external users who are no longer necessary from the security groups.
- ☐ Send attestation to the group owners or a custom address, with the option to include an additional message.
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft admin responsible for security group management if the workflow fails.

Microsoft Teams management

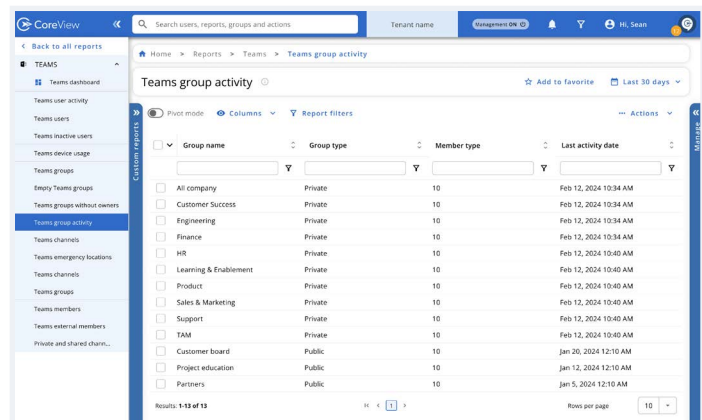
Microsoft Teams management best practices

As the most essential and widely used application in the Microsoft landscape, Teams is where work happens. As a single place for communication and collaboration, you can access SharePoint, OneDrive, and various Office 365 apps from it. With all of that access available to users within Teams, organizations must require that confidential files remain secure and mitigate potential risks both inside and outside the organization.

Here are the must-have best practices for Teams governance. Use them as the foundation for building your governance framework using PowerShell scripts or a Microsoft 365 management platform.

Best practice #1: Archive or remove empty teams groups

While unoccupied Teams pose a lower risk to security, they are still a waste of resources. These Teams should be periodically reviewed. Identifying Teams lacking members and deciding whether it's best to archive them after a period of inactivity can save resources. In some cases, deleting them altogether might be the best course of action.



Group name	Group type	Member type	Last activity date
☐ All company	Private	10	Feb 12, 2024 10:34 AM
☐ Customer Success	Private	10	Feb 12, 2024 10:34 AM
☐ Engineering	Private	10	Feb 12, 2024 10:34 AM
☐ Finance	Private	10	Feb 12, 2024 10:34 AM
☐ HR	Private	10	Feb 12, 2024 10:34 AM
☐ Learning & Enablement	Private	10	Feb 12, 2024 10:34 AM
☐ Product	Private	10	Feb 12, 2024 10:34 AM
☐ Sales & Marketing	Private	10	Feb 12, 2024 10:34 AM
☐ Support	Private	10	Feb 12, 2024 10:34 AM
☐ TAM	Private	10	Feb 12, 2024 10:34 AM
☐ Customer board	Public	10	Jan 20, 2024 12:10 AM
☐ Project education	Public	10	Jan 12, 2024 12:10 AM
☐ Partners	Public	10	Jan 5, 2024 12:10 AM

→ ACTION PLAN:

- ☐ Identify all Teams without members.
- ☐ Archive or remove the empty Teams group.
- ☐ Set a recurring schedule for this remediation action.
- ☐ Configure the workflow to alert the Microsoft Teams admin if the workflow fails.

Best practice #2: Archive or remove inactive teams groups

Project-specific groups in Microsoft Teams can be invaluable for collaboration but consider sunsetting these groups post-project completion. For example, policies could be developed that delete Teams after a certain period of inactivity. When defining what Inactivity means for your organization, consider that it can be action-based and/or time-based.

Organizations may also want to use an automated system for monitoring and managing their inactive Teams. Carefully consider the ramifications of archiving or deleting an inactive Team — retaining a record might offer valuable insights for future reference.

→ ACTION PLAN:

- ☐ Define 'inactivity' and monitor your Teams accordingly.
- ☐ Send an attestation to the appropriate recipient.
- ☐ Archive (or remove) the inactive Teams group.
- ☐ Establish a time-out period (minimum: 1 day, maximum: 180 days).
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft Teams admin if the workflow fails.

Best practice #3: Manage public Teams groups

Organizations using Microsoft Teams can control the number of Public Teams that employees can join. For instance, an attestation process can require Team owners to periodically confirm whether their team's membership is still required.

If there's no response or if a team is no longer in use, it may need to be archived or removed to improve organizational efficiency and security.

→ ACTION PLAN:

- ☐ Set an attestation process requiring confirmation from Team owners on the necessity of their team's membership.
- ☐ Send attestation to the Group Owner or a specified recipient, optionally including an additional message.
- ☐ Archive or remove the Teams group, as per the requirement.
- ☐ Set a time-out period (minimum: 1 day, maximum: 180 days).
- ☐ Schedule the remediation action to recur on a weekly, monthly, or yearly basis.
- ☐ Configure the workflow to alert the Microsoft Teams admin if the workflow fails.

Best practice #4: Regularly review and manage guest users in Teams groups

Inviting external users to be members of a Microsoft Team can enhance collaboration with outside entities. However, guest-user access may give visibility into files and content intended for internal use only. For this reason, organizations should establish a policy that mandates team owners to regularly review whether granted guest-user permissions are necessary.

→ ACTION PLAN:

- ☐ Regularly send attestation to the Group Owner or to a specified recipient, asking for a review of guest-user permissions.
- ☐ Based on the review outcome, execute the action of either archiving the Teams group or removing the Teams group.
- ☐ Change the recipient of the attestation to either the group owner, a custom address, or opt to not send the attestation depending on organizational requirements.
- ☐ You may insert an additional message in the attestation, if necessary.
- ☐ Set a time-out period for the attestation (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails to ensure potential issues are addressed promptly.
- ☐ Schedule the recurrence of the remediation action to keep guest-user permissions under regular check.



We had over 400 Teams channels that needed cleaning. This [CoreView] tool cleaned this up and set permissions to limit the access to create Teams channels.”

– User, Higher Education | [Read full review here](#)

Best practice #5: Regularly review and manage sensitivity labels for guest users in Teams

Sensitivity labels in Microsoft Teams provide a robust mechanism to secure information by assigning different levels of protection. Restricting guest-user access based on the assigned sensitivity labels ensures that only those who require such access have it. To enhance security further, it's good practice for Team owners to regularly review all guest users with sensitive data permissions, disabling any unnecessary accounts immediately.

→ ACTION PLAN:

- ☐ Regularly send attestations to a specified recipient, such as the group owner or a custom address, to review guest user permissions.
- ☐ Remove any unnecessary guest users from the Teams group.
- ☐ Set a time-out period for the attestation (between 1 and 180 days).
- ☐ Either archive the Teams group or remove the Teams group based on your organizational objectives.
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.

Best practice #6: Maintain multiple owners in Teams groups

Avoiding single-owner Teams groups is essential, particularly if an employee leaves the company or transitions to a new role or project. Having multiple owners secures a degree of continuity in the group. Microsoft recommends assigning at least two owners per team to avoid any gap caused by an owner's departure or role change. Regular evaluation of your Teams is crucial; if a team lacks multiple owners, add more members, or consider terminating the group.

→ ACTION PLAN:

- ☐ Send a communication to the group's owner or a specific recipient if multiple owners are not present.
- ☐ Change the recipient of the communication to either the group owner or a custom address if necessary.
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.

Best practice #7: Avoid Teams groups without owners

Teams without the proper owner assigned are vulnerable to misuse and potential security risks. To prevent ownerless Teams from proliferating, it's crucial to have a policy that ensures every team has an owner. Teams without owners might also indicate inactivity or lack of usefulness. Ensuring ownership of existing Teams helps keep Teams secure and sensitive data protected.

→ ACTION PLAN:

- ☐ Send a communication to the group's email owner or a specific recipient if a team lacks an owner.
- ☐ Change the recipient of the communication to either the group's email or a custom address if necessary.
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.



We are able to separate all of our departments and have CoreView assign a block of numbers to each department [in Teams]. Once a new user needs to be added, we automate it with the workflow, and it will automatically assign the department to the user. If we offboard the user, it opens it back up into that department with over 3,000 phone numbers this is a huge time saver”

– User, Government | [Read full review here](#)

License management

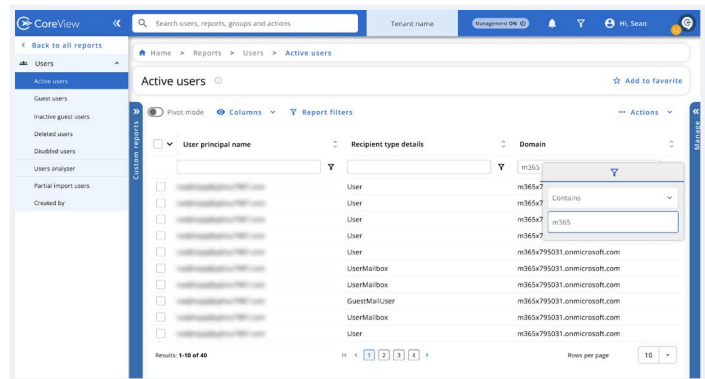
Microsoft 365 license management best practices

Managing licenses is critical for Microsoft 365 customers to maximize cost-effectiveness and drive operational efficiency. By proactively tracking and assigning the right tools to the right employees, you can prevent license waste, enable access to critical features, and align technology investments with organizational needs.

Here, we provide essential best practices for license management. Each best practice includes recommended remediation actions to support your governance plan.

Best practice #1: Consistently monitor and manage inactive Microsoft 365: E/F/G and EDU plans

Monitoring inactive plans is crucial for organizations to eliminate unnecessary costs and optimize license allocation. Identifying inactive plans enables organizations to reassign licenses from employees who no longer require certain features or tools to others who may benefit from them. This practice also aids in identifying opportunities for training or support, ensuring employees fully utilize the available tools and stay updated with the latest features and benefits of their Microsoft 365 subscription.



→ ACTION PLAN:

- ☐ Regularly send attestations to the manager or a specific recipient to review the usage of the Microsoft 365 plans.
- ☐ Convert the user's mailbox into a shared one, giving access to a named user, and assign the user's OneDrive permission to a new owner if the user is inactive.
- ☐ Remove the license from inactive users.
- ☐ Schedule the recurrence of the remediation action and set a time-out period (between 15 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.

Best practice #2: Monitor licenses assigned to guest users

Monitoring licenses assigned to guest users is essential to maintain control over resources and manage external access effectively. This practice ensures that only authorized individuals have access to specific services, protecting sensitive data and maintaining security standards. Monitoring guest user licenses also allows organizations to evaluate the value of collaboration with external parties, ensuring the right licenses are allocated to achieve organization objectives without overspending on unnecessary licenses.

→ ACTION PLAN:

- ☐ Regularly send attestations to the manager or a specific recipient to review the licenses assigned to guest users.
- ☐ Execute the action "Remove all licenses" from guest users who no longer require access.
- ☐ Schedule the recurrence of the remediation action and set a time-out period (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.

Best practice #3: Track licenses assigned to basic shared mailboxes

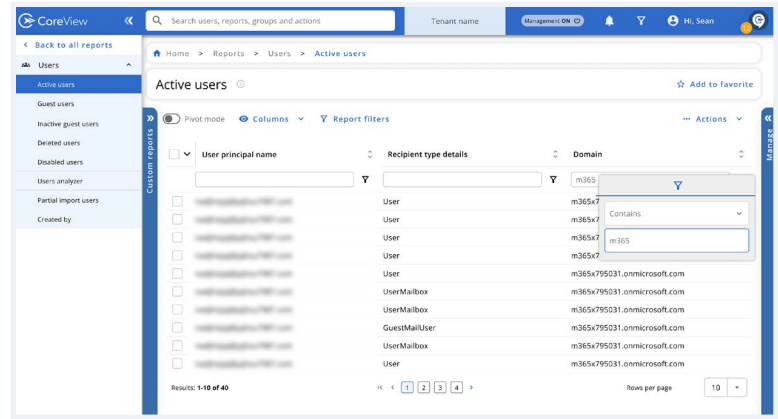
Keeping track of licenses assigned to basic shared mailboxes allows organizations to identify mailboxes that are no longer needed or actively used, freeing up licenses for other purposes. This ensures optimal utilization of resources, eliminates unnecessary expenses, and helps maintain a streamlined and cost-effective licensing framework. This practice also aids in improving productivity by ensuring that licenses are allocated appropriately to users who require access.

→ ACTION PLAN:

- ☐ Regularly send attestations to a specific recipient to review the licenses assigned to basic shared mailboxes.
- ☐ Execute the action "Remove all licenses" from shared mailboxes that are no longer active or needed.
- ☐ Schedule the recurrence of the remediation action and set a time-out period (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.

Best practice #4: Regularly monitor disabled users with assigned licenses

Regularly monitoring disabled users with licenses allows organizations to promptly identify and reclaim unused licenses for reassignment, saving costs, and optimizing resource allocation. This ensures that disabled accounts are not inadvertently granted access to sensitive information, reducing potential security risks and maintaining a robust data protection framework.



→ ACTION PLAN:

- ☐ Regularly send attestations to the manager or a specific recipient to review the licenses assigned to disabled users.
- ☐ Execute the action “Remove all licenses” from disabled users who no longer require access.
- ☐ Schedule the recurrence of the remediation action and set a time-out period (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.



The ability to delegate license management with excellent compliance controls is a great feature. Rules for what licenses can be managed and how many can be managed are fantastic.”

– User, IT Services | [Read full review here](#)

SharePoint and OneDrive management

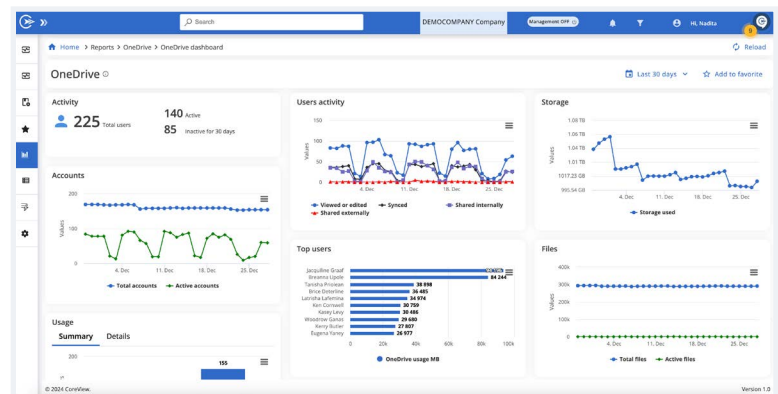
SharePoint and OneDrive management best practices

SharePoint and OneDrive are the backbones of collaboration, content management, and data storage in the Microsoft 365 ecosystem. These tools are the keys to seamless teamwork, document management, and collaboration.

Since these applications are so pivotal, implement the following best practices and the accompanying remediation actions to support your collaboration goals. These best practices work as the foundations for your governance framework, PowerShell scripts, or when implementing a Microsoft 365 management platform.

Best practice #1: Regularly monitor and manage inactive SharePoint sites

Active monitoring and identification of inactive SharePoint sites enable organizations to reclaim storage space, reduce maintenance costs, and optimize SharePoint performance. Moreover, it helps ensure that valuable information is not spread across abandoned sites, fostering better knowledge sharing, streamlined communication, and enhanced data security.

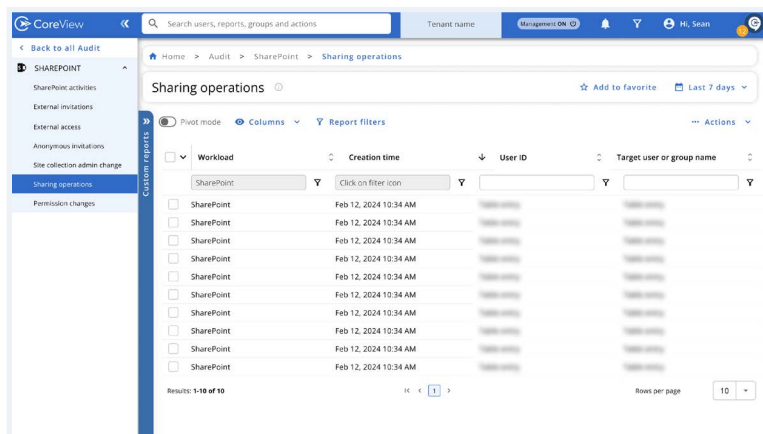


→ ACTION PLAN:

- ☐ Regularly send attestation to a specified recipient to review the activity of SharePoint sites.
- ☐ Delete SharePoint sites that are identified as inactive.
- ☐ Change the recipient of the attestation to either the site owners or a custom address as per requirement.
- ☐ Set a time-out period for the attestation (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.

Best practice #2: Monitor SharePoint sites with anonymous sharing

Monitoring SharePoint sites with anonymous sharing allows organizations to identify potential vulnerabilities and unauthorized access, ensuring that confidential data is not exposed to unauthorized users. Additionally, it lets organizations evaluate the necessity and effectiveness of such access, striking a balance between collaboration and data protection.



Workload	Creation time	User ID	Target user or group name
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		
SharePoint	Feb 12, 2024 10:34 AM		

→ ACTION PLAN:

- ☐ Regularly send attestation to a specified recipient to review anonymous sharing settings on SharePoint sites.
- ☐ Disable external and anonymous sharing for SharePoint sites where it's not needed.
- ☐ Set a time-out period for the attestation (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.

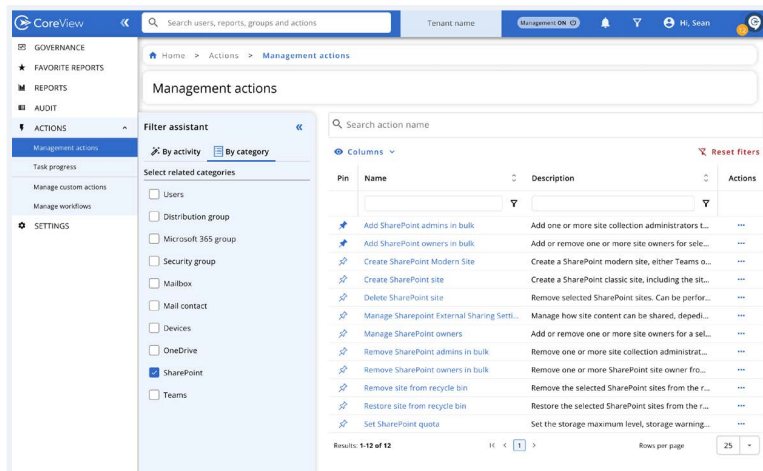


If you are considering using CoreView, I highly recommend that you do. This product has saved us time, money and effort. Once setup is complete, you have so much DATA and Management at your fingertips.”

– Senior Systems Engineer | [Read full review here](#)

Best practice #3: Monitor SharePoint sites with anonymous sharing and a certain sensitivity label

Monitoring SharePoint sites with anonymous sharing and a specific sensitivity label helps organizations identify any unauthorized attempts to access or share classified information with external parties, ensuring data confidentiality and compliance with regulatory requirements. It also reduces the potential for data breaches and maintains a secure collaboration environment.



→ ACTION PLAN:

- ☐ Regularly send attestation to a specified recipient to review anonymous sharing settings on SharePoint sites with a specific sensitivity label.
- ☐ Disable external and anonymous sharing for SharePoint sites where it's not needed.
- ☐ Set a time-out period for the attestation (between 1 and 180 days).
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.



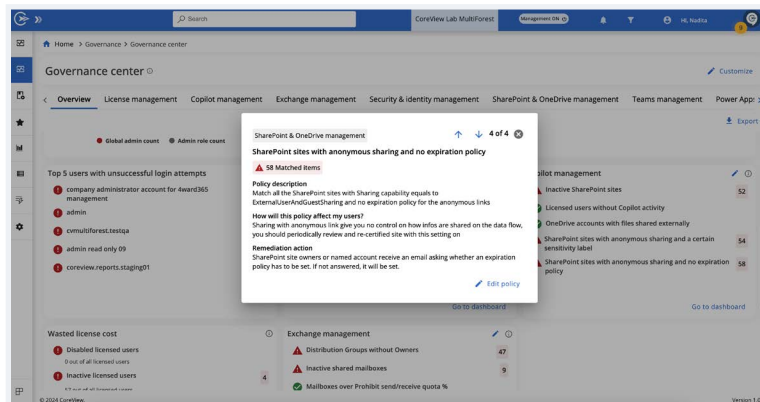
CoreView helps us segment and provide role and location-specific access to our teams, better enabling them to support our employee base and their use of our investment in Microsoft."



– IT Application Analyst | [Read full review here](#)

Best practice #4: Monitor SharePoint sites with anonymous sharing and no expiration policy

Monitoring SharePoint sites with anonymous sharing and no expiration policy allows organizations to enforce periodic reviews and updates, ensuring that SharePoint sites are still relevant and necessary. This proactive approach strengthens data protection measures, promotes data governance, and safeguards confidential information within the SharePoint environment.



→ ACTION PLAN:

- ☐ Regularly send attestation to a specified recipient to review the expiration policies of SharePoint sites.
- ☐ Set a customizable expiration policy for anonymous links on SharePoint sites.
- ☐ Set a time-out period for the attestation (between 1 and 180 days).
- ☐ Define the number of days after which the links expire.
- ☐ Enable or disable the email alert if the workflow fails.
- ☐ Schedule the recurrence of the remediation action.

Exchange management

Exchange management best practices

By implementing best practices in Exchange management, you can safeguard sensitive information, prevent unauthorized access, and adhere to regulatory requirements. As such, it's not just about mitigating potential risks and protecting reputation, it's also about fostering effective teamwork and streamlined workflows.

This section offers essential best practices for governing Exchange. Each practice comes with specific remediation actions and configurable settings to serve as a foundation for building PowerShell scripts, fine-tuning policies in your Microsoft 365 management platform, or as a framework for your governance program.

Best practice #1: Assign ownership to distribution groups

Assigning ownership to distribution groups is crucial for maintaining accountability and effective management of a group. An owner can manage access permissions, control who can send messages, and monitor activities within the group. This prevents miscommunication, delays in decision-making, and difficulty in coordinating efforts. It also reduces the risks of unauthorized access, potential data leaks, and compromises in sensitive information while preventing accumulation of outdated or irrelevant content within the group, simplifying storage and search processes.

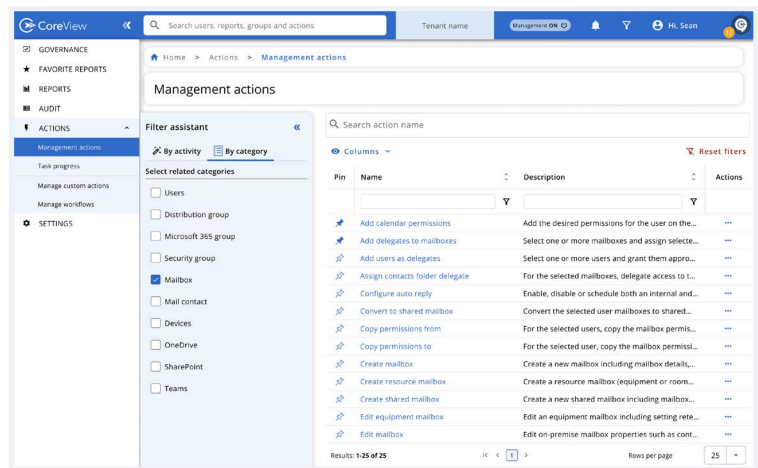
Without an owner, groups can lead to a lack of accountability and responsibility, potentially increasing security risks and hindering productivity. Important announcements or information may not reach the intended recipients, impacting collaboration.

→ ACTION PLAN:

- ☐ Identify distribution groups without owners.
- ☐ Assign a responsible owner to each identified group.
- ☐ Regularly review and update the ownership of each distribution group.
- ☐ Implement a policy that requires an owner for every newly created distribution group.
- ☐ Consider implementing automatic notifications to alert IT admins of distribution groups with no assigned owners.
- ☐ Schedule regular audits of distribution group ownership to ensure compliance with this best practice.

Best practice #2: Deactivate inactive shared mailboxes

Inactive shared mailboxes not only consume valuable licenses and storage space but also add unnecessary complexity to mailbox management. They may still contain sensitive information, posing a risk for data breaches and non-compliance with regulations. Deactivating these mailboxes frees up resources, maintains security, and promotes efficient resource allocation.



Inactive shared mailboxes can lead to unnecessary costs, inefficient resource allocation, and potential security risks. They may still contain sensitive information and emails that are open to unauthorized access, which could result in data breaches, non-compliance, and potential legal consequences.

→ ACTION PLAN:

- ☐ Identify inactive shared mailboxes.
- ☐ Review the content of the inactive mailboxes for sensitive information.
- ☐ Send attestation to a specified recipient to confirm the deactivation.
- ☐ Execute the action to remove the inactive mailbox.
- ☐ Regularly monitor shared mailboxes for activity.
- ☐ Schedule the recurrence of the remediation action.



The most crucial feature is the ability to manage mailboxes, edit them, work permissions, assign licenses, etc. almost everything necessary for administrators.”

– Manager | [Read full review here](#)

Best practice #3: Manage mailbox sizes within appropriate limits

Exceeding the mailbox quota can cause a loss of important emails and critical organization information, compliance issues, and even legal consequences. It can also lead to performance degradation, server instability, and increased storage costs. Monitoring and managing mailbox sizes within appropriate limits are essential to mitigate these risks, ensure smooth organization operations, and maintain system efficiency.

→ ACTION PLAN:

- ☐ Identify mailboxes that are over the Prohibit send/receive quota.
- ☐ Enable the Mailbox archive by setting the “Has archive” to “True” for the mailbox.
- ☐ Send an alert to the mailbox owner informing them of the issue.
- ☐ Provide guidance to the mailbox owner on how to manage the mailbox properly.
- ☐ Regularly monitor mailbox sizes.
- ☐ Schedule the recurrence of the remediation action.

Best practice #4: Monitor mailbox sizes and enforce warning quotas

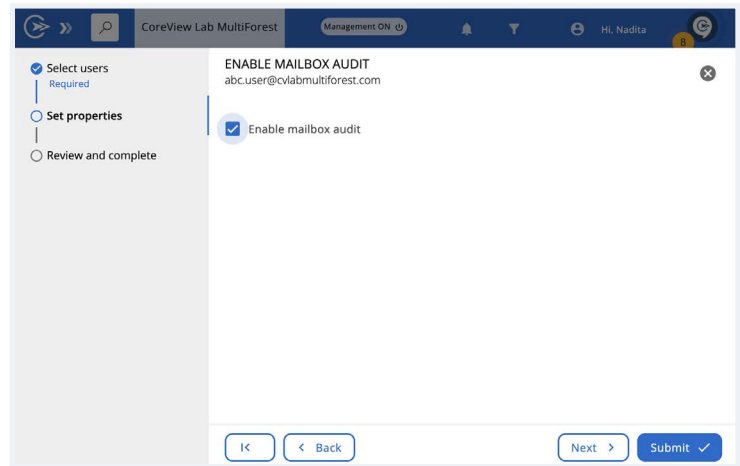
Exceeding the warning quota of mailboxes can lead to data loss, as users may not be aware of imminent mailbox space limitations. These limitations can cause important emails and information to be discarded. This also strains system resources, slows down email delivery, and increases server load, impacting the overall performance and stability of the email infrastructure. Closely monitoring mailbox sizes and managing them within the warning quota limits is crucial.

→ ACTION PLAN:

- ☐ Identify mailboxes that are over the warning quota.
- ☐ Enable the Mailbox archive for these mailboxes.
- ☐ Send an alert to the mailbox owner informing them about the issue.
- ☐ Provide guidance to the mailbox owner on how to manage the mailbox properly.
- ☐ Regularly monitor mailbox sizes for compliance with the warning quota.
- ☐ Schedule the recurrence of the remediation action.

Best practice #5: Enable auditing for all mailboxes

When audit logs for mailboxes are disabled, it becomes challenging to track and investigate any unauthorized access or data breaches. This can lead to potential legal repercussions, non-compliance penalties, and damage to the organization's reputation. Enabling audit logs for all mailboxes is required for maintaining security, regulatory compliance, and effective incident response.



→ ACTION PLAN:

- ☐ Identify mailboxes with audit logs disabled.
- ☐ Send attestation to a specified recipient for approval to enable auditing.
- ☐ Execute the action to enable mailbox auditing.
- ☐ Regularly review audit logs for any suspicious activities.
- ☐ Schedule the recurrence of the remediation action.

Best practice #6: Block sign-in for shared mailboxes with unblocked credentials

Unblocked credentials on shared mailboxes may allow unauthorized users to impersonate legitimate users, leading to unauthorized actions, data manipulation, or theft. This can disrupt email workflows, impact email deliverability, and potentially expose the organization to malware or phishing attacks. Therefore, blocking sign-in for shared mailboxes with unblocked credentials is essential to prevent unauthorized access and maintain security.

→ ACTION PLAN:

- ☐ Identify shared mailboxes with unblocked credentials.
- ☐ Execute the action to block sign-in for these accounts.
- ☐ Regularly review the sign-in status of shared mailboxes.
- ☐ Schedule the recurrence of the remediation action.

Best Practice #7: Assign delegation for shared mailboxes

Shared mailboxes without specific delegation can lead to inefficiency, bottlenecks in managing and responding to shared emails or customer inquiries, and lack of clarity on who is responsible for handling specific tasks or requests. Assigning delegation for shared mailboxes reduces data redundancy, inconsistencies, and potential privacy breaches, and it improves customer satisfaction, collaboration, and overall operational effectiveness.

→ ACTION PLAN:

- ☐ Identify shared mailboxes without delegation.
- ☐ Assign specific users or groups with delegation rights to the mailbox.
- ☐ Send an alert to a specified recipient about the delegation status.
- ☐ Regularly monitor shared mailboxes for proper delegation.
- ☐ Schedule the recurrence of the remediation action.

Best practice #8: Monitor unlicensed shared mailboxes approaching 50GB limit

Unlicensed shared mailboxes nearing the 50GB limit can disrupt collaboration and productivity, and there's a risk of data loss as exceeding the limit could result in emails being deleted. Monitoring these mailboxes and maintaining them within acceptable limits ensures smooth system performance and prevents potential stability issues with the email infrastructure.

→ ACTION PLAN:

- ☐ Identify unlicensed shared mailboxes approaching the 50GB limit.
- ☐ Send an alert to the tenant admin about the issue.
- ☐ Provide guidance on how exceeding limits affects the environment and suggest actions (like archive efforts).
- ☐ Regularly monitor mailbox sizes.
- ☐ Schedule the recurrence of the remediation action.

Best Practice #9: Enable litigation hold for users

Not implementing litigation hold can result in loss or accidental deletion of critical data required for legal or compliance reasons. Enabling litigation hold for users mitigates risks of data loss due to accidental deletion or malicious activities, and it facilitates the preservation and retrieval of relevant information during eDiscovery processes.

→ ACTION PLAN:

- ☐ Identify users without litigation hold.
- ☐ Execute the action to enable litigation hold.
- ☐ Send an alert to the user principal name about the status.
- ☐ Regularly review users for compliance with this best practice.
- ☐ Schedule the recurrence of the remediation action.

The screenshot displays the 'MANAGE LITIGATION HOLD' configuration page for a user in the CoreView Lab MultiForest environment. The left sidebar indicates the current step is 'Select user mailbox', which is marked as 'Required'. The main content area shows the user 'abc.user@cvlabmultiforest.com' with the 'Litigation hold enabled' checkbox checked. Below this, there is a 'Duration' section with an 'Unlimited' checkbox and a text field for 'Litigation hold duration (days)'. There are also text fields for 'Litigation hold url' and 'Litigation hold note'. At the bottom of the panel, there are navigation buttons: '< Back', 'Next >', and 'Submit ✓'.

Conclusion

By now, you know that the importance of a solid governance framework cannot be overstated. And, the volume of work will only increase as Microsoft customers rely on AI to work better and faster. It's about more than just policy enforcement and security measures; it's about ensuring the seamless, efficient, and secure operation of your M365 environment—regardless of how the IT landscape evolves over the next five or ten years.

Incorporating CoreView into your governance plan grants deep visibility into your Microsoft 365 environment, helping you to identify potential compliance gaps and optimize IT operations. As the industry continues to shift, delaying the adoption of an advanced governance solution could leave you vulnerable to attacks, data breaches, and compliance violations.

Now is the time to proactively enhance your Microsoft 365 governance strategies with CoreView.

For more on implementing these and other Microsoft 365 governance best practices, check out the related resources below.

WEBINAR

Governance for everyone:
Five building blocks for a stress-free Microsoft 365 world

[Watch now](#)

BLOG

An admin's guide to navigating
audit logs in Office 365

[Read now](#)

CASE STUDY

Organization saves over \$1M
in Microsoft 365 licensing costs
with CoreView

[Learn more](#)

SOLUTION

Automated governance
solutions from CoreView

[Learn more](#)

About the author



Kas Nowicka | Product Marketing Manager

With a decade of experience exclusively focused on Microsoft cloud solutions, Kas Nowicka melds her tech knowledge with her background in understanding human behavior and being an educator and technology evangelist at heart—covering fundamentals of governance, adoption and productivity in Microsoft 365. She has worked in the field as a solutions architect and helped dozens of organizations to ease their most pressing Microsoft 365-related pains.

[Connect on LinkedIn](#)



David Mascarella

Chief Global Strategist and CoreView cofounder with over 20 years of experience in Microsoft systems integration, cloud environments, and compliance.

[Connect on LinkedIn](#)



Roy Martinez

CoreView Technology Evangelist with over 16 years in Microsoft with a passion for Microsoft 365 governance, adoption, and automation.

[Connect on LinkedIn](#)

CoreView stands as the leading Microsoft 365 management platform for IT teams. It revolutionizes the way Microsoft 365 stacks are managed, providing a unified approach to configuration management, delegated administration, and automated governance. CoreView is a Microsoft AI Cloud Partner, available in the Azure Marketplace, and works exclusively with Microsoft resellers, solution integrators, and managed service providers, ensuring organizations get the most out of Microsoft 365.