RSA® ARCHER® PUBLIC SECTOR SOLUTIONS

Solution Brief

INTRODUCTION

Federal information assurance (IA) professionals face many challenges. A barrage of new requirements and threats, a need for better risk insight, silos imposed by people and technologies, and a shortage of resources create a complex environment for IA teams. FISMA (Federal Information Security Management Act) compliance in itself is a significant challenge, even before factoring in federal budget constraints, new cyber threats, and new compliance requirements. The additional challenge of trying to integrate real operational security data into compliance activities complicates these efforts further.

Risk insight is another enormous challenge. Applying cookie-cutter processes and controls to every asset results in under or over protection, typically at great expense. To avoid this, the federal community has grasped the importance of making risk-based decisions and risk-based spending. Security management tools can determine how many patches are missing or how many vulnerabilities are present, but very few provide real business context. As a result, risk decisions are made at a management level without the full risk picture, and security administrators do not know which findings or deficiencies to fix first.

Compliance with OMB (Office of Management & Budget) memo and circulars, and the assessment and authorization (A&A) required by FISMA, costs the federal government billions of dollars per year. The current IA paradigm is tremendously expensive. The added factors of funding dramas and continuing resolutions over the past few years have hurt the probability that IA budgets can adequately accommodate the tools, staffing and training to meet current and future challenges.

Finally, siloes can exist within the federal community – at large, individual departments and even the workflows of a single office. From both inter-organizational and intra-organizational perspectives, disparity and redundancy occur in tools, processes, standards, data, and language.

ALIGN SECURITY, COMPLIANCE AND RISK MANAGEMENT INTO ONE PROCESS

Establishing a central repository for risk and control related data is the first step in ensuring you have an accurate and comprehensive view of risk that can be readily conveyed to all stakeholders. You must break down data and communication silos between tools and people. You must then exploit this streamlined data flow to save time, increase data sharing, and make more informed risk decisions. Use of common tools and processes allows you to track and manage FISMA and OMB compliance requirements and leverage assessment data for reuse, including GAO (Government Accountability Office) and other audits. Integrating automated and manual continuous monitoring tools will satisfy federal compliance requirements, and will also drive faster defect remediation, reduce actual risk, and provide complete risk metrics which are always current.

THE RSA ARCHER PUBLIC SECTOR SOLUTIONS ADVANTAGE

RSA® Archer® Public Sector solutions are purpose-built to meet the unique needs of U.S. federal agencies, providing capabilities essential for effective information

assurance program management and maximizing existing agency infrastructure investments.

Harness the Power of Convergence

With a common platform, common taxonomy, and integrations to scanners, sensors, and other security tools, IA teams can collect and share data in a common environment. This infrastructure eliminates the need to constantly import, export, and reformat data, breaking down silos and allowing your stakeholders to share information faster and easier. In addition, information sharing provides a broader view and for stakeholders to make the right risk decisions to reduce risk and ensure compliance.

Your Security Program's Path to Maturity

You need to accommodate a wide spectrum of maturity levels and to push your security program forward on its maturity path. For many years, FISMA only required a set of Certification and Accreditation (C&A, now A&A) artifacts. RSA Archer Public Sector solutions produce not only A&A artifacts, but could enhance companion solutions to enable Contingency Planning, Continuous Monitoring, and third party and supply chain management. This integrated approach pushes the organization to manage more security functions in a more informed, more efficient way.

Leverage True Agility

Unlike most of the solutions that the public sector currently uses, RSA Archer is not hard coded into one rigid use case. Applications, workflows, and reports and dashboards can be quickly reconfigured to adjust to changes in your internal policies or processes. As federal guidance or your program changes, the solution can be modified to ensure your processes are appropriately aligned.

RSA ARCHER PUBLIC SECTOR SOLUTIONS

RSA Archer Public Sector solutions allow you to leverage people, process, and technology to build an integrated approach to Assessment & Authorization, Continuous Monitoring and overall risk management. In addition to solving IA challenges, RSA Archer Public Sector solutions can also provide significant ROI by saving labor hours, reducing software license and training costs, increasing productivity, reducing risks and incidents, and bringing the IA organization into an improved, common culture through improved data sharing and the use of a common taxonomy and workflow.

Assessment & Authorization

With RSA Archer Assessment & Authorization, you can assess and authorize all new information systems before they go into production to ensure they are operating at an acceptable level of risk. RSA Archer gives the authorization team the ability to define authorization boundaries, allocate and assess controls, assemble authorization packages, make informed authorization decisions, and determine whether each information system stays within acceptable risk parameters. RSA Archer Assessment & Authorization allows organizations to comply with FISMA and OMB requirements while improving overall security and controls. It also integrates with RSA Archer Continuous Monitoring to provide a true ongoing authorization (OA) capability.

RSA Archer Assessment & Authorization enables more efficient identification, management, and mitigation of issues, including common (inherited) control management. This means enabling current staff to do more with less pain. Reports and authorization artifacts are automatically updated. Additional context and more current data mean improved compliance, visibility, and security.

Continuous Monitoring

RSA Archer Continuous Monitoring serves as a hub for many types of scanner and sensors, allowing the organization to build an aggregate risk view at any level of the enterprise. Individual defects can be monitored and scored. Defects are aggregated at each level of the hierarchy, from the individual device up to the Department level. Through this aggregation, a risk score can be designated at any layer and the amount of relative risk introduced can be measured. The reporting and workflow allows limited resources to be focused on the remediation efforts that will provide the greatest benefit.

RSA

With RSA Archer Continuous Monitoring, you can make a faster, more targeted response to emerging risks. Your staff will be able to mitigate the findings in the order in which they will reduce risk most. When used in tandem with RSA Archer Assessment and Authorization, it can enhance your FISMA and OMB compliance activities by verifying that information systems are abiding by authorization agreements (ATO) and are operating within acceptable levels of risk. This translates to a more secure environment with more insight and the ability to make better, more informed risk decisions.

Plan of Action & Milestones Management

RSA Archer Plan of Action and Milestones (POA&M) Management allows you to centralize findings and defects and then track the remediation effort into dates, milestones and costs. The use case also provides the capability to route POA&Ms through formal approval and review processes and capture performance management and cost metrics.

CONCLUSION

With RSA Archer Public Sector solutions, you can exceed the minimum Assessment & Authorization and Continuous Monitoring requirements set by FISMA and OMB and improve the maturity and efficiency of your security program. Breaking down silos with RSA Archer's integrated platform and solutions will improve communication and visibility. The flexible and configurable nature of the RSA Archer platform, as well as the path left open to integrate with other RSA Archer solutions, means your security program can continue to adapt and mature in the future.