ANOMALIX

ANOMALIX
WHITE PAPER

Anomalix Strategy Services



Anomalix Strategy Services

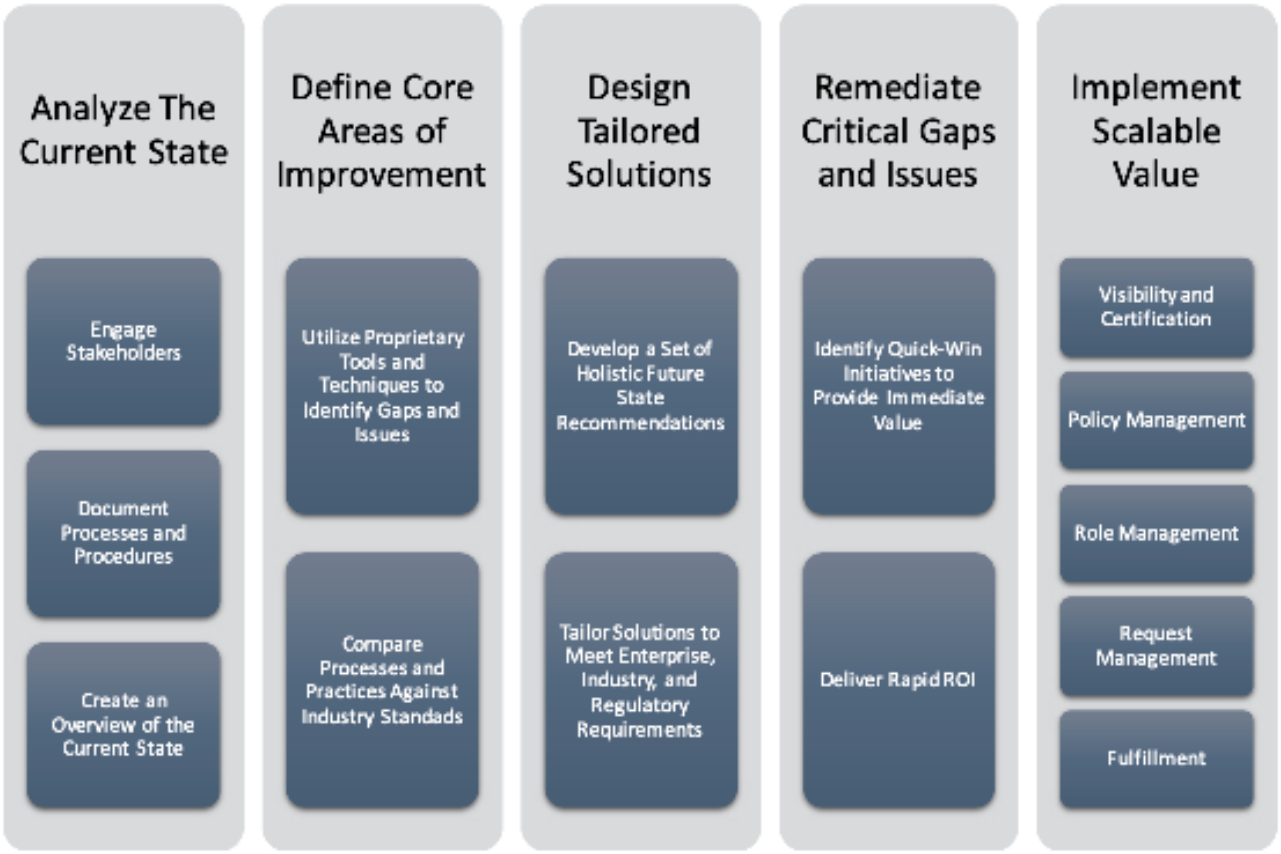
Professional Services Assessments are geared towards helping our clients with areas of cyber security, risk mitigation and compliance reporting. Anomalix solutions and services are rooted in deep subject-matter and domain expertise to address identify Cyber Security and Identity related challenges. Anomalix clients are of various sizes and in various stages of evaluating, building or overhauling a Cloud-First, Cyber Security or Identity and Data and Governance program.

Given the increased visibility and scrutiny of organizational security and compliance programs these days, it warrants an investment to insure that managers are implement solutions that incorporates business processes and compliance controls to effectively mitigate risk, enable the business and reduce operational costs and inefficiencies related to Identity and Access.

The Anomalix Cyber Security and Identity Risk Assessment can cover any or all of the following areas:

- Identity and Data Access Governance
- Identity Management Managed Service
- Business Process Architecture and Automation
- Audit Remediation
- Authoritative Identity Sources (Consolidation & Unification)
- Cloud and On-Premise Access Governance (Access Visibility & Attestation)
- Enterprise Access Request (Manage the User Experience, Enforce Policies, Apply Approvals and Orchestrate Fulfillment Changes)
- Entitlement Management
- Unstructured Data Governance (O365, File Share, SharePoint, Box, OpenDrive)
- Privileged Identity and Access Management
- Data Exfiltration
- Segregation of Duties Enforcement & Remediation
- Attribute-Driven Enterprise Roles (Strategy & Implementation)
- Active Directory Clean Up
- Single Sign-on (SSO)
- Risk-based Authentication
- Endpoint Protection
- Cloud DevOps
- Ransomware
- Network Behavior Monitoring
- Identity Analytics
- Security Analytics
- Anomaly Analytics That Drive Provisioning Changes (Detect Suspicious Behavior and Disable Access in Real Time)

Assessment Methodology



Analyze The Current State

- Interview key functional, business, and technical stakeholders
- Show what's working well for your organization and where improvements can be made
- Model current practices for access governance, provisioning, access request and approval, and fulfillment
- Document business-oriented rules for managing access that are currently in place
- Evaluate organizational goals for mitigating risk and gaining operational efficiencies

Define Core Areas of Improvement

- Utilize deep industry experience and proprietary techniques to identify gaps and issues
- Highlight findings with the greatest risk exposure
- Identify operational inefficiencies
- Compare your company's current processes and practices with industry standards and identify areas of improvement

Design Tailored Solutions

- Utilize findings from the assessment activities to develop a set of specific recommendations tailored to the organization
- Work with IT security, risk, compliance, business, and operations stakeholders to balance organizational priorities with assessment recommendations
- Ensure that recommendations with regulatory requirements including SOX, GLB, FFEIC, and HIPAA compliance

Remediate Critical Gaps and Issues

- Identify solutions for your company's most critical gaps and issues
- Find opportunities for quick-win initiatives while setting the foundation for long-term maturity
- Demonstrate rapid return on investment through increased operational efficiencies and reduced risk exposure

Implement Scalable Value

- Visibility and Certification – implementing solutions that provide visibility into user application, system, and data access
- Policy Management – set the stage for automated enforcement of enterprise security and user-access policies
- Role Management – utilize centralized user access information to design business-oriented roles, taking the confusion out of managing user entitlements
- Request Management – empower users to manage their own access while enforcing robust approval and request management processes
- Fulfillment – automating the processes of granting, updating, and removing user access to applications and systems. This reduces the risk of human error and allows people to focus on the core job activities

Implement Scalable Value

Johnson Financial Group selected Anomalix to provide Cyber Security, Identity Management and Access Governance expertise to address Business and Compliance mandates. Anomalix worked with JFG closely throughout the various stages of evaluating, building and overhauling a Cyber security and Identity and Data Governance program. Given the increased visibility and scrutiny of organizational security and compliance programs these days, it warrants an investment to ensure that managers are putting processes and controls in place to mitigate risk, enable the business and reduce operational costs and inefficiencies related to Identity and Access. Anomalix provided value across the following areas:

- Access Visibility to compliance relevant systems
- Business Process Architecture and Automation
- Automated Access Certifications
- Automated Active Directory Provisioning
- Reduced manual access administration for Joiners, Movers and Leavers by + 60%
- Closed-loop validation enables Audit reporting
- Reduce manual effort associated with access certification effort by +80%
- Increased inappropriate access revocations by 25%
- Improved overall compliance and audit posture



Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144