# Mitigating Active Directory Risk

## What Is Your Experience Navigating Active Directory?

Microsoft's Active Directory (AD) is critical and complex to manage -- the figurative keys to the corporate kingdom that provide permissions and access to all IT assets across the enterprise, from devices and desktops to servers.

All users who are granted Domain Privileges -- whether on purpose, by accident or a part of a breach -- have the ability to cause serious problems for an IT organization that does not stay on top of the day-to-day management of the Directory and all its complexities.

Having the ability to crawl the Directory to look for problems and correct them quickly by leveraging native Microsoft tools or third-party solutions is critical to a healthy working environment. Yet, there remain functional gaps to be filled and unforeseen risks that need to be managed.

## What's at Risk:

Due to internal security and risk concerns, human error, as well as internal/external auditors of regulated firms, all IT organizations have strict policies and standards that are dictated by upper management. (Or they should.) Although there are a number of different AD services supported by a logical directory structure consisting of objects, forests, trees, domains and organizational units, inherent operational issues need to be addressed regularly or attested to by individuals with management or ownership privileges, to ensure the AD environment is functioning properly.

**Group Policy** Many of the inherent problems large organizations experience over time within AD are directly associated with Group Policy. Group Policy Object (GPO) management should be a major focus of any regulated organization looking to limit exposure and risk. This is the hierarchical structure within the directory, allowing administrators to implement specific configurations or changes for users and computers – and to be effective, it should be uniform across the entire enterprise. Without uniformity and consistency, security and configuration settings such as a password expiration and policy, audit configurations and event logging will be inconsistent. This will cause conflict and slow down a user's log in experience, not to mention issues of business continuity and potential breach risk.

**Privileged Access** Problems associated with Active Directory can become systemic when they bleed into other critical areas such as Privileged Access. Privileged Users can make changes to the system without authorization. A post change audit-log could potentially capture the occurrence, but then what? If these types of events are happening and Privileged Users are making unauthorized changes, PAM solutions are being bypassed! More importantly, stale accounts that still have privileged access create risk and technical debt. Unknown users can potentially make changes to the domain including Group Policy Objects, which is an extremely bad and risky practice.

SPHERE
TECHNOLOGY**SOLUTIONS**

# Mitigating Active Directory Risk

## What Is Your Experience Navigating Active Directory?

**Active Directory Nesting:** Other areas within Active Directory that should be addressed to ensure efficiencies are nested groups, circular nesting, broken inheritance, or the more serious violations involving domain administrators granting unknown access to colleagues in clear violation of corporate policy.

## Resolving Operational Issues with SPHEREboard:

SPHERE Technology Solutions is a niche software and services company that works with large, complex IT organizations helping them limit IT risk while addressing many of the security, governance and compliance issues they face on a quarterly basis. SPHERE's proprietary technology solution, SPHEREboard, directly addresses areas of AD risk through GROUPcontrols, consolidating problematic AD groups and providing insights and automation to certify and understand how even the most simple of changes can impact critical systems.

- **GPO Analysis** Identify all issues that need to be resolved to meet standards, identify security gaps, compliance violations or other risks to the infrastructure.
- **AD Permissions Analysis** Understanding administrative access to gain visibility into who has the ability change accounts and to ensure remediation is managed and maintained.
- **AD Delegate/Privileged Access Analysis & Clean-Up** Operational Unit delegate access, domain privileged access through group membership and Group Policy Object (GPO) management rights. Provide additional analysis of who has access to elevated roles to clean up and certify ownership.
- **Owner Certification & Review** Detailed review identifying "probable" owners before any changes are implemented.
- **Remediation** Simple, flexible templates allow for automated actions and the ability to trend future state and help drive priorities.
- **Customization** Additional metrics and functionality can be added or developed upon request.

Take the complexity out of Active Directory groups.
Contact sales@sphereco.com or call (201) 659-6204 to talk to one of our data security experts.