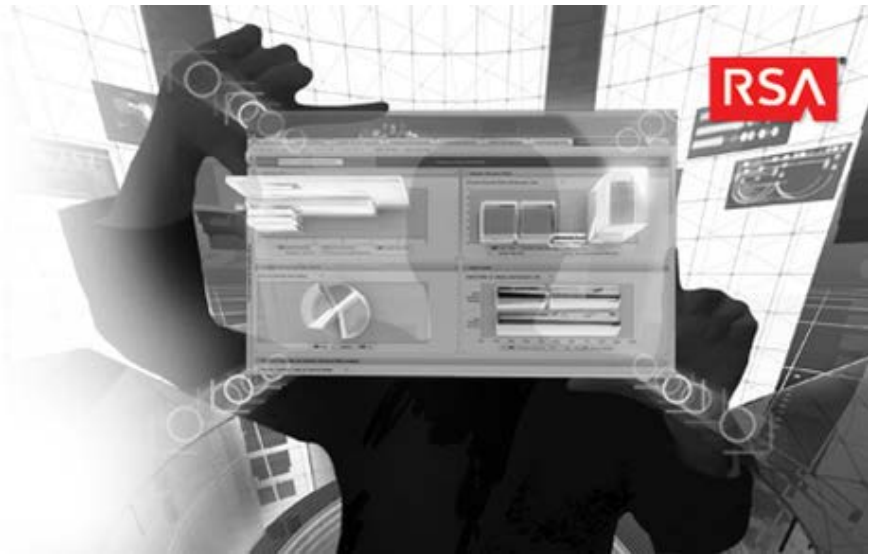
ENHANCE ROI WITH RSA ARCHER® FEDERAL SOLUTIONS



ABSTRACT

This paper illustrates the major challenges faced by today's Federal Information Assurance professional, and enumerates solutions that RSA Archer provides for each of those challenges. Finally, the ROI for each of the proposed solutions is identified for prospective customers.

Audience - This paper is intended for Information Assurance stakeholders and practitioners in the federal space. This includes government employees in the military, intelligence, and civilian communities and integrators, consultants, and contractors supporting those communities.

Authors: Chris Hoover, Raj Meel

June 2013

EMC WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION 3

CHALLENGES 3

- New Requirements Require Agile Response 3
- Cyber Threats Require New Response Strategy 3
- Current Tools Lack Deep Risk Insight 4
- Stovepipes / Silos Severely Limit Efficiency 4
- Need To Do More With Less Resources 5

SOLVE WITH PURPOSE-BUILT RSA ARCHER FEDERAL SOLUTIONS 6

- Solving the "New Requirements" Challenge 6
  - Continuous Monitoring 6
  - NIST SP 800-53 Rev 4 6
  - CNSSI 1253 / DIARMF Support 7
  - FedRAMP Support 7
- Solving the Threats Challenge 7
- Solving the Risk Insight Challenge 7
- Solving the Stovepipes / Silos Challenge 7

THE ROI OF USING RSA ARCHER 9

CONCLUSION 10

CONTACT US 10

INTRODUCTION

This paper illustrates the major challenges faced by today's Federal Information Assurance professional, and enumerates solutions that RSA Archer provides for each of those challenges. Finally, the paper discusses ROI implications to an organization using RSA Archer's Federal solutions. This will be covered in three sections.

- Challenges
- Solving the challenges with RSA Archer
- ROI of using RSA Archer

CHALLENGES

New Requirements Require Agile Response

One challenge facing the federal Information Assurance (IA) professional is the constant barrage of new requirements. As soon as you begin to implement and manage the last set of requirements, a new set is introduced. The tools, resources, and support infrastructure available to you dictate how well you can respond to these new requirements and how agile you can be. In 2013, the new requirements (or new *emphasis* on existing requirements) that present the biggest challenges will be:

- Implementing Continuous Monitoring
- Switching to 800-53 Rev 4
- Department Of Defense (DoD) switching to National Institute of Standards and Technology (NIST) / CNSSI 1253 / DIARMF
- Federal Risk and Authorization Management Program (FedRAMP)
- Supply Chain Management

Continuous Monitoring (CM) is a challenge for many reasons. Many departments/agencies are waiting for more definition about what needs to be monitored, how often, and what methods to use. Many organizations do not understand what tools they will need or if their current tool sets will support CM. There is also a resource problem, which will be covered below.

NIST SP 800-53, Revision 4 presents challenges, like every new revision does. First, there is the logistical aspect of how to get all current Information Systems reassessed and reauthorized over time to the new control set. Every new revision of 800-53 introduces dozens of new controls. So, there is the burden of understanding and implementing those, including an entire new family of controls for privacy. NIST also introduces the concept of overlays in the new revision. This concept will affect how controls are allocated and tailored.

Department Of Defense (DoD) is expected to switch from DoD Information Assurance Certification and Accreditation Process (DIACAP) to an Assessment & Authorization (A&A) methodology aligned with NIST RMF and using CNSSI 1253. This will be a significant source of stress considering the fundamental level of change, including different nomenclature, different method for categorizing systems, and a different control catalog.

FedRAMP is the cloud A&A initiative that has been around for several years, but will only really begin to take off in 2013. FedRAMP is intended to reduce waste and save money, but it is a new process and there is some ambiguity about how it will work. For this reason alone, it is a cause of significant anxiety. Add to that the fact that only one cloud environment has made it through the Authorization To Operate (ATO) process, and FedRAMP starts to appear quite challenging. Perhaps worst of all, FedRAMP has its own templates and controls which are not supported by first-generation A&A tools.

Supply chain management is a hot topic recently. Threats to the supply chain are valid and significant. NIST has even issued an interagency report (NIST IR 7622) to cover the subject. The difference between understanding and implementing a new requirement, however, is enormous. Managing risk to the supply chain effectively and to the level defined by NIST is overwhelming. There is a current shortage of tools capable of managing the supply chain, especially tools that can integrate this process with other IA and risk management processes.

Cyber Threats Require New Response Strategy

Cyber threats are a constant challenge in the federal space. New threats are being introduced and discovered faster than ever. There are threat feeds to help identify cyber threats, but there are many disparate and inconsistent threat feed providers, and integrating them all can be a challenge. Mapping cyber threats to a remediation process can be a challenge. New threats require

new responses, and can dictate the implementation of new methods, new processes, and new tools. Not every threat can be addressed at once, and knowing how to rank them can be nerve-wracking. It only takes one serious threat to seriously impact an enterprise or a mission.

Current Tools Lack Deep Risk Insight

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

Stovepipes / Silos Severely Limit Efficiency

Stovepipes or silos exist within the federal community at large, within individual departments, and even within the workflows of one office. This is a significant challenge every federal IA professional faces. From both an inter-organizational and *intra*-organizational perspective, disparity and redundancy occur in:

- Tools
- Processes
- Standards
- Data
- Language

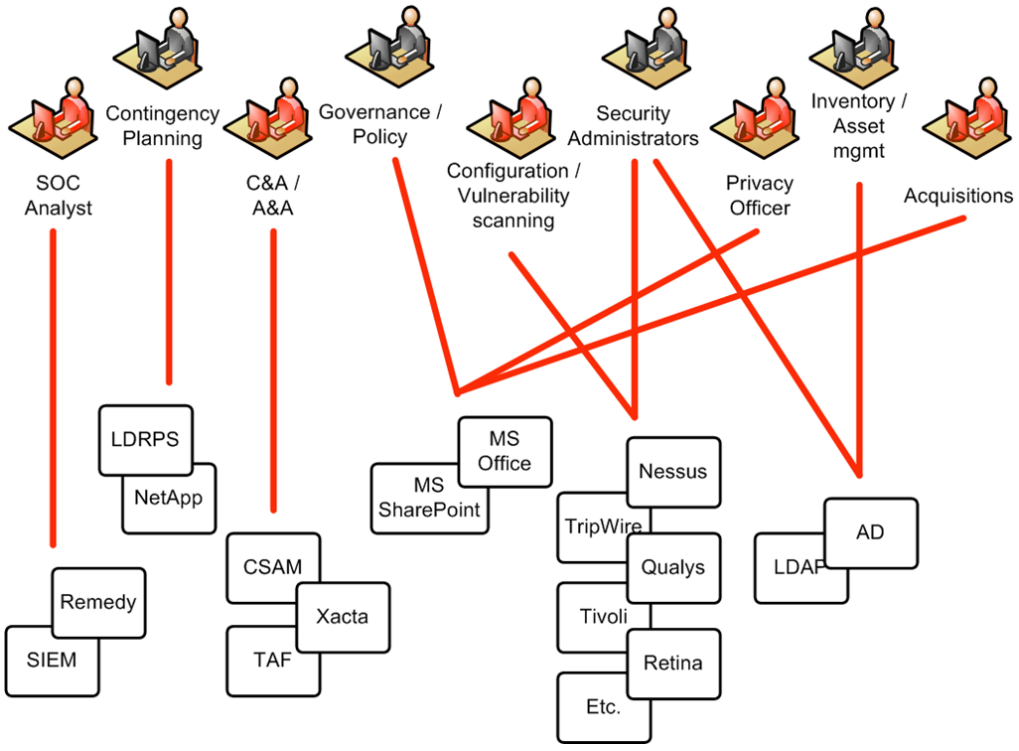


Figure 1 – Current Information Assurance (IA) Process

Consider the figure above. Collectively, the people depicted are implementing and enforcing an IA program. The data covered in the diagram covers the domain of IA management data, but look where each stakeholder gets their data and where they put it. This is another example of stovepipes/silos that is common. The SOC Analyst uses one tool to create and manage incidents. The Contingency Planning team uses a separate tool. The A&A team uses still another. The rest of the stakeholders are creating Microsoft Office documents and posting them in various file servers or in different areas within SharePoint.

This is an example of a bad scenario because a large number of disparate tools lead to:

- Duplicate work
- Conflicting records
- Problems with common format / interoperability
- Greater cost in licenses
- Greater cost and burden for training
- More accounts to manage
- More “attack surface”

Need To Do More With Less Resources

The last (but likely most significant) challenge is one of resources. A&A and compliance auditing required by the Federal Information Security Management Act (FISMA) costs the federal government several billion dollars per year. Since enactment of FISMA in 2002, the federal government has spent over $40 billion. The current IA paradigm is already enormously expensive. Now, factor in the debt crisis, several fiscal cliff events over the past few years, and the recent Sequester. These hurt the probability that IA budgets will increase enough to provide the tools, staff, training, etc. to meet current and future challenges.

Continuous Monitoring, for example, means assessing and monitoring more controls, more often. Because of the current fiscal climate, however, this may need to be done with the same staff as before! This is the quintessential example of “do more with less.”

SOLVE WITH PURPOSE-BUILT RSA ARCHER FEDERAL SOLUTIONS

Solving the "New Requirements" Challenge

Continuous Monitoring

RSA Archer enables Continuous Monitoring in several ways.

First, RSA Archer provides a monitoring dashboard environment which can be used to drive rapid risk improvement and to inspire competition between system owners and administrators. This dashboard provides "worst first" risk scoring by ranking the risk scores by host, information system, and organization.

In addition, the CM solution accommodates CAESARS FE model by allowing more complex scoring, analysis, and hierarchical data roll-up. RSA Archer makes this possible through effective integration with common security tools, sensors, and scanners such as vulnerability and configurations scanners, management servers, and SIEMs. Data integrations can be made using SCAP, traditional XML, API, RSS, and data imports.

The RSA Archer CM solution allows for automated control assessment. Even though most of the controls in 800-53 are not automatable, RSA Archer is able to handle this. RSA Archer allows for the definition of a monitoring strategy, including keeping track of control assessments that are manual or automated, and the frequency at which each control needs to be assessed. The monitoring strategy is managed in a simple matrix. The matrix is automatically integrated into the System Security Plan (SSP), and automatically sends notifications to assessors for manual control assessments when they are due.

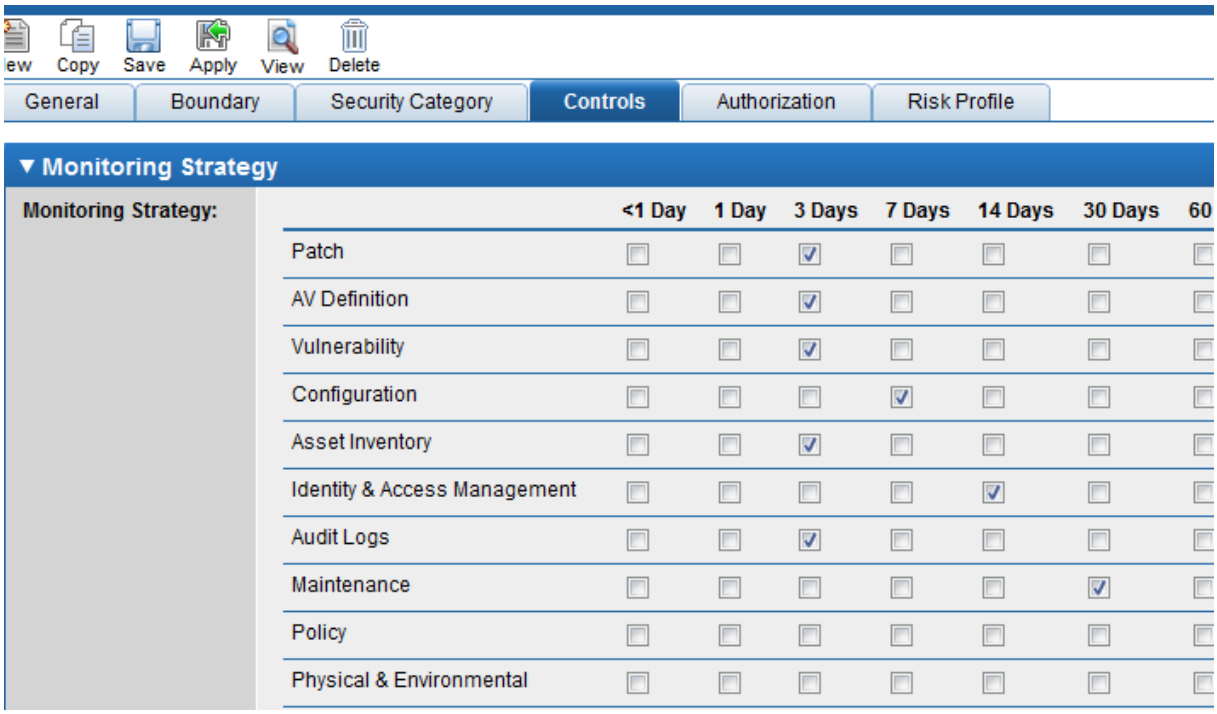


Figure 2 – Monitoring Strategy

NIST SP 800-53 Rev 4

RSA Archer customers benefit from an ongoing content-development process. New content such as policies, standards, and other authoritative sources are consumed into RSA Archer as they become available. For example, RSA Archer currently contains FIPS, NIST SP 800 series, and DoD 8500 series documents in its content library. RSA Archer accommodates multiple control catalogs, so migrating between revisions of 800-53 is not a problem. Lastly, overlays will be supported in the control allocation and control tailoring workflows within the A&A solution.

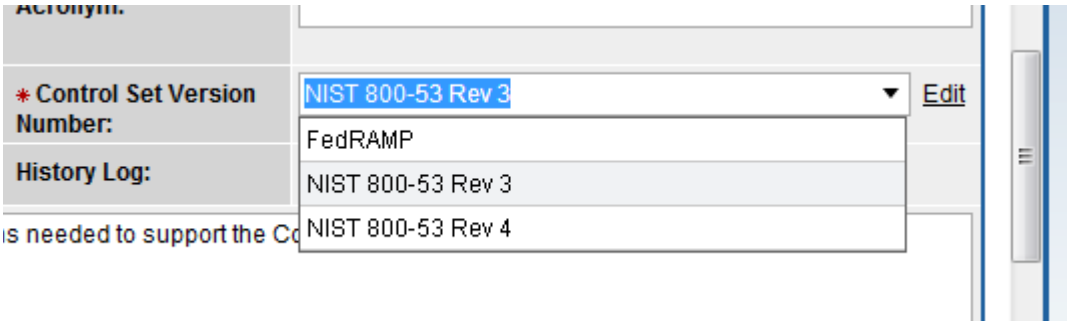


Figure 3 – Control Sets

CNSSI 1253 / DIARMF Support

Since DIARMF is based on NIST RMF, the A&A solution can also be used for DoD systems. Archer accommodates the CNSSI 1253 method of categorization and control allocation.

FedRAMP Support

Similarly, since FedRAMP is also based on NIST RMF, the A&A solution can be used for FedRAMP cloud systems. By simply selecting the FedRAMP control set (as in the figure above), the RSA Archer A&A solution becomes a FedRAMP A&A solution, including a specially formatted FedRAMP SSP.

Solving the Threats Challenge

RSA Archer has a mature Threat Management module. The threat module accepts live threat feeds from multiple sources. The threat module "speaks" multiple SCAP specifications and ranks threats by severity. It also manages reports on threat remediation activities, which can be tied to specific hosts, information systems, and organizational components for scoring and reporting.

Solving the Risk Insight Challenge

RSA Archer enables IA stakeholders to make better risk decisions on many levels. RSA Archer correlates multiple risk scores and risk factors across the enterprise and IA Program for a comprehensive risk picture. The Risk Management module allows for the creation of NIST SP 800-30-based Risk Assessments. The CM module highlights which hosts and which failed controls introduce most risk for rapid, "worst first" resolution. Custom reports and dashboards are extremely easy to configure and can be used, for example, to match risk scores to costs, for true risk-based spending. Consider the report below.

POA&M ID ▲	POA&M Status	Estimated Start Date	Estimated Cost	Control Number	Control Name	Residual Risk Score ▼
POAM-6	Ongoing	1/30/2013	$ 400,000.00	CM-08	Information System Component Inventory	332
POAM-7	Delayed	1/23/2013	$ 30,000.00	AC-02(01)	Account Management	272
POAM-8	Delayed		$ 10,000.00	PS-06	Access Agreements	272

Figure 4 – Risk-Based Spending

This is an example of a report that compares the risk metric introduced by a finding/failed control with the cost of the associated POA&M. Note the risk scores are only *incrementally* different, but the first POA&M costs *exponentially* more to fix. In a scenario where there are not enough resources to fund the remediation of every open item, this context is invaluable in informing an organization as to where they should be spent. This is true risk-based spending.

Solving the Stovepipes / Silos Challenge

RSA Archer can bridge and eliminate stovepipes /silos in several ways. It can eliminate other tools through consolidation. One of RSA Archer's trademark strengths is in policy and control mapping, which allows support for multiple methodologies / frameworks. This means many teams, missions, and processes can be "brought under one roof." The common use of one tool fosters common language and forces the use of a single data set. The tools selected below in grey can be consolidated into RSA Archer.

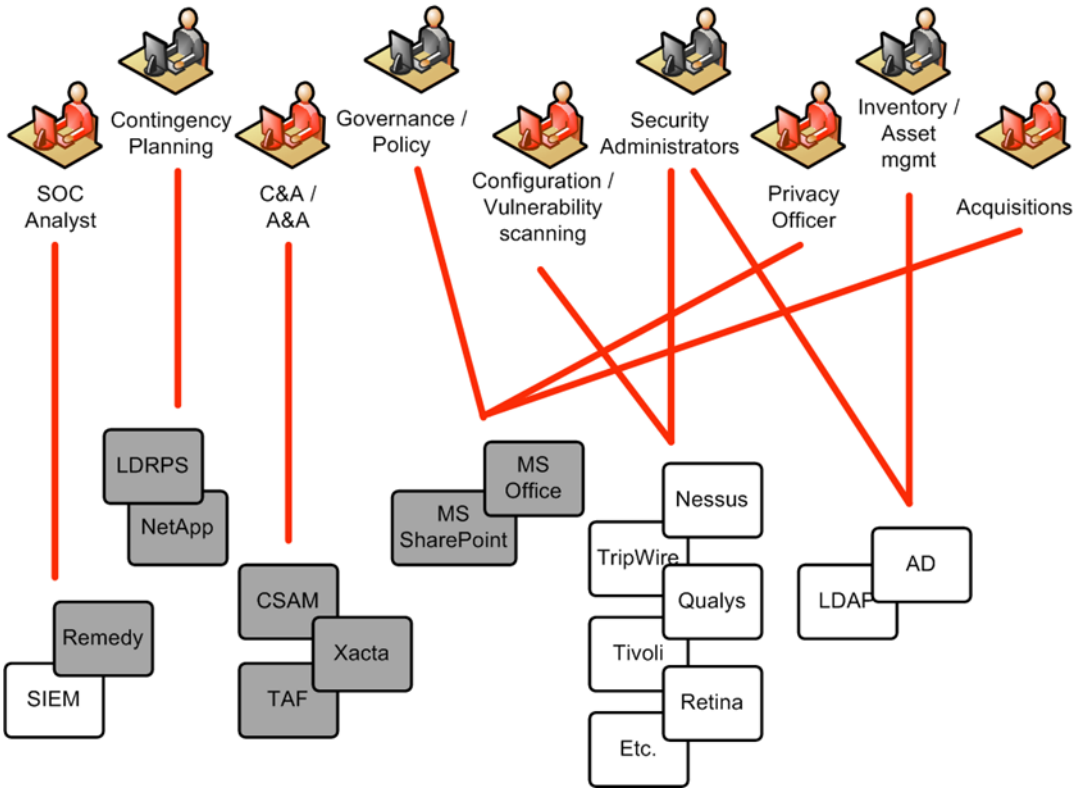


Figure 5 – Candidates for Consolidation

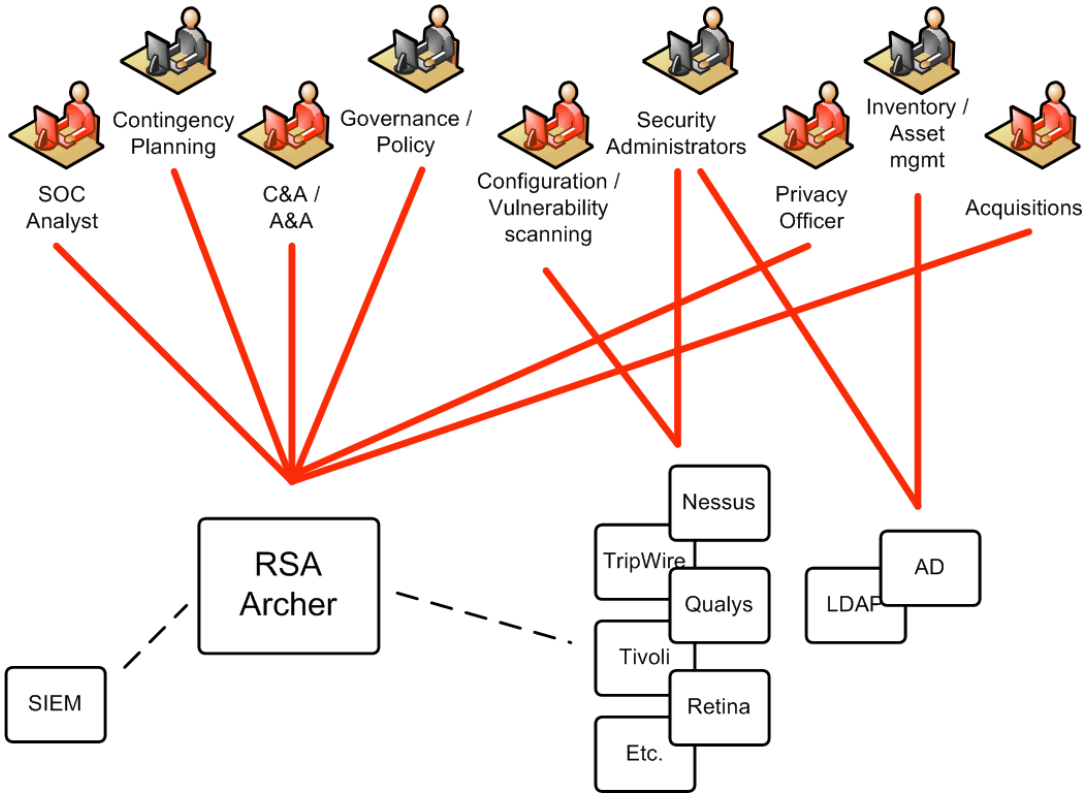


Figure 6 – Consolidate with RSA Archer

THE ROI OF USING RSA ARCHER

Having defined the Federal IA challenges and seen how RSA Archer can be used to solve them, it is time to see the real ROI of using RSA Archer to manage an Information Assurance program.

	Summary	ROI Benefit
1	RSA Archer's range of options for integrating sensors and tools increases the chances you can use your existing tools for CM, or replace fewer of them at the least.	Save tool replacement cost.
2	Automated assessments save time and money as compared to manual assessments.	Save resource cost and achieve higher productivity.
3	CM increases insight to risk by providing more current security data, which translates to better security and fewer incidents. Incidents have a tangible cost in dollars and intangible costs to reputation, trust, exposed data, and personnel safety.	Save security incident management cost.
4	The monitoring strategy matrix and notifications make it possible to plan and manage the ongoing manual assessments of hundreds of controls per information system at an appropriate risk-based frequency, which again translates to better security and fewer incidents.	Automation and higher productivity.
5	The notifications sent by the monitoring strategy matrix also provide the control assessors with the ability to update their assessment plans and know which controls to assess on which days. This is a force multiplier for the assessment team, saving them significant time and effort. In most organizations, the assessors are the most expensive facet of the A&A process.	Save assessment cost.
6	The ability to leverage more and duplicate less means less data entry and less time writing narratives and editing/peer reviewing narratives.	Derive efficiency from existing resources.
7	Working from a common set of data enforces data integrity, which translates to lower risk of data corruption/loss and less time checking and recreating data. This saves labor hours and prevents data loss.	Avoid duplicate effort, achieve higher productivity.
8	The guaranteed common format and interoperability among RSA Archer solutions precludes the need to reformat, re-enter, or transform data feeds, reports, or documents between tools. This results in big savings in labor hours.	Save labor cost.
9	Reducing the number of tools through consolidation within RSA Archer provides several cost benefits. • Lower cost associated with software licenses. • Lower cost associated with providing software training for multiple tools. • Less training burden on the individual results in new hires being productive faster. • Fewer accounts to manage and a smaller overall attack surface as a result of having fewer tools. This saves labor hours and also reduces security risk.	Save costs with software licenses and training. Save future costs by reducing overall security risk.
10	The modular nature of RSA Archer means buy what you need, as you can afford it. This saves money versus buying more than you need. In addition, you don't have to wait for the next funding cycle to have features you can use now.	Maximize use of budget dollars.

11	Streamlining A&A workflow and consolidating data and processes in one tool translates to fewer labor hours.	Save labor cost.
12	Furthermore, all of the labor-hour savings mentioned above allow for Continuous Monitoring assessment of more controls, more often, with the same staff (in light of budget and hiring constraints/ CR /Sequester).	Significant automation benefits.

CONCLUSION

The federal IA professional faces many challenges: a barrage of new requirements and threats, a need for better risk insight, artificial boundaries imposed by cultures and technologies, and a shortage of resources. RSA Archer has the potential to not only solve the IA challenges but also provide a 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.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com.