RSA® IDENTITY GOVERNANCE & LIFECYCLE

CYBERARK VISIBILITY AND GOVERNANCE IMPLEMENTATION BLUEPRINT

AT-A-GLANCE:

A simple, packaged solution, which RSA Professional Services have created to reduce implementation time and cost. This solution follows RSA's recommended practices.

Why?
- Reduce the application and audit risk for CyberArk and your privileged accounts
- Lower administration costs regarding CyberArk authorisation management
- Streamline user authorisation requests and processes within CyberArk (e.g. Leavers)

What?
- Provide governance capabilities and lifecycle automation for CyberArk
- Gain visibility and control of privileged user data and access permissions

How?
- Automate the privileged user provisioning process based on groups, policies and approval workflows
- Provide user access reviews for privileged users
- Simple to use access request forms for CyberArk

SUPPORTED VERSIONS*

This has been validated to work on:
- RSA IGL v7x
- CyberArk v9.3 and above

**Please always check and confirm, as this solution may have been updated since this was created*

OVERVIEW:

Together, CyberArk and RSA Identity Governance and Lifecycle (RSA G&L) deliver an enhanced privileged identity and access governance solution that allows centralised management and control, of all identities, both privileged and non-privileged, to quickly detect and mitigate access risks, which ensuring continuous compliance.

This Implementation Blue will help the business to quickly detect security and compliance access risks and amend access entitlements issues associated with privileged users

Closed loop validation and user access reviews will help the business to get their environment under control, with clear visibility around who has access to what.

KEY FEATURES & BENEFITS:

This implementation blueprint provides the following benefits:

- Enhanced visibility and control of privileged accounts and access data, directly within RSA G&L
- Ensures privileged users are granted appropriate access permissions based on similar privileged users attributes (e.g. Roles or job function) and in accordance with the organizations access policies
- Reduces the attack surface and enhances regulatory compliance by limiting access privileges and deactivating stale/orphan privileged accounts.
- Identify key users with segregation of duties violation that pose serious risks.

For more details, please contact your local RSA Sales representative or RSA Solution Principle.