Microsoft Teams Governance

with Oxford Computer Group and Saviynt

OXFORD COMPUTER GROUP

A Comprehensive Solution for Teams Governance

Saviynt wraps automation, access requests, risk visibility, and certification around the collaboration environment, enhancing security without impeding business agility or adding friction to collaboration. Oxford Computer Group is Saviynt's 2018 and 2019 Impact Partner of the Year, and our implementation and managed services expertise integrates Microsoft Teams Governance with Saviynt into your business processes.

Saviynt enables organizations using Teams to adopt an identity-based approach to Teams governance with user friendly request and approval workflows, enabling them to control access configuration, data, and identities within Teams.

Complete visibility into each Team's risk profile

Saviynt's combined identity, application access, infrastructure, and privileged access solution gives organizations a real-time view into risk across the ecosystem. For Microsoft Teams, this means alerting administrators to Teams configured to allow Guest users to create Channels, Teams with only Guest users, Teams with disabled owners, and other potential security risks. This allows administrators to make informed decisions to remediate each situation.

Team member lifecycle management

Saviynt's real-time automation capabilities provision users directly into teams based upon their identity, or remove them when they no longer need access, while also providing an intelligent access-request capability for users. Access certification reviews let Team owners inspect the validity of Team members. When a Team owner departs or changes roles, Saviynt provides automated succession management to assign a new owner so no Team is ever unmanaged.

The Business Challenge

Managing access, configuration and ownership of your Microsoft Teams ecosystem can be challenging. Users can create Teams and Channels, add members, change roles, and invite external collaborators to join a Team. This means that a Team or a Channel may have members with access they no longer need, overpermissioned external users accessing private business discussions, or a Team or Channel operating without appropriate security controls.

Data shared on Teams Channels or in Teams Site Collections can easily escape scrutiny. Once a Team Site Collection is created, access to data can be granted outside of the Team as well as through it. This can result in Personally Identifiable Information (PII), Payment Card Information (PCI), Personal Health Information (PHI), or Intellectual Property being inappropriately exposed, leading to reporting and compliance issues.

To combat these risks, organizations must upgrade their control around team creation and configuration, what rights different roles within teams have, who can upload documents, what data should be exposed to whom, and so on. Security around Teams can be enhanced with lifecycle management, approval workflows, and succession management, and you get all that—and more—with Saviynt for Microsoft Teams.

Data discovery, analysis, and governance

Teams enables collaborators to upload and share large numbers of documents, either to Channels or to Site Collections. Saviynt lets organizations scan Teams data stores and locate PII, PCI, intellectual property, or other high value data to see who has access to it. Organizations can restrict what users can do—such as not allowing a Guest to edit files—and can restrict access to sensitive data.

Continuous compliance for Teams

Saviynt provides out-of-the-box controls for common platforms to meet compliance mandates such as SOX, HIPAA, GDPR, and more, as well as allowing organizations to design their own controls based on corporate security policy. Microsoft Teams becomes compliance-enabled with the Saviynt solution, ensuring Segregation of Duties (SoD) and other controls are monitored and enforced.