

Active Directory & Entra Configuration Assessment

A secure and well-managed identity foundation begins with visibility. RKON's IAM advisory team delivers a targeted assessment of your Microsoft Entra and Active Directory environments, uncovering misconfiguration, legacy settings, and potential exposure points. Using deep-dive analysis and proven assessment techniques, we provide clear insights into identity-related risks and operational weaknesses. Whether you're preparing for a migration, reducing support burdens, or modernizing your directory services, this focused review equips your team with prioritized findings and actionable recommendations.

Key Business Outcomes

- ✓ Identify critical Indicators of Exposure (IOEs) across Active Directory and Entra configurations
- ✓ Detect known Indicators of Compromise (IOCs) tied to attacker behavior and post-exploitation techniques
- ✓ Surface misconfigurations in domain trusts, replication, and authentication protocols
- ✓ Highlight risky delegation paths and excessive permissions exposing lateral movement vectors
- ✓ Reveal legacy settings, stale accounts, and insecure Group Policy configurations
- ✓ Provide a categorized list of findings with severity rankings and remediation guidance

Strategic Value Summary

- Establishes a baseline identity security posture
- Highlights critical configuration and exposure gaps
- Supports audit and security review efforts
- Enables cleanup of legacy identity risks
- Reduces privilege and delegation-related risk
- Improves visibility across hybrid identity environments

Why RKON

- Microsoft Solutions partner for Security, specializing in Identity & Access Management
- Full stack, technology-agnostic solutions

