Assessment & Authorization & Continuous Monitoring

How do federal agencies and contractors stay compliant? Let us count the ways: meeting FISMA requirements, adapting to NIST 800-53 revisions, moving to the cloud and using FedRAMP and FITARA, factoring in unique department/agency directives, keeping up with new compliance demands, working around budget constraints—and that's just for starters.

Monitoring systems for compliance with security controls is an ongoing challenge. Continuous monitoring sounds great in principle, but in practice, it can be tough to know what exactly to monitor and which tools to use. Having to keep up with emerging security threats just adds to the challenge.

Make no mistake: Continuous monitoring can provide a more mature and nuanced understanding of risk. But to fully realize its potential, federal IA professionals must learn how to focus their finite resources where they're needed most and use them with maximum efficiency.

Capabilities: What it takes to mature A&A and CM processes

Managing IT and security risk in this new reality means having a collaborative, coordinated effort to:

- Align security policies to regulatory requirements
- Define authoritative authorization boundaries
- Implement, document and assess security controls
- Blend many streams of data into a cohesive risk picture

RSA Archer's Assessment & Authorization and Continuous Monitoring solution provides capabilities to:

Categorize assets and information systems using clearly defined authorization boundaries

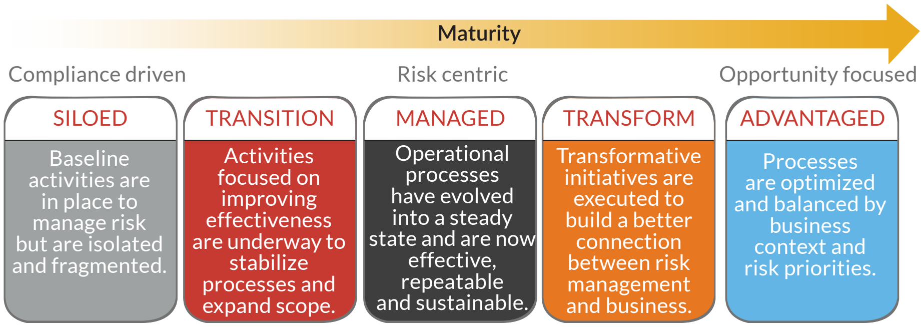
Select and implement controls and provide the ability to tailor controls for various methodologies

Analyze risk and authorize using a means to efficiently route and grant authorization requests (or not)

Implement continuous monitoring and ongoing authorization.

Stage by stage: Mapping the maturity journey

RSA Archer Maturity Models guide organizations through the journey from baseline risk management to optimized processes that balance opportunities and risks. There are five stages along the way:



SILOED Baseline activities are in place to manage risk but are isolated and fragmented.

TRANSITION Activities focused on improving effectiveness are underway to stabilize processes and expand scope.

MANAGED Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.

TRANSFORM Transformative initiatives are executed to build a better connection between risk management and business.

ADVANTAGED Processes are optimized and balanced by business context and risk priorities.

The Siloed stage: Mastering the basics

Organizations at this stage are often overwhelmed just trying to meet the demands of compliance.

- Compliance efforts are reactive and just-in-time.
- The organization is likely to be a revision behind on the control catalog.
- IT teams are completely siloed in their approaches to compliance.

SILOED Baseline activities are in place to manage risk but are isolated and fragmented.

The Transition stage: Stabilizing and strengthening

Moving from Siloed to Managed, A&A and CM teams push to integrate tools and processes.

- Integration of communication and tools helps break down information silos.
- Teams look to redesign or replace processes and tools for a more efficient common interface.
- The resulting visibility can lead to more opportunities for integration.

TRANSITION Activities focused on improving effectiveness are underway to stabilize processes and expand scope.

The Managed stage: Standing firm

As processes become more defined, they also become more objective and repeatable.

- Metrics and context begin to infiltrate decision making.
- Improvements in common control management help bring down control assessment costs and improve security.
- Vulnerability scan data includes business context, so incidents can be prioritized based on business impact.

MANAGED Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.

The Transform stage: Asserting control

At this stage, the goal is to move away from static or infrequent control assessments.

- Continuous Monitoring is implemented in earnest, including both manual and automated assessments.
- Effective assessment methods are tied to every control of every system.

TRANSFORM

Transformative initiatives are executed to build a better connection between risk management and business.

The Advantaged stage: Riding the wave

A&A and CM merge into common processes and technologies.

- Security issues are reported on with integrated business attributes and impact.
- Findings from compliance processes are reconciled back to policies to address underlying issues.
- True Ongoing Authorization is in place to support continuous monitoring and remediation.

ADVANTAGED

Processes are optimized and balanced by business context and risk priorities.

Organizations ultimately realize the benefits of a more rigorous, agile and comprehensive compliance strategy meeting missions with calculated efficiency, and avoiding major issues that could cause significant damage.

For more detailed information about the RSA Archer Maturity Model for Assessment & Authorization and Continuous Monitoring, visit **rsa.com/en-us/resources.**

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 outlines the segments of risk management that organizations must address to transform GRC.

About RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world.
For more information, visit **rsa.com.**

©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 Maturity Model, H16145-1 W386667.