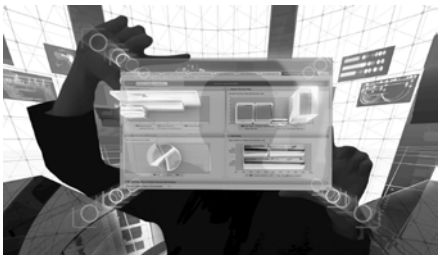
RSA ARCHER® ASSESSMENT & AUTHORIZATION

Comply with FISMA while improving security



AT-A-GLANCE

- Easily manage all phases of NIST risk management framework (RMF)
- Vastly improve risk insight through meaningful , current metrics from any tier of the organization
- Incorporate current risk metrics into FISMA reports and authorization artifacts
- Save money and labor hours through consolidation and streamlining
- Integrate with Continuous Monitoring (CM) and other essential RSA Archer solutions

CHALLENGES

A federal Information Assurance (IA) professional has many challenges. FISMA (Federal Information Security Management Act) compliance in itself is a large challenge, even before factoring in federal budget constraints, new cyber threats, and new compliance requirements (CyberScope requirements, FedRAMP, revisions to NIST 800-53 and unique agency directives). There is an additional challenge trying to integrate real operational security data into compliance activities.

SOLUTION

The RSA Archer Assessment & Authorization (A&A) solution is an ideal foundation for a comprehensive RSA Archer-based IA Management suite. It serves as the system of record for every person, location, component, and tier in your organization, as well as every piece of hardware and software and every information asset. IT assets can be assigned into Information System boundaries for A&A and FISMA compliance and reporting. The A&A solution manages the full cycle of NIST RMF (800-37) activities. It integrates seamlessly with the RSA Archer Continuous Monitoring solution and maximizes existing agency infrastructure investments. Many other RSA Archer GRC solutions can be integrated with the A&A solution to tie Incident Management or Contingency Planning to specific Information Systems for more contextual tracking and reporting.

KEY BENEFITS

- Easy management of all phases of NIST RMF with high integrity and rigid, role-based access enforcement
- Deep risk insight and metrics can be rolled up from end user through each component level to department and federal levels
- Effective common control management maximizes the ability to leverage assessments without permitting abuse
- Streamlined assessments through Monitoring Strategy application and notifications which aid in building assessment plans and with manual continuous assessments
- More powerful and configurable dashboards and reports than other A&A tools
- Integrates with other RSA Archer solutions focused on operational security (Incident Management, Vendor Management, and Contingency Planning)
- Guaranteed common format and interoperability among RSA Archer solutions to preclude the need to reformat, re-enter, or transform data feeds, reports, or documents between tools
- Deployed agency IT infrastructure tools support agency A&A and CM requirements

KEY FUNCTIONALITY

– ***Define assets and information systems***

Serves as the system of record for all hardware, software, and information assets. These assets are uniquely tied to Information System boundaries for A&A (formerly known as Certification & Accreditation (C&A)). Relationships are easily built between assets and the stakeholders and organizational components that own the assets.

– ***Manage control assessments and compliance, including common controls***

Efficiently tailor the control set and manage common controls (inheritance) through a two-way handshake to prevent abuse. Each control has a unique record for holding the history of implementation details and assessment findings, including risk impacts and scoring associated with each control.

– ***Create and track workflows and approvals around risk decisions***

Create and internally manage approvals for several types of risk decisions. These include creating and tracking of POA&Ms (plan of action and milestones), RBDs (risk-based decisions), and SDLC (system development life cycle)-phase approvals like pre-assessment review, authorization (ATO) decision, and decommissioning.

– ***Integrate with continuous monitoring and other essential RSA Archer solutions***

Adding RSA Archer Contingency Planning, Incident Management, or Vendor & Supply Chain Management will automatically tie the incidents and contingency tests to the Information Systems and organizational components defined in the A&A solution. Because RSA Archer solutions are built on the same platform, they are interoperable and share data easily, out of the box.

– ***Reports and dashboards***

Broad range of reports and dashboards out of the box can be easily customized to meet unique agency needs. Quickly and easily create custom reports. Assign them to a dashboard for many format options (bar/pie chart, heat map, scatter chart). All RSA Archer solutions are equipped with highly configurable, real-time reports and dashboards.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption and key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading GRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.