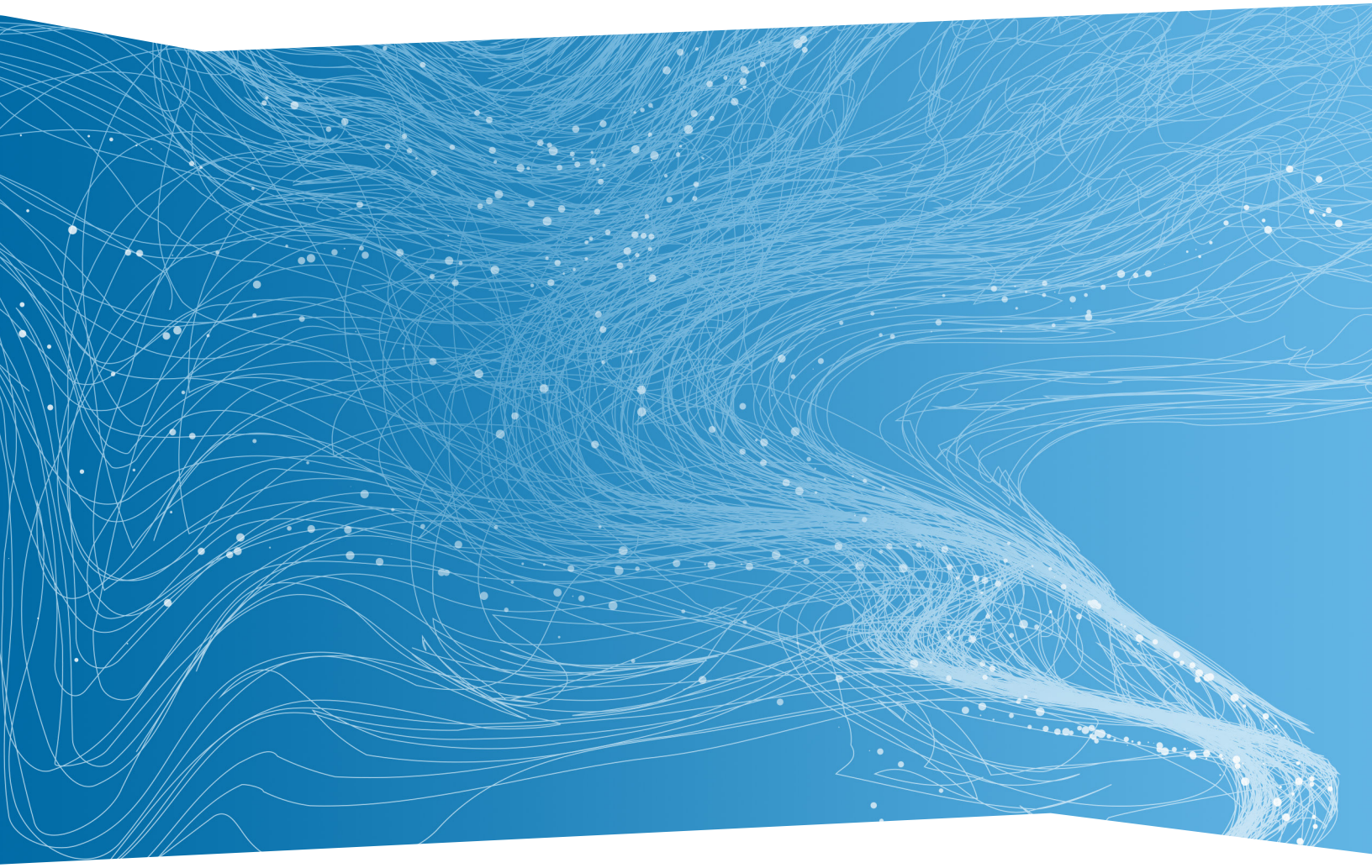
RSA



WHITE PAPER

RSA ARCHER® MATURITY MODEL: ASSESSMENT & AUTHORIZATION & CONTINUOUS MONITORING

RSA

OVERVIEW

Federal organizations and the federal vendor community face a litany of compliance hurdles and threats to their IT assets. Managing an effective Information Assurance (IA) program today requires a mixture of technology controls, effective and efficient processes and skilled, informed people. The RSA Archer Maturity Model for Assessment & Authorization (A&A) and Continuous Monitoring (CM) outlines RSA Archer's role in the critical stages in an organization's journey from reactive, compliance-driven processes to a risk-centric, opportunity-focused security program that is a competitive advantage to fuel the enterprise.

CONTENTS

RSA

WHY ASSESSMENT & AUTHORIZATION AND CONTINUOUS MONITORING?

Federal IA professionals face many challenges, whether they are federal employees or support contractors. Federal Information Security Management Act (FISMA) compliance is a large challenge in itself, even before factoring in federal budget constraints, new cyber threats and new compliance requirements, including Cyberscope requirements, moving to the cloud and using FedRAMP, revisions to NIST 800-53 and unique Department/agency directives.

When federal information systems are first put into operation, they have to get through the gating process of A&A to ensure they are operating at an acceptable level of risk. Following this costly, resource-intensive process, there are several challenges to monitor those systems to ensure changes are documented and evaluated for risk, security control assessments are updated regularly, and real operational security metrics are represented in the compliance activities.

Continuous monitoring is an idea that has been around for years, but has been mandated only recently. Most organizations have not begun to implement it, and those that have are in the beginning stages. Therefore, there are very few examples to point to and the written guidance can be vague. This leaves many organizations wondering how to implement the CM process, which tools to use, as well as what to monitor and how often. In addition, the cyber threat landscape is constantly changing, many of the available tools are inadequate, and many Departments/agencies are often late in responding to the latest security threats.

The sum of these challenges for federal IA professionals is how to make things more secure, using more stringent standards, while staying out of trouble from a compliance and reporting perspective, with the same amount of resources and staff? Each federal organization must learn how to operate their A&A and CM programs more efficiently. Part of this efficiency is a need for better tools and processes and part is a need for better risk insight. A more mature and nuanced understanding of risk enables the finite resources of the IA program to be focused where they are most needed with the greatest efficiency.

KEY CAPABILITIES

RSA Archer GRC Maturity Models focus on key capabilities enabled by the RSA Archer solution. As a technology enabler, RSA Archer provides the critical infrastructure to leverage processes, share data and establish common taxonomies and methodologies.

All organizations face similar security challenges and IA represents a significant 'cost of doing business'. Those organizations that can execute efficiently and effectively can reduce efforts and costs. In addition, with better security processes in place, the organization has the safety net to pursue and exploit new opportunities such as adopting new technologies or expanding missions and providing new services.

When a security executive, like the Chief Information Security Officer (CISO) or Authorizing Official (AO), looks at putting together the picture of IT security risk, it requires multiple dimensions and operational groups to collaborate and coordinate efforts.

- Security policies, procedures, and control catalogs must be aligned to regulatory and mission requirements

- Authorization boundaries must be defined and authoritative. The contents of each boundary must be categorized by criticality and sensitivity and with regard to the missions it supports.
- Security administrators need to implement security controls, system owners need to document the implementations, and assessors need to assess them.
- Security managers and risk officials need to be able to interpret the amount of risk each asset and each defect introduces, and blend many streams of security data and metrics into a cohesive risk picture to decide on remediation plans and priorities, or whether or not to allow a particular system to operate.
- A CM strategy must be defined and implemented to ensure that systems operating at an acceptable level of risk continue to do so.

To achieve these goals, RSA Archer's A&A and CM solutions focus on the following key capabilities:

Categorize assets and information systems
Define authorization boundaries, down to the individual hardware and software component, in a way that is scalable from one to many thousands, and can sync with asset management tools and scanners to stay current, accurate and authoritative.

When the boundaries are defined, use many contextual elements to accurately define the security category. These contextual elements can include information types used in the system, risk assessment results, privacy assessments and interconnections, and missions and business processes supported.

Select and implement controls
Provide the ability to allocate the appropriate baseline of security controls, tailor the controls and apply overlays to arrive at the most appropriate final control set for each authorization package. This applies to several control catalogs and A&A methodologies (NIST RMF, DOD RMF, FedRAMP).

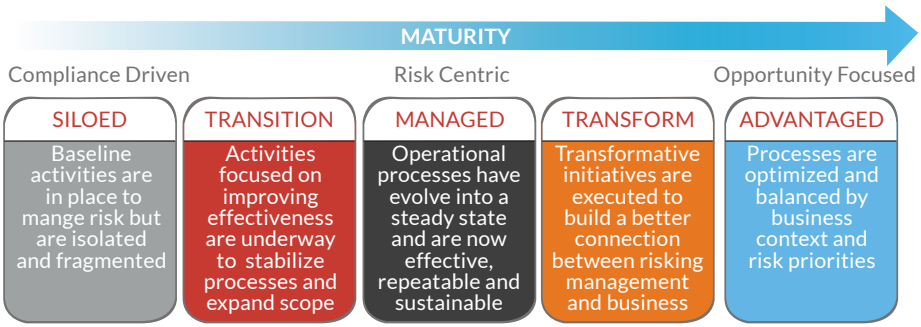
Analyze risk and authorize
Provide an array of reports, A&A artifacts and current CM metrics to enable the AO and other stakeholders to fully understand the risk posture of each information system. Provide a means to efficiently route and approve/disapprove authorization requests, as well as tracking POA&Ms, exception requests and Authorization to Operate (ATO) expiration dates.

Implement continuous monitoring and ongoing authorization
Provide the means to define the CM monitoring strategy and schedule and streamline the performance of both automated and manual assessments. Integrate assessment results into current risk reports and update A&A documentation automatically. Evolve into the Ongoing Authorization phase,

where A&A and CM are synthesized and risk metrics can augment or replace ATO dates.

THE MATURITY JOURNEY

RSA Archer Maturity Models are segmented into five major stages: Siloed, Transition, Managed, Transform and Advantaged.



The RSA Archer Maturity Model is designed to be pragmatic and implementable. Elimination of the "Level 0" that typical Maturity Models include avoids the unnecessary definition of a stage of maturity that will not meet today's security challenges.

- The **Siloed stage** focuses on baseline activities that all organizations need to manage risk.
- The **Managed stage** is intended to depict the phase that organizations reach a coordinated, sustainable security program.
- The **Transition stage** and **Transform stage** help the organization "turn the corner" with initiatives that evolve critical capabilities and set the stage for advanced capabilities.
- The **Advantaged stage** is designed to be achievable for most organizations, allowing the organization to target an advanced stage of maturity that optimizes security programs.

The RSA Archer Maturity Model for Assessment Authorization and Continuous Monitoring focuses on building these capabilities over time by implementing the broad strategy with tactical, intelligently designed processes.

FOUNDATIONS

Foundations are critical elements necessary for the overall success of the Maturity Journey. Without these foundations in place, the organization will face difficulties throughout the journey either through the lack of focus, commitment, resources or strategy.

- **Management commitment** – The degree and level of leadership commitment to IT security risk management culture, strategy and priorities

- **Performance and acceptable risk** - Defined levels of performance and acceptable risk for IT Security.
- **Expectations and measurement** - Clear expectations and success criteria defined for the IT Security program.
- **Stakeholder involvement** – Importance of improvement and maturity of IT security risk processes to your stakeholders and business constituents.
- **Budget and resources** – Sufficient resources for IT security risk management program to achieve success.

THE SILOED STAGE: IMPLEMENTING THE BASICS

The organization in the Siloed stage is fulfilling its requirements, but often at a minimal level and with maximum pain and effort to the staff involved. They perform basic security reporting and minimum FISMA compliance reporting. Their efforts are compliance-driven, striving to stay out of trouble and just ahead of the next batch of compliance reports.

They use many specialized tools and have admins with specialized training, but this knowledge and context is segmented, hence the name of this maturity level. For example, technical security reporting is oriented around technical attributes only (IP addresses, server names, etc.). Little to no detail of how the technical device is used within the business is utilized in managing, prioritizing or describing technical security issues. This lack of cross-domain data sharing is partly due to the culture and partly due to limitations in their tools.

Compliance efforts are reactive and just-in-time. If an ATO is expiring next month, that is the system that gets the most attention. If a group of POAMs is expiring next week, the same applies. Even if it is obvious that the ATO or POAMs that are expiring are not the most critical, they have the greatest potential to hurt compliance reporting scores and invite unwanted scrutiny.

The Siloed organization is likely to be a revision behind on the control catalog they use. They perform fundamental defect identification and remediation, but infrequent reassessment of systems with current ATOs. They often have no in-house assessment talent, and so deal with constant budget issues and can only plan for external assessor costs for the next one or two assessments in advance.

THE TRANSITION STAGE: BUILDING CONTEXT FOR THE FUTURE

The organization that wants to move through the Transition level is seeking better integration, efficiency and visibility. One goal at this level is to push for better integration of tools, data and processes.

Communication between stakeholders is an important theme at this level overall. Integration between tools also breaks down information silos.

RSA

This type of communication and integration could, for example, lead from using only information types to decide a security category to also including other contextual data, like mission and business context, interconnections and privacy assessments. This provides more assurance that the right category was chosen, which has enormous downstream impacts.

Another goal at this level is to redesign processes or replace tools to better enable assessment result reuse or more effective common control inheritance. This will provide time and resource savings that can be used to mature another area of the program.

Finally, better visibility is important at the Transition level. Visibility is a by-product of the communication and integration already mentioned, but it also creates a positive loop. The visibility gained can point out more opportunities to do further integrations or to further improve the leveraging of assessment results. All goals of this level feed each other.

THE MANAGED STAGE: OPERATIONALLY SOUND

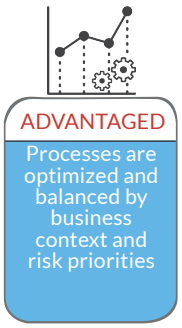
The Managed level organization is beginning to reach a new plateau of stability. They are bringing their staff out of old painful and inefficient habits. As their processes are more defined, they become more objective and repeatable.

Greater visibility means that justifications, metrics and context begin to infiltrate decision making. With greater assurance in this visibility, the organization is better able to tailor their control sets or change their assessment frequencies or methods. The organization can now decide to allocate fewer controls to lower impact information systems or tailor controls to a lower level of rigor or perform assessments less often. It is the new visibility and risk insight that allows the organization to defend such decisions with confidence. The time and resources gained back could be reallocated to assets that need more protection. Rather than asking "which ATO or POAM is expiring next?" as in the Siloed stage, attention is now focused on "which system is at greatest risk right now?"

A stable and informed A&A program will also foster improvements in common control management, which will alleviate control assessment costs and provide additional security.

An organization in the Managed stage will also begin to use time and resource gains to ensure that an ATO is maintained after it has been issued. All changes go through a control board and the responsible stakeholder(s) ensure that A&A artifacts will kept current. If a person who performs a change documents it right away, it is much less painful and time-consuming and more accurate than someone trying to devise what happened a year later when the ATO is expiring. This forward-thinking efficiency is foreign to the Siloed organization, and part of why their job is so painful.

RSA



Business context (relationship between IT and Business assets) is added to vulnerability scan data to provide IT administrators with prioritization guidance.

THE TRANSFORM STAGE: PRIORITIZATION AND CONTROL

The Transform stage for today's federal organization is very simple. In the context of A&A and CM, the Transform stage is laying the foundation to get away from static or infrequent control assessments. In other words, CM is implemented in earnest, including both manual and automated assessments. This ultimately means getting away from the ATO expiration paradigm. The organization at this level is focused on developing a CM strategy, including tying an appropriate assessment frequency and methods to every control of every system. They are also exploring ways to leverage more automated security assessments.

THE ADVANTAGED STAGE: OPTIMIZED FOR RISK MANAGEMENT

In the Advantaged stage, business context has been infused in security processes and technologies. Security issues are reported on at macro and micro levels with integrated business attributes and impact.

Findings resulting from compliance processes are reconciled back to policies, standards and procedures to identify and address underlying systemic issues. Compliance is providing a key feedback loop into the design and operating environments for controls. Policy exceptions are used as a leading indicator to identify misaligned or ineffective policies. Instead of just fixing and closing POAMs, a root cause analysis is performed to see if similar findings can be prevented in the future.

True Ongoing Authorization is in place, augmenting or replacing ATO dates. Risk thresholds are defined, and risk scores are monitored in near real-time. This continuous monitoring and remediation keeps the information systems operating at an acceptable level of risk at all times. More assessments are being performed, but this extra effort is offset by gains in other areas, including fewer incidents.

MATURITY MODEL CROSSOVER

IT Security is a critical risk for all federal organizations today and is a major piece of an overall Operational Risk Management program. Cited by executives as one of the fastest growing areas of risk today, IT Security has a significant place in an organization's strategic portfolio of risks and therefore should be factored into the Operational Risk program. In addition, security incidents can quickly escalate into major crisis. Companies should address this issue by ensuring security incident response processes are aligned with crisis management, disaster recovery and business continuity processes within Mission/Business Resiliency strategies.

Another factor in security risk management is the growing reliance on outside providers for mission support. Third Party Governance must be tackled as part of managing IT security given many organizations provide access to internal systems to external parties or rely on third parties for critical business operations.

Finally, data protection is a critical component of today's regulatory and compliance environment. Compromise of the confidentiality of protected data, such as personally identifiable information (PII), can lead to significant regulatory fines, reputational damage and compliance issues.

CONCLUSION

Implementing a future ready Information Assurance program is not a simple click-the-button effort. It is a maturity journey that organizations MUST take to turn security into an advantaged position to enable the business to exploit opportunities.

Companies in the Siloed stage your security function must reduce "the noise" and evolve traditional approaches that may get the job done but will never keep pace with today's climate. In order to move from Siloed to Managed stages, organizations Transition through projects that catalog and organize IT asset information and integrate security data sources. Companies in the Managed stage have solved (or are well on their way to solving) the integration of security and risk management through better visibility into security issues through common data and analytical capabilities, effective security processes and efficient methods to measure, monitor and report on security activities.

In order to reach the Advantaged stage, security processes Transform through rationalizing security plans and strategies, harmonizing across mission requirements and reducing administrative overhead and costs. By prioritizing effectively through mission/business context and awareness when incidents and events occur, security teams can keep up to speed with the business enabling risk-based decisions to explore the Opportunity Landscape.

Organizations in the Advantaged stage are now ready to realize the competitive advantage of harnessing risk – expanding missions, launching new services with calculated efficiencies, avoiding major issues that affect reputation and the bottom line. Companies in this phase focus on speaking "business language" and are able to identify and respond to emerging requirements ahead of the curve – using common taxonomies, common approaches, well-oiled decision making processes and, most importantly, data to support their conclusions.

ABOUT THE RSA ARCHER MATURITY MODEL SERIES

RSA Archer's vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model series of white papers outlines multiple segments of risk management that organizations must address to transform their GRC programs.

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime.

For more information on RSA, please visit rsa.com.