



Identity Access Management Services

Identity is your most powerful security tool. Ensure the right people have access to the right resources for the right reasons.

Identity remains the single biggest risk exposure and security gap facing organizations. The challenge only multiplies with the proliferation of Non Human Identities (NHIs) and AI-related threats. Despite this critical vulnerability, very few companies maintain ongoing, clear visibility into their overall identity posture.

Tevora's Identity Access Management consultants help you uncover blind spots and comprehensively understand your access control gaps. We partner with your team to mature your identity lifecycles, optimizing everything from secure user provisioning and access reviews to privileged access management.

Comprehensive Identity Security Services:



Identity Governance and Administration (IGA)

Tevora helps you establish airtight access controls using the right identity solutions for your organization. We'll help you implement the right Identity Solution to address your specific business and security needs, assessing authentication and authorization, SaaS account provisioning, SSO, MFA, password reset, B2C, and other aspects of access management.



Identity Access Management

As the most critical security tool in your organization, Tevora expertly assesses your IAM environment to identify potential security risks. We consider all IAM architecture components, including Governance, Federation, Access Management, Identity Management, and Credential Management, to ensure a holistic look. The resulting analysis and remediation roadmap outlines prioritized steps necessary to implement your state-of-the-art IAM program.



Identity Provider Migration

Switching between Identity Providers (IdPs) – such as Okta, Microsoft Entra ID, Ping, or others – can be an arduous and time-consuming task. Tevora has the experience and tools required to help even the largest enterprises migrate identities, applications, associations, etc. between IdPs. Our unique approach meticulously considers user experience, executive concerns, and accomplish zero down-time during the migration process.

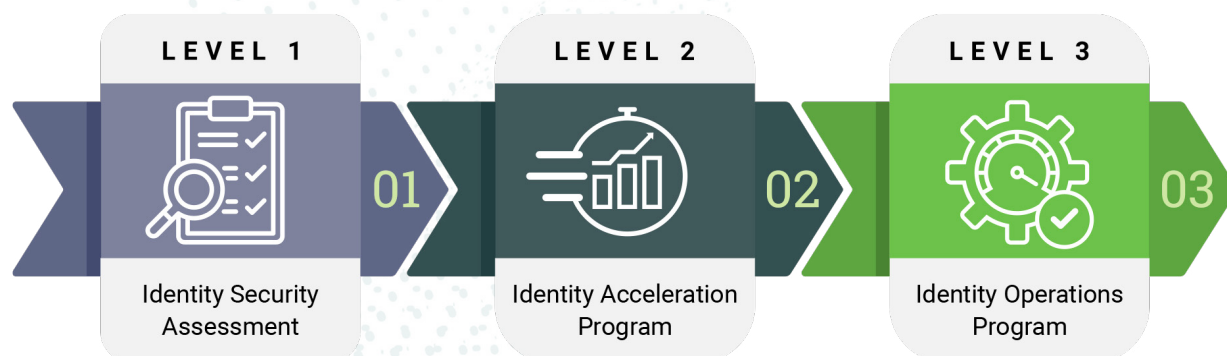


Zero Trust

Tevora helps design and implement a Zero Trust security framework within your organization. Through strict access controls, risk-based authentication (RBA), integrated authentication, device posture monitoring, and access control, we assess and help operationalize all aspects of a successful Zero Trust strategy.

Service Levels

Organizations are at different stages in their AI adoption journey, requiring varying levels of assessment, guidance, and operational support. Our service offerings are structured across three engagement tiers to align with your organization's current maturity, operational goals, and desired level of hands-on assistance. Whether you are looking for a high-level assessment, strategic optimization guidance, or deeper implementation and automation support, each tier is designed to help maximize the effectiveness of your Identity Access Management investments.



Level 1: Identity Security Assessment

Evaluate your current Identity Access Management operating lifecycle and automation maturity with recommendations on areas for improvement.

Level 2: Identity Acceleration Program

Implementation of Identity Access Management solutions and processes, optimized for the organization's unique environment of PAM, IGA, CIAM, etc.

Level 3: Identity Operations Program

Ongoing guidance with tracking metrics and buildout of additional integrations across tooling and IAM roadmap programs.

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's organizations, people, and assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and—year after year—apply our cumulative learnings to continually strengthen the company's digital defenses.

ACHIEVED ACCREDITATIONS



ACHIEVED ASSESSOR

