SOLUTION BRIEF

RSA ARCHER® PUBLIC SECTOR SOLUTIONS

INTRODUCTION

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. Compliance is a significant challenge, even before factoring in agency budget constraints, new cyber threats, and new and increasing 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 underprotection or overprotection, typically at great expense. To avoid this, the public sector 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 mission 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 Office of Management & Budget (OMB) memos and circulars, as well as assessment and authorization (A&A) required by the Federal Information Security Management Act (FISMA), costs the government billions of dollars per year. The current IA paradigm is tremendously expensive, and the added factors of funding 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, silos can exist within the public sector community—at large, individual departments and even workflows for 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 IN 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 better informed risk decisions. Use of common tools and processes allows you to track and manage FISMA, OMB and other compliance requirements and leverage assessment data for reuse, including Government Accountability Office (GAO) and other audits. Integrating automated and manual continuous monitoring tools will satisfy compliance requirements, drive faster defect remediation, reduce actual risk and provide complete, current risk metrics.

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.

THE RSA ARCHER® PUBLIC SECTOR SOLUTIONS ADVANTAGE

RSA Archer Public Sector Solutions are purpose-built to meet the unique needs of the public sector, providing capabilities essential for effective information assurance program management and maximizing existing agency infrastructure investments.

HARNESS THE POWER OF CONVERGENCE

Armed with a common platform and taxonomy, and integrations with scanners, sensors and other security tools, IA teams can collect and share data in a collaborative environment. This infrastructure eliminates the need to constantly import, export and reformat data, breaking down silos and making it faster and easier for stakeholders to share information. Information sharing provides stakeholders with a broader view to make the informed risk-based decisions to reduce risk and ensure compliance.

THE PATH TO MATURITY FOR YOUR SECURITY PROGRAM

For many years, FISMA was considered a checkbox process that required a set of Certification and Accreditation (C&A, now A&A) artifacts and would be reviewed at least every three years. Recently, OMB has directed agencies to continuously monitor their systems to ensure that they are operating within its approved security posture. RSA Archer Public Sector Solutions produce A&A artifacts that 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 and continuously monitor security functions in a more informed and efficient way.

LEVERAGE TRUE AGILITY

Unlike most solutions currently used within the public sector, RSA Archer is not hardcoded as 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 regulations, guidance or programs change, 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 and authorization, continuous monitoring, plan of action and milestones (POA&M) management, and overall risk management. In addition to solving IA challenges, RSA Archer Public Sector Solutions can also provide significant return on investment 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. It gives your 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 your organization to comply with FISMA and OMB requirements while improving overall security and controls. It also integrates with RSA Archer Continuous Monitoring to provide true ongoing authorization (OA) capabilities.

RSA Archer Assessment & Authorization enables more efficient identification, management and mitigation of issues, including common (inherited) control management, allowing 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 scanners and sensors, allowing you to build an aggregate risk view at any level of your organization. Individual defects can be monitored and scored. With defects aggregated at each level of the hierarchy, from the individual device up to the department level, a risk score can be designated at any layer and the amount of relative risk introduced can be measured. Reporting and workflow allow limited resources to be focused on remediation efforts that provide the greatest benefit.

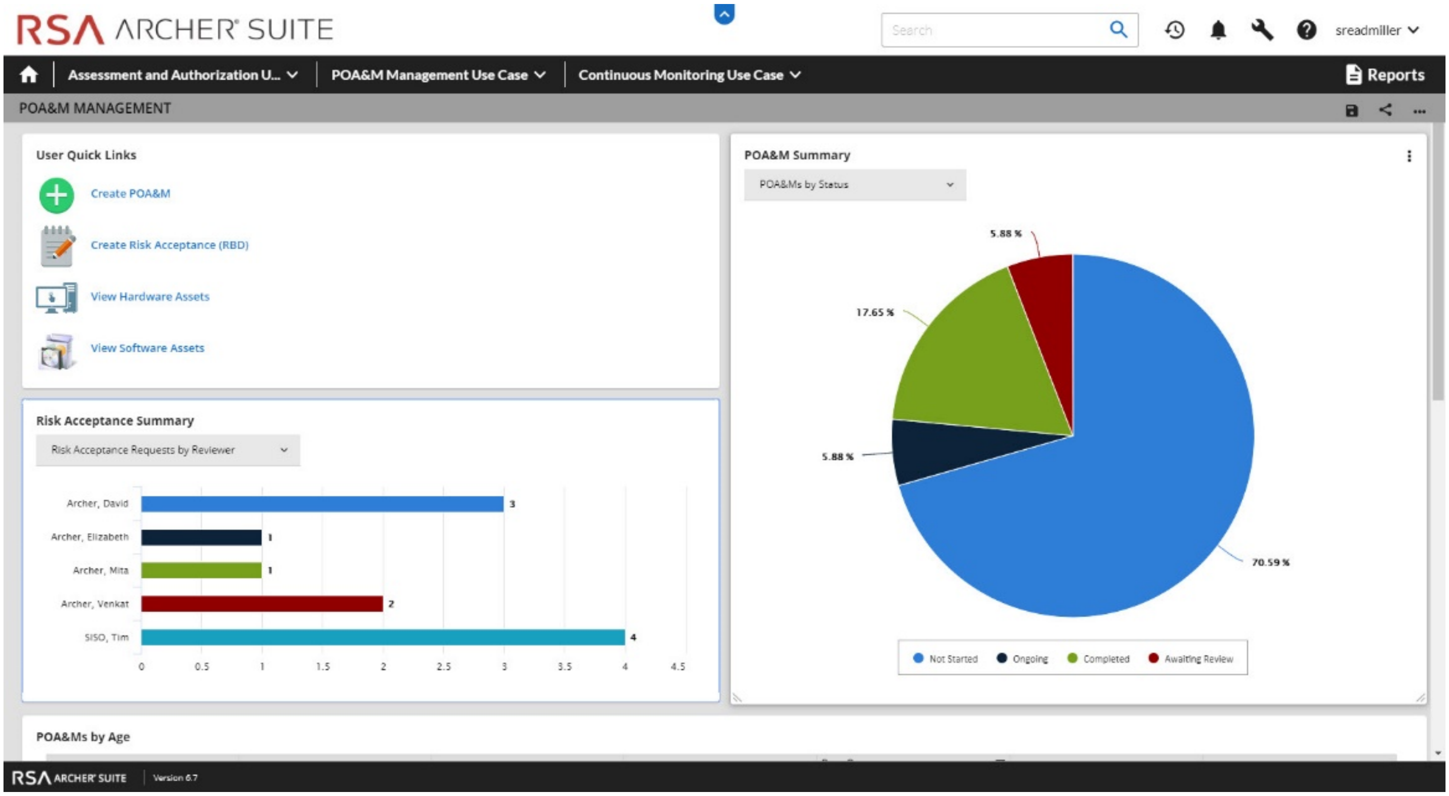
With RSA Archer Continuous Monitoring, you can enable faster, more targeted response to emerging risks. Your staff can mitigate findings in the order in which they will most reduce risk. When used in tandem with RSA Archer Assessment and Authorization, it can enhance your FISMA and OMB compliance activities by verifying that information systems are abiding by authorization agreements 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 & Milestones (POA&M) Management allows you to centralize findings and defects and then track the remediation effort into dates, milestones and costs. It also provides the capability to route POA&Ms through formal approval and review processes and capture performance management and cost metrics.

CONCLUSION

RSA Archer Public Sector Solutions allow you to exceed the minimum assessment and authorization and continuous monitoring requirements set by FISMA and OMB and improve the maturity and efficiency of your IA program. Using RSA Archer Suite, you can break down silos to improve communication and visibility. The flexible and configurable nature of the RSA Archer platform, as well as integration with other RSA Archer Solutions, means you can continue to adapt and mature your IA program as your needs and requirements change.



ABOUT RSA

RSA offers mission-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce mission risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com/publicsector.

©2020 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 09/20, Solution Brief, H15122-2 W386667.