



NORTH STAR IDENTITY

Your Trusted Partner to Navigate the Identity Journey.

Innovation | Leadership | Excellence

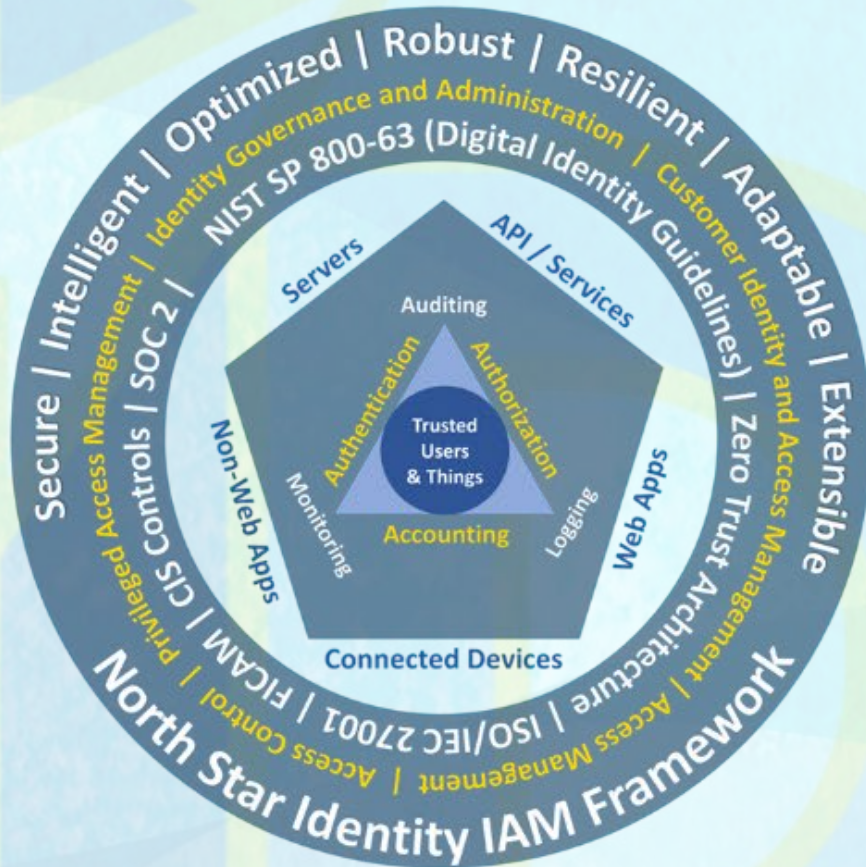


Cyber Security

Identity and Access Management (IAM)

Consulting Services

Strategy – Implementation – Managed Services



Protecting the digital identity of trusted Users and Things is the core objective of **North Star Identity Identity and Access Management (IAM) Framework**. Users — including employees, contractors, and customers and Things — like devices, applications, and systems, are central to IAM. Effective management of these entities is essential for securing organizational resources.

IAM focuses on key principles: authentication to verify identities, authorization to define access levels, and accounting to track activities. To ensure thoroughness, IAM incorporates auditing, logging, and monitoring for detailed oversight and real-time threat detection.

Advanced IAM services, such as Identity Governance and Administration (IGA), Privileged Access Management (PAM), and Access Management play a critical role in controlling access and managing identities. North Star Identity follows frameworks like NIST, SOC 2, and CIS to maintain strong security practices and compliance with industry standards.

Together, these elements form a comprehensive IAM infrastructure that protects resources, adapts to evolving threats, and upholds best practices in security and compliance.

“Identity is the digital fabric that enables seamless and trusted interaction across businesses, applications, and technologies, and ensures that trusted users and things, have access to the authorized information, from the right location, at the right time, using the right device, and for the right purpose.”

"Our mission is to enhance global security and trust by delivering innovative IAM solutions. We help organizations reduce costs, drive digital transformation, and strengthen their security posture, while improving compliance and efficiency across their people, processes, and technology."



OUR GUIDING PRINCIPLES

A. North Star Identity's principle is to provide seamless and secure access to all users for any resource, from any device, and from anywhere. We understand that in today's fast-paced digital world, the ability to access information and tools without barriers is crucial for productivity and innovation. Our services are designed to ensure that every user, regardless of location or device, can connect to the resources they need with the highest level of security. By leveraging advanced technologies and industry best practices, we enable a flexible, reliable, and secure environment that supports the evolving needs of modern businesses, ensuring that your workforce remains connected and protected at all times.

B. North Star Identity embraces generative AI in IAM — people, processes, and technology — as a cutting-edge approach to enhance security and efficiency. By leveraging AI, we can rapidly analyze vast amounts of data and identify anomalies in user access patterns much faster than traditional methods. This enables us to detect potential security threats in real-time, ensuring that only authorized users have access to critical resources. By integrating generative AI into our identity governance processes not only improves accuracy and speed in detecting risks but also empowers our clients with advanced tools to maintain robust security postures in an increasingly complex digital landscape.



C. North Star Identity is committed to delivering valuable and in-depth security posture for every asset as part of our comprehensive managed services. We provide a holistic view of access and identity management, ensuring that every user and system interaction is secure and properly governed. Our services also focus on maintaining strong security hygiene by regularly assessing and improving the health of your IT environment to prevent potential threats. By offering a unified and detailed perspective on access control, identity governance, and overall security hygiene, we enable you to proactively manage risks, ensure compliance, and sustain a robust security posture across all digital assets.

D. North Star Identity encourages a shift-left approach in IAM as a core principle and service offering. By integrating security measures early in the development process, we proactively address potential vulnerabilities before they become critical issues. This approach enhances the overall security posture and streamlines the implementation of IAM solutions, ensuring that security is not an afterthought but a built-in feature of every solution we deliver. Through this proactive strategy, we empower organizations to operate with confidence, knowing that their IAM processes are both comprehensive and resilient.



“Whether you are already on your identity journey or just beginning, North Star Identity will make it seamless with our Identity AI Solutions.”

Identity Governance and Administration (IGA)

- Source of Truth Integration
- Identity Life Cycle Management (LCM)
- Accelerated Application Onboarding Framework
- Business Rule-Based Access Control
- Automated Access Request Workflows
- Automated Provisioning and Deprovisioning
- Automated User and Privileged Access Reviews
- Preventive and Detective Segregation of Duty (SoD)
- IT Service Management Integration
- Identity Analytics and Reporting
- AI based Access Governance

Customer Identity and Access Management (CIAM)

- Self-Service Registration and Password Management
- User Experience and User Journey Workflows
- Privacy and Consent Management
- Social Identity Integration
- SaaS Integration - SAML, OIDC
- Reporting and Analytics
- Directory Integration
- Identity Proofing
- Identity Verification
- Behavior and Data Analytics

Strategy and Roadmap

- Identify Business Objectives
- Analyze Current state - Review people, process & technology stack
- Develop North Star architecture aligned with business objectives
- Identify Gaps - Security and Compliance, User experience, Operational efficiency
- Develop recommendations to fill the gap & develop future state implementation roadmap
- Analyze dependencies & identify high level timelines, and develop Roadmap
- Conduct Vendor and Product qualitative & quantitative analysis
- Develop Total Cost of Ownership (TCO)
- Develop Executive Summary with Business case based on the high priority initiatives

Zero Trust Access Management (ZAM)

- Web Access Management (WAM)
- Coarse Grained Authorization
- Passwordless Authentication - FIDO2, QR Code
- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)
- Adaptive, Risk-Based, Context-Aware Authentication
- Directory Services (DS)
- Virtual Directory Services (VDS)
- Biometrics

Privileged Access Management (PAM)

- Privileged Account Discovery and Inventory
- Password/Secrets Vault Management
- Privileged Account Governance and Compliance
- Privileged Access Session Monitoring and Recording
- Non-human Privileged Account Life Cycle Management
- CI/CD Integration

Dynamic Access Control (DAC)

- Access Control Strategy
- Access Control Governance Framework
- Risk Based Authorization
- Access Control Operating Model
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Policy Based Access Control (PBAC)

Emerging Identity Services (EIS)

- Self-Sovereign Identity
- IoT Gateway
- Fraud Prevention
- Cloud Infrastructure Entitlements Management (CIEM)
- SaaS Security Posture Management (SSPM)
- Cloud Security Posture Management (CSPM)
- Digital Asset Ownership Management (DAOM)



Online Brochure

Our Partners

