Anomalix Health Check for RSA SecurID Identity Governance and Lifecycle

ANOMALIX

RSA and Anomalix Inc. – Partnership Background and SecurID (G&L) Health Check Overview

Since 2014, Anomalix has been RSA's first certified go-to-market partner for Identity Management (Access, Governance and Lifecycle). With over 25 trained and certified billable SecurID consultants, Anomalix can point to numerous successful deployments of RSA SecurID Identity Governance & Lifecycle that have yielded triple-digit returns (ROI) for our clients. In 2016, Anomalix partnered with Microsoft and is currently a certified Microsoft Cloud Solution Provider (MCSP) and has announced RSA SecurID (Governance & Lifecycle) as managed services. Anomalix also offers expert Advisory and Implementation services. Anomalix offers deep subject matter expertise for any Identity Management initiative that encompasses process, products and personnel required to be successful.

As RSA SecurID G&L customers continue to invest and expand compliance and provisioning capabilities, pausing briefly between production rollouts to gauge project success and operational efficiency gains can yield tremendous returns and continued project success. Are the business and technical merits of the initial investments paying off? Are there opportunities to optimize TCO and ROI?

Anomalix's RSA SecurID G&L Health Check deliverable is an actionable report identifying issues and opportunities with respect RSA SecurID Governance & Lifecycle Version 6.x & 7.x clients.

Health Check Deliverable Reports will identify opportunities to gain incremental value on existing RSA SecurID Governance & Lifecycle investments including:

- Technical stability
- Operational Efficiency
- Operational Risk Management
- Operational Maturity
- Governance, Risk, and Compliance Maturity

IAM Program Health Check

- Establish a current state snapshot of the IAM program.
- Determine the long-term goals of the IAM program.
- Compare the current state against the long-term IAM Program goals and utilize the Anomalix Identity Maturity Model to provide course correction steps and create a roadmap to reach long-term goals.

Anomalix Analytics at Work

Anomalix uses its vast Identity and Access Management experience and proprietary tools to analyze the client systems and perform an in-depth health check. The data from these Health Check activities is compiled into actionable items and a roadmap to help guide the client to Identity and Access Management maturity.

IAM Project Health Check

- Analyze project scope to make sure it aligns with the long-term IAM program goals. Identify and review any parts of project scope that do not align
- Determine if the project scope and success criteria were well defined at the start of the project and whether that criteria have been satisfied.
- Determine whether original project goals, business drivers and initial motives for investment were fulfilled.
- Determine if the implementation methodology has been followed.
- Determine if project requirements were documented, signed off and followed.
- Identify business and technical challenges and/or delays being faced.
- Identify resource related issues.
- Identify product specific issues.
- Identify environment related issues.

Compliance Health Check

- Define compliance requirements and review existing processes.
- Review existing Identity and Application Collection and Visibility.
- Define current Provisioning capabilities
- Document existing Approval Processes and potential gaps.
- Review current User Access Review capabilities.
- Review existing definitions of Data Risk and Sensitivity.
- Determine whether Policy Enforcement (Detective vs. Preventative) is in place.
- Determine current Role definition maturity and usage.
- Review use of Reporting for compliance-related activities.
- Determine whether Privileged Access has been defined and is being sufficiently managed.

Infrastructure Health Check

- Review and document physical and logical architecture
- Confirm Software versions and patching are up to date
- Review security settings
- Check CPU and disk utilization
- Determine if monitoring is in place for the major components of RSA SecurID G&L.
- Verify that regular backups of the RSA SecurID G&L environment exist
- Identify the development/change process for RSA SecurID G&L

Archer & SecurID L&G Integration Health Check

- Review and document the integration architecture
- Confirm that the software versions and patching are up to date
- Determine if all the critical business applications have been identified
- Determine if controls are in place to mitigate risk
- Determine if the access approval workflows and review cycles are dynamic or static
- Determine if all the business owners for critical applications are engaged
- Determine if the Risk levels (High/Low/Medium) have been defined for the applications and entitlements
- Determine if a financial threat is posed by risky applications
- Determine if targeted policies and controls have been defined in Archer and properly enforced in SecurID L&G
- Determine if continuous monitoring of access to high risk applications and failed controls is in place
- Determine if proper controls are in place to mitigate orphan and dormant accounts
- Determine if access to Archer is monitored through review campaigns

www.anomalix.com
info@anomalix.com
222 Merchandise Mart Plaza, Suite 1212, Chicago, IL 60645
800.939.6491