ServiceNow Continuous Authorization and Monitoring

The Risk Management Framework (RMF)

The NIST Risk Management Framework (RMF) is a highly mature set of processes that provides a "common information security framework" for the federal government and its contractors. Compliance to NIST RMF is mandatory in the US Federal government, and increasingly is being voluntarily adopted by state, local and foreign governments, and critical infrastructure and high-risk industries. RMF is made up of a preparation stage and 6 defined steps with a series of tasks and potentially hundreds of controls that must be applied and continuously monitored. When scaled to a typical Agency, this results in thousands of controls and tasks that must be managed across multiple departments and roles.

Figure 1: NIST RMF process including applicable publications (source: BAP)

Automating RMF with ServiceNow Continuous Authorization and Monitoring allows you to automate more of the overall RMF process and its associated tasks and reduce risk and costs while decreasing the time and effort involved in authorizing a system.

The Continuous Authorization and Monitoring (CAM) application applies ServiceNow Integrated Risk Management to the NIST Risk Management Framework and other high assurance frameworks. CAM makes it easy to automate more of the work of RMF in the platform, manage all stages of RMF, and authorize systems faster and easier.

Built on ServiceNow Integrated Risk Management

ServiceNow Integrated Risk Management (IRM) works with the Now Platform® to provide a framework for managing policies, controls, and risks. It includes the ability to easily create controls, continuously monitor for compliance, identify risks, obtain approvals or exceptions, and track responses throughout your enterprise. The ServiceNow cloud-based platform consolidates the data into a single platform with flexible workflows, context for prioritization, and automation and orchestration capabilities. ServiceNow IRM includes Policy and Compliance, Risk, Operational/Advanced Risk, Vendor Risk, and Business Continuity Management. It helps organizations manage everything from OMB A-123, Enterprise Risk, Operational Risk and now high maturity cyber risk frameworks such as RMF on a single platform.

"… An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks…"

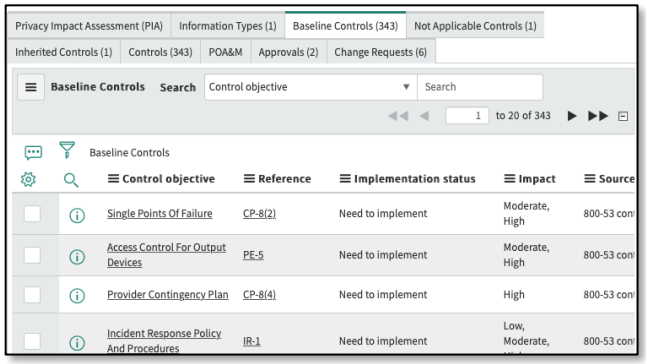
OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [OMB M-17-25]

Prepare

CAM allows you to easily define authorization boundaries and their systems. The CMDB allows you to create entity filters to identify assets, as well as manually add or remove individual assets. You can also attach diagrams and documents, determine impact thresholds and perform impact analyses as well as manage roles and responsibilities.

Categorize

CAM allows you to manage and tailor NIST 800-60 information types and their impacts, as well as the overall system impact, with justifications for any overrides. And automatically perform system categorization approvals in the platform.



Select

Select, inherit, and tailor controls with ease. CAM will automatically assign baseline controls based on categorization, and let you manage control overlays, tailor individual controls, and designate non-applicable controls. You can inherit common controls with visibility into the control status, and common control providers can easily select controls they wish to provide to others.

Implement

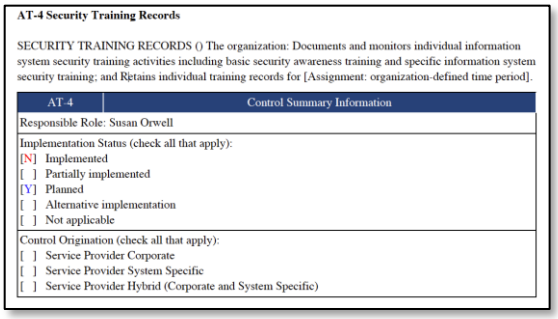
CAM automatically assigns controls to the system owners, or they can be created manually. You can trigger attestations to the System Owners to ensure controls are implemented for the respective information assets and ask for evidence. In case of non-compliance, IRM automatically generates an issue to ensure remediation is done quickly and controls are implemented.

Assess

Leverage the built-in Audit management to automatically create an Audit Engagement linked to your authorization package. Audit Tasks are automatically created for Security Control Assessors (SCAs), allowing them to manage, perform, and report on control design and operational effectiveness tests within the platform. Ineffective controls automatically generate an Issue, which are tracked as a Plan of Action & Milestones (POA&M) along with their associated remediation tasks.

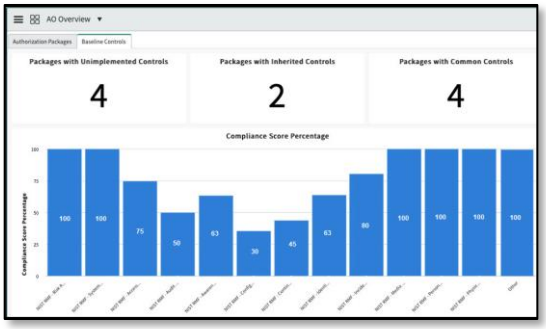
Authorize

CAM allows you to easily review evidence and documentation, control status, POA&Ms and other data without leaving the platform. Automatically generate a System Security Plan based on customizable self-populating templates. And authorize the system for a fixed time period or ongoing basis.



Monitor

Easily monitor your authorized systems with data from the CMDB, ITSM, ITOM and Security Operations. View all vulnerabilities, POA&Ms, configuration compliance failures, security incidents and more for each boundary in a single place. CAM ships with dashboards built specifically for Authorizing Officials, SCAs, and other roles that you can customize and build upon - or build your own dashboards.



Built on ServiceNow

Leverage ServiceNow's broad enterprise service management, workflow, and automation capabilities to transform and automate work processes, gain visibility into the network, and monitor key metrics.
www.servicenow.com/risk

servicenow

© 2020 ServiceNow, Inc. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.
SN-Solution-Brief-CAM-RMF-091420