SOLUTION BRIEF

RSA Archer® Cybersecurity Framework Management App-Pack

Challenge

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, which places national security, the economy and public safety at risk. The National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**) was created to provide government agencies and private sector organizations with standards and best practices in managing cybersecurity risks in the nation's critical infrastructure. With the May 2017 signing of the **U.S. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**, which holds government agencies and owners and operators of critical infrastructure in the U.S. accountable for managing cybersecurity risks, NIST CSF has become even more widely adopted by all types of organizations across the U.S. and around the world.

RSA Archer Cybersecurity framework management

The **RSA Archer® Cybersecurity Framework Management** app-pack is designed to help critical infrastructure-related organizations manage cybersecurity framework requirements based on NIST CSF guidance. Offered via the new and improved RSA Exchange via RSA Link, this offering provides your organization with the methodology to assess and measure your cybersecurity posture, address gaps and report on cybersecurity in a meaningful way that is understood by all of your key stakeholders.

RSA Archer Cybersecurity Framework Management enables profile owners to catalog the current state, prioritize and scope profile eleme nts, and define their desired or targeted state outcomes for the organization's cybersecurity program. Assessors can then evaluate these profiles against the NIST CSF categories. Previous assessments can be archived for comparison with a Current Profile and measure progress. Reports and dashboards provide clear insight into the cybersecurity current state and progress being made toward the desired cybersecurity state.

Key features

- Prioritize and scope the organization's business objectives and priorities
- Create a Current Profile that indicates progress being made toward target outcomes
- Risk assess the operational environment and identify the likelihood and impact of a cybersecurity event
- Identify a Target Profile that describes the organization's desired cybersecurity outcomes
- Analyze the Current Profile against the Target Profile to determine gaps
- Implement an Action Plan to identify necessary steps to remediate gaps

Key benefits

- Concise methodology allows organizations to understand how their cybersecurity efforts stack up relative to NIST's guidance
- Common language ensures clear communication of requirements and progress across all stakeholders, including the IT security team, management, partners, contractors, suppliers and others
- Application of NIST CSF principles and risk management best practices improves cybersecurity and resiliency of critical infrastructure, regardless of organization size or level of cybersecurity sophistication
- Designed to assist government and critical infrastructure entities manage cybersecurity requirements in keeping with the U.S. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Prerequisites

For a full list of applications, use cases and prerequisite dependencies for this offering, please review the **Implementation Guide** for the RSA Archer Cybersecurity Framework Management app-pack on RSA Link.

REQUIRED RSA ARCHER APPLICATIONS:

- Business Units
- Business Processes
- Applications
- Devices
- Authoritative Sources

REQUIRED RSA ARCHER PLATFORM VERSION:

RSA Archer Cybersecurity Framework Management was developed for and validated on RSA Archer Platform Release 6.2 Patch 3+.

REQUIRED RSA ARCHER ON-DEMAND APPLICATION (ODA) LICENSES:

RSA Archer Cybersecurity Framework Management requires three (3) RSA Archer On-Demand Application (ODA) licenses.