Microsoft

Azure Active Directory Identity Governance

Managing access to resources is one of the most challenging jobs for today's enterprise. Employees are not the only users accessing organizational resources—the ability of contractors, partners, and vendors to access resources is key to the modern workplace.

It's important to have a comprehensive identity governance solution that delivers access to all applications and information that users need when and where they need it, based on the organization's security policies.

Azure Active Directory (Azure AD) Identity Governance enables organizations to efficiently and securely manage their digital identities by ensuring that the right people have the right access to the right resources.

This native capability within Azure AD helps your organization protect, monitor, and audit access to critical assets while ensuring employee productivity.

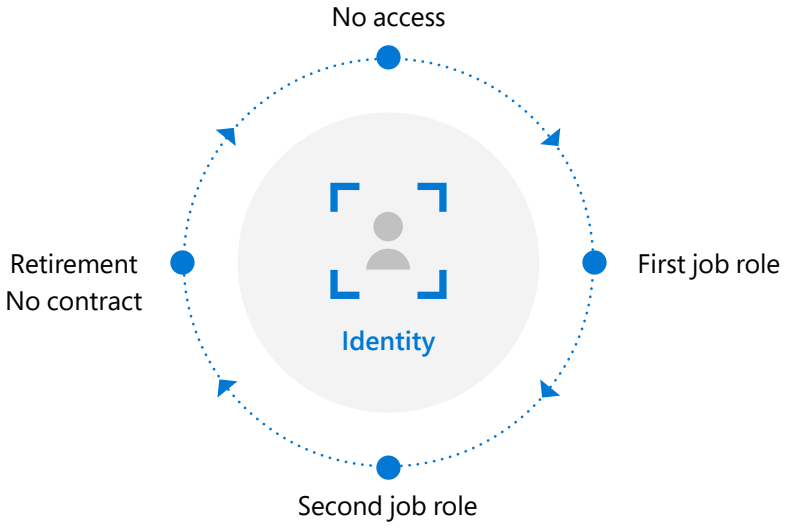
With Azure AD Identity Governance, you'll be able to secure the following aspects concerning employees, business partners and vendors, and services and applications:

- Identity lifecycle
- Access lifecycle
- Privileged Identity Management

Identity lifecycle

Identity lifecycle management helps to set the foundation for identity governance. In order to have successful governance at scale, there needs to be a shift in how a user's identity across an organization is managed during the lifespan of that user's relationship with the organization. Everyone within the organization has their own subset of resources necessary for their job, but without a defined list of what each role needs for each project, managing access is challenging. Adding guest users compounds the challenge.

As a user—regardless if they're an internal employee or a guest—joins, moves within, or leaves an organization, their system identity and resource access should adjust with them. The identity lifecycle capabilities solve this challenge by facilitating the creation, maintenance, and ultimate deletion of user identities across applications for better collaboration.



Access lifecycle

Go beyond simply giving users birthright access when they are onboarded. Maintain a process that enables your users' access to change as their needs change. The access lifecycle provides efficient and appropriate access permissions to users based on their business needs. To ensure users don't have excessive and unnecessary access rights, team members gain and lose access to resources as teams form and then disband.

With tools like dynamic groups for defining who can access SaaS apps, you can turn access management into an automated access process to reduce the burden on IT and business decision makers. Further, entitlement management enables users, including guests, to request access across groups and applications as well as SharePoint Online sites.

Users' rights can be reviewed and adjusted regularly during access reviews. Selecting reviewers who can approve or deny a user's continued access is especially important when it comes to guest users. For all users in your environment, Azure AD Identity Governance will help recommend a decision to the reviewer based on the user's sign-in activity, giving you the ability to proactively engage with resource owners, remove excessive rights, and help provide resources while ensuring productivity.

To combat the struggles surrounding access, entitlement management lets resource owners create access packages containing:

- SaaS apps (Salesforce and ServiceNow)
- Line-of-business apps
- Azure AD and Office groups
- Teams and SharePoint Online sites

Privileged Identity Management

Another key lifecycle in identity governance is that of users' privileged access. Minimizing the number of users with access to sensitive resources helps maintain an overall secure environment, but there are still users who need admin rights. Govern admin access to mitigate the risk of excessive, unnecessary, or misused access rights—whether they're from your organization or an outside vendor, contractor, or partner. Azure AD Privileged Identity Management (PIM) orchestrates assigning privileged-access rights to resources to reduce the risks of today's threat landscape.

What is privileged access?

Just-in-Time and scheduled access, alerting, and approval workflows for Azure AD and Azure Resource roles.

What can I do with PIM?

- **Get Just-in-Time access** for privileged resources
- **Create time-bound** access to resources
- **Require approval** for activation of a privileged role
- **Take action** if admins attempt to create backdoor admin accounts
- **Ensure compliance** with corporate privileged-access policies
- **Track changes** in privileged role assignments and role activation history with an audit log

Help protect your organization

with the proper identity governance tools.

Update your identity and access management to better protect critical resources and still provide access to the users who need it—when they need it. Use tools from Microsoft to help keep you up to date as you navigate the modern environment.

Try a free trial of this trusted solution today.