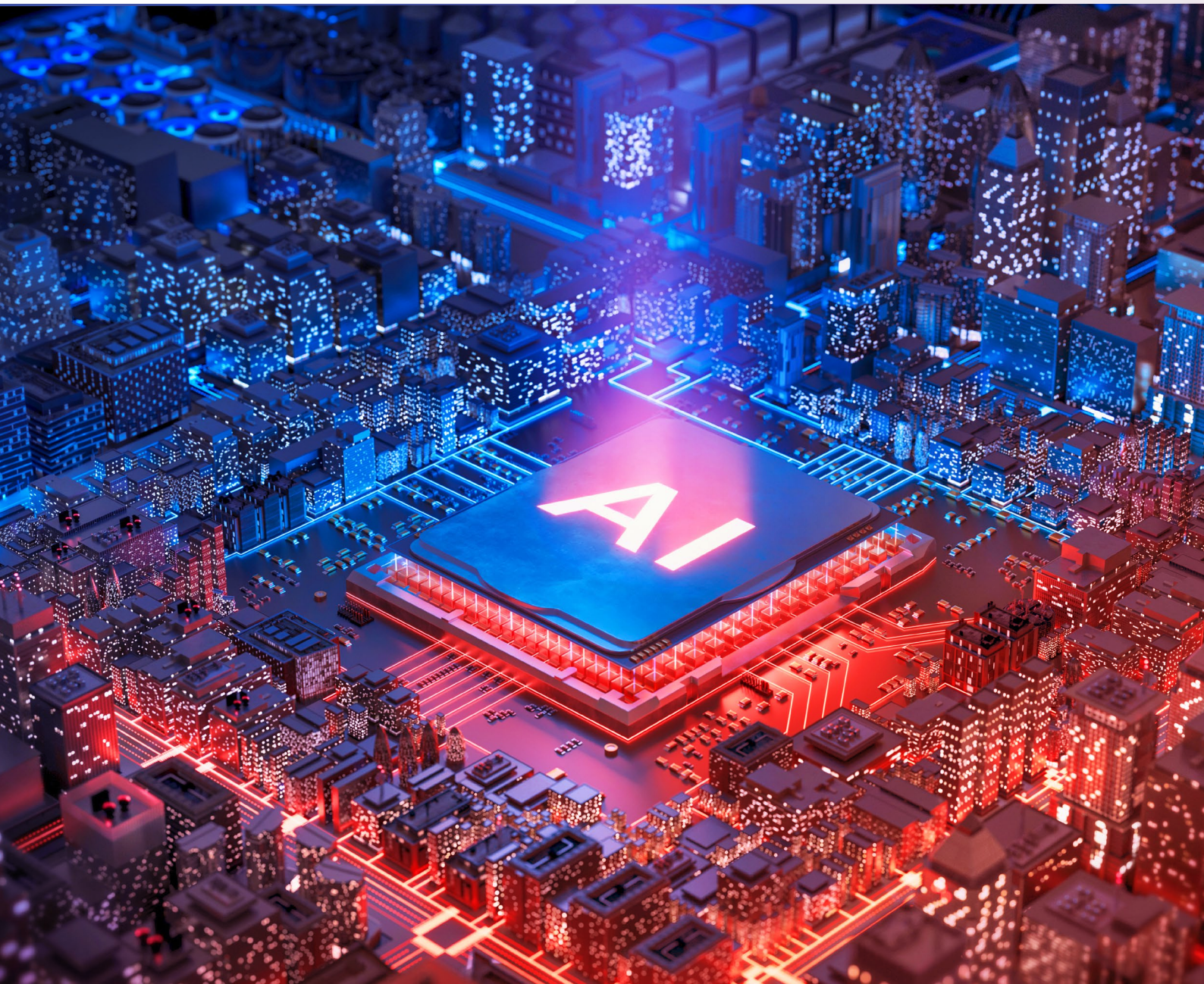
AvePoint®

3 Automation Strategies to Overcome AI Governance Challenges



3 AUTOMATION STRATEGIES TO OVERCOME AI GOVERNANCE CHALLENGES

The integration of AI-powered tools like Microsoft 365 Copilot represents a transformative opportunity for organizations seeking to enhance productivity and innovation across their digital workspaces. However, the journey toward realizing the full potential of these advanced technologies extends far beyond initial implementation.

While technology and data readiness will get you started on Copilot, they're not enough to scale and sustain AI success that delivers a meaningful return on investment (ROI). Executive buy-in and proper data governance policies are a must for employees to get the most from Copilot's capabilities.

However, data governance remains a roadblock for organizations looking to adopt AI. PwC's 2024 US Responsible AI Survey revealed that 43% of organizations had deployed generative artificial intelligence (GenAI) for operational tasks, but only 11% have fully implemented responsible AI measures, which involve having AI-specific governance and risk management measures in place.

Why? The same survey finds that most organizations struggle to quantify the risk mitigation from having responsible AI strategies (29%), while for some, it is just not a budget priority (15%), or the leadership is unclear about its value (15%).

These kinds of deployments – implementing GenAI without proper measures in place – now form part of the organizations that face governance problems as they use AI.

This guide explores these top governance challenges when using GenAI in the digital workplace and how to resolve them.

CHALLENGE #1: PROPER WORKSPACE PROVISIONING

Organizations typically entrust IT administrators with the full burden of creating users, workspaces, and sometimes even content. Allowing objects to be created in workspaces without proper provisioning can increase risk within organizations and create tons of "clutter," making it more difficult for users to find what they need.

With the use of GenAI, this becomes more complex. According to a Salesforce report, 59% of organizations do not have a unified data strategy. With the speed at which documents are created and shared across workspaces, data clutter becomes easier, and there are bigger risks of sensitive data sitting in workspaces without proper data governance in place.

Many organizations limit creation to a set of users or admins who are responsible for receiving requests and then creating the workspaces with the necessary security and content settings applied. This process can take many hours for a nu mber of different reasons.

Sometimes, the person who should or can have access to a certain workspace might need to be verified before it's created.

Often, users' requests are unclear, and admin teams may need to communicate with one or more users to clarify what is needed and verify that the user's request is within organizational policies.

Solution: Implement a Delegation Framework

Implementing a robust authority delegation framework enables organizations to distribute access management responsibilities without compromising security protocols. By allowing designated users to grant permissions within their domain of expertise, companies can significantly ease IT bottlenecks while maintaining governance standards.

For organizations leveraging GenAI, delegated permissions become even more crucial. Project owners can:

- Control which AI models access specific datasets

- Define which team members can access sensitive content with AI tools
- Establish clear boundaries for AI-generated content distribution

Benefits of a Delegation Framework

Reduced IT bottlenecks. Distributing access management responsibilities alleviates the constant burden of handling all access requests by IT teams. This improves overall efficiency and allows them to focus on more strategic tasks.

Enhanced security. Delegating permissions within specific domains of expertise ensures that access is granted based on a thorough understanding of the data and its sensitivity. This improves security by minimizing the risk of unauthorized access.

Improved compliance. With clear boundaries and guidelines for AI-generated content, organizations can ensure that all data-handling practices comply with business policies and regulatory requirements. This reduces the risk of non-compliance and associated penalties.

Faster response times. Empowering project owners and designated users to manage access within their domains enables quicker responses to access requests. This improves productivity and ensures that team members have timely access to the resources they need.

Scalability. As organizations grow, a delegation framework allows for scalable access management. New projects and teams can be quickly onboarded with appropriate access controls, ensuring seamless expansion without compromising security.

CHALLENGE #2:

MICROSOFT TEAMS AND GROUPS ACCESS MANAGEMENT

Ensuring that the right people have the right authority in the Group and that the Group is labeled and categorized with the correct business context is essential. As teams audit and review information in their systems, it will be necessary to correct settings and permissions that do not align with business policies.

This requires communication with end users and stakeholders to justify such changes and advise of the corrections. Depending on what needs to be corrected, this entails many hours of communications and meetings, let alone the actual correction of solution settings to fix the problems

Similarly, recertifying access is often manually intensive and requires extensive communication between IT and business users. However, settings and permissions that do not align with business policies introduce security risks to the organization.

GenAI usage in organizations exacerbates this challenge. It can generate content and automate processes, but it also introduces new layers of complexity in access management. Ensuring that AI-generated content adheres to business policies and that AI systems have appropriate access permissions requires additional oversight. This can lead to increased coordination efforts between IT, business users, and AI governance teams.

Solution: Automate Security Reports and Policy Enforcement

To ease the burden on IT teams or organizational admins in reviewing, renewing, and revoking access, administrative and security reports must be automated.

Automated security reports can provide insights into access permissions, highlight discrepancies, and ensure compliance with business policies at a time or frequency of the organization's choosing. These reports can also help identify potential security risks and unauthorized access, enabling quicker corrective actions.

Challenge #1: Proper Workspace Provisioning

Challenge #2: Microsoft Teams and Groups Access Management

Challenge #3: Lack or Absence of Data Lifecycle Processes

Similarly, to reduce time spent on recertification and revocation of access, admins can:

- **Automate the addition of metadata** to collaboration spaces as they are being provisioned and force accuracy by adding properties reflecting the business use. This is done based on the users, user properties, and organization structure and by forcing the requester to select from a few options during the provisioning process.
- **Automate policy enforcement**, such that if users make changes to settings or permissions that are outside business policies, the action can be automatically reverted. This capability maintains the safety of the organization's data and ensures that no information can be accessible to unauthorized users, especially as they use GenAI in the organization.
- **Monitor security and permissions** to identify who has access to restricted data or if any external users pose a threat to your workspace information. Understand where anonymous links are stored and update out-of-policy permissions to curb risks in the environment. These steps can ensure that no user can access sensitive information as they use AI.

Challenge #1: Proper Workspace Provisioning

Challenge #2: Microsoft Teams and Groups Access Management

Challenge #3: Lack or Absence of Data Lifecycle Processes

CHALLENGE #3:

LACK OR ABSENCE OF DATA LIFECYCLE PROCESSES

Old Teams and Groups degrade content quality within the organization, making it hard for employees to find the right information quickly.

Because a Team sits on top of Microsoft 365 Groups, several artifacts are left behind. Continuing to manage, backup, and store this information could translate to recurring storage costs. In addition, obsolete artifacts also make your collaboration environment messy, potentially leading to data sprawl.

To properly manage the data lifecycle, organizations must install mechanisms for determining when data is ready to be systematically archived or deleted. When it comes to managing and enforcing lifecycle rules, organizations need more than basic blanket controls. Equally important, they need reporting and oversight over the process.

However, the rapid pace of content creation with GenAI can make it challenging to keep up with lifecycle management. GenAI can generate vast amounts of content and automate processes, which can increase the volume of data that needs to be managed. Ensuring that AI-generated content adheres to lifecycle policies and determining when such content should be archived or deleted requires additional governance.

Solution: Automate Information Lifecycle Policies

The implications of a well-enforced lifecycle process are clear: users find relevant content faster, and don't waste as much effort re-creating what's already there.

In addition, organizations do not have to worry about retaining relegated content for discovery, and the ability to classify and access information more quickly and accurately reduces risk and shortens any regulatory or internal audits that may need to be conducted.

Organizations can automate the application of retention policies on content based on its nature and relevance to users and their roles

Challenge #1: Proper Workspace Provisioning

Challenge #2: Microsoft Teams and Groups Access Management

Challenge #3: Lack or Absence of Data Lifecycle Processes

among other factors. This means that far beyond blanket retention policies, organizations have the necessary level of control over archiving or removing stale data and irrelevant content as soon as allowed by business policies and regulations.

Understand the Value of Automated Governance

A clear deployment and ongoing success strategy rooted in effective workspace provisioning, access management, and data lifecycle practices are critical to delivering accurate and role-appropriate results that drive value at every stage of your AI adoption journey.

To understand how your organization spends time in implementing data governance policies, AvePoint's automated governance value calculator provides conservative estimates of how many minutes per year, per workspace in an environment, IT spends maintaining and managing settings and services for user productivity and service delivery.

Once the time savings are quantified, we can convert them to monetary savings by estimating the amount of salary per minute spent on each task.

Calculate the value of automated governance

Try the calculator now

While the value is impressive, it only scratches the surface of the value of automating governance as organizations continue to steer towards AI utilization in their workspace. This is where understanding the level of governance that is right for your organization and how third-party tools can help you achieve your required governance level is critical.

AvePoint US Headquarters
525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310
+1.201.793.1111 | sales@avepoint.com