ANOMALIX

ANOMALIX

WHITE PAPER

Cyber Security and Identity Risk Assessment

Cyber Security and Identity Risk Assessment

Since 2013 Anomalix has partnered with leading F1000 companies in North America to identify and implement Identity focused cyber security solutions for the following areas:

- Identity Management
- Data Governance
- Privileged Access Management
- Risk-based Authentication
- Endpoint Protection and Network-Centric Dark Threat Detection

Our Professional Services Assessments are geared towards helping our clients with areas of cyber security, risk mitigation and compliance reporting. Anomalix offers solution and services provides deep subject-matter and domain expertise to address help 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
- Identity Analytics
- Endpoint Protection

- Cloud DevOps
- Ransomware
- Network Behavior Monitoring
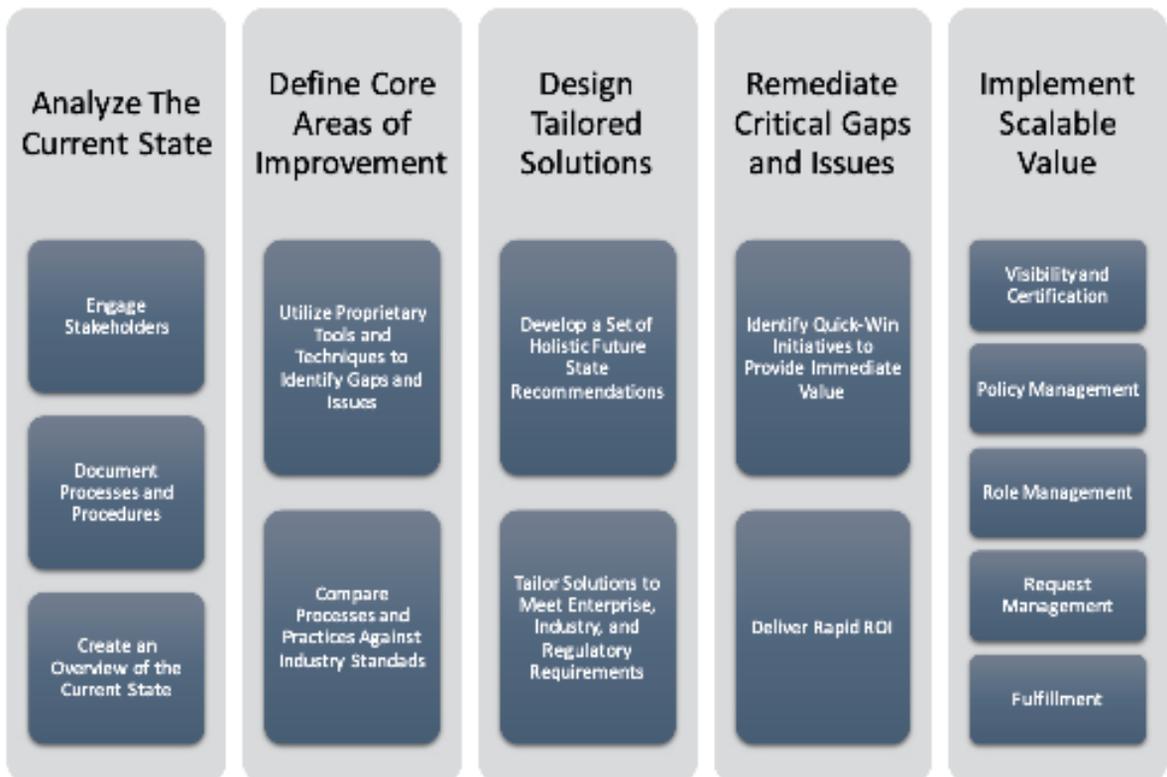- Anomaly Analytics That Drive Provisioning Changes (Detect Suspicious Behavior and Disable Access in Real Time)

Offering Overview

Anomalix utilizes decades of Cyber Security and Identity expertise to perform a thorough assessment with an actionable outcome. We work with our clients to develop custom-built assessments that will analyze the current state of their Cyber Security and Identity related products and practices in order to develop concrete recommendations and roadmap activities.

The assessments cover areas including:
- Cyber Security Program
- Identity and Access Management Program
- Joiner, Mover and Leaver Policies and Processes
- Data Access Governance
- Enforcement and Access Controls
- Identity Lifecycle Management
- Privileged Access Management
- Data Exfiltration

Our Assessment Methodology

Analyze The Current State	Define Core Areas of Improvement	Design Tailored Solutions	Remediate Critical Gaps and Issues	Implement Scalable Value
Engage Stakeholders	Utilize Proprietary Tools and Techniques to Identify Gaps and Issues	Develop a Set of Holistic Future State Recommendations	Identify Quick-Win Initiatives to Provide Immediate Value	Visibility and Certification
Document Processes and Procedures				Policy Management
				Role Management
Create an Overview of the Current State	Compare Processes and Practices Against Industry Standads	Tailor Solutions to Meet Enterprise, Industry, and Regulatory Requirements	Deliver Rapid ROI	Request Management
				Fulfillment

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, GDPR 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
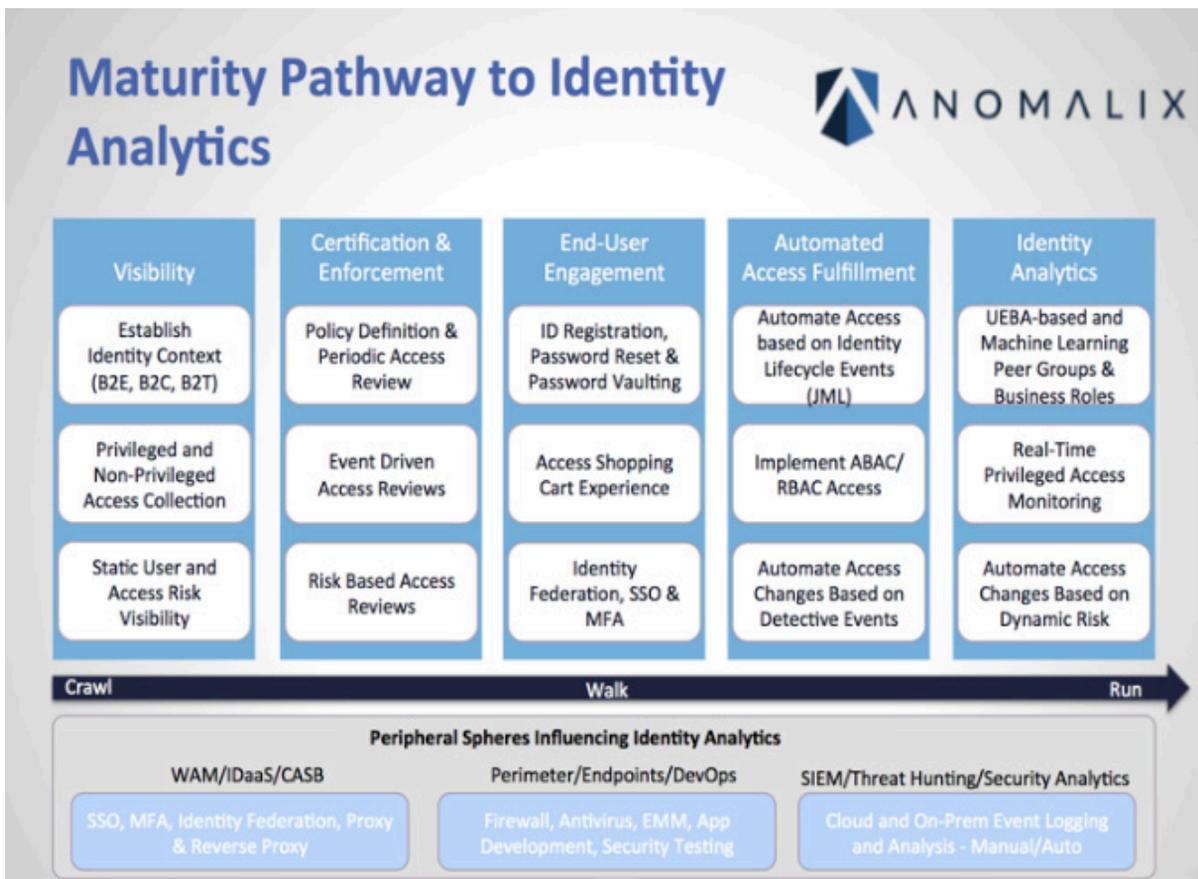
Implement Scalable Value
- Visibility and Certification – implementing solutions that provide visibility into user application, system, and data access
- Policy Management – set the stage for automated enforcement of enterprise security and user-access policies
- Endpoint and Network Protection – safeguard endpoints and monitor network behavior to identify attacks and dark threats such as Ransomware and Malware
- Role Management – utilize centralized user access information to design business-oriented roles, taking the confusion out of managing user entitlements
- Access Request Management – empower users to manage their own access while enforcing robust approval and request management processes
- Self-Service – how to empower end users to manage attributes and data they know best. Whether it's employees, customers or partners, end-users need flexible and immediate options for controlling credentials and updating profile information
- 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

Measurable and Actionable Outcomes

Must Have Capabilities

The Cyber Security and Identity Risk Assessment leverages an Industry Standard approach to achieve short-term and long-term security, risk and compliance objectives. The Anomalix formulated Identity Maturity Model highlights capabilities and functionality that allow organizations to have immediate protection while planning for compliance reporting, risk mitigation, business process automation and operational cost reductions.
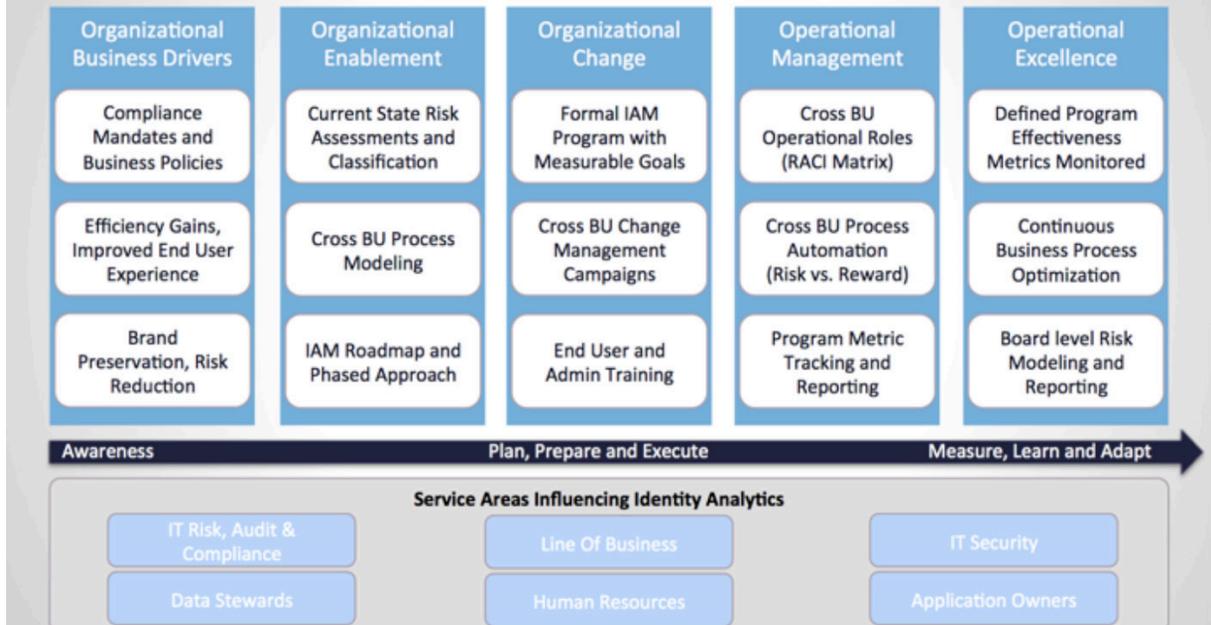
Conclusion

Operational Excellence

Anomalix will help identify what Security and Identity program activities can be effectively established or refined and how to build out a sustainable approach that impact many areas of the business and technology services.

Anomalix's Cyber Security and Identity Risk Assessment Deliverables include:

- An unbiased assessment of the current state of your Cyber Security, Identity Management and Data Governance practices at your organization
- Models of your current state Cybersecurity, Identity Management and Data Governance practices and architecture and   processes
- A short and long-term roadmap with prioritized recommendations
- Advice on potential remediation solutions as well as how Anomalix can help achieve your goals

ANOMALIX

Third-Party Identity Management in a Decentralized World