REDSEAL

SECURITY CONTROLS AND RISK MANAGEMENT

FRAMEWORK

THE MEASURE OF RESILIENCE

BACKGROUND

The National Institute of Standards and Technology (NIST) Special Publication 800-53 defines a comprehensive set of controls that is the basis for numerous federal compliance and cybersecurity initiatives. However, implementing and continuously enforcing the controls defined in NIST SP 800-53 Rev.4 is a labor-intensive challenge for many federal organizations. SP 800-53 recommends a set of security controls that represents IT security best practices endorsed by the U.S. Department of Defense, intelligence community and civil agencies to produce "the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems." These new requirements have forced security departments to spend an inordinate amount of time collecting, organizing, monitoring and reporting in order to detect and manage control-related activity. It is therefore no surprise that cybersecurity and compliance teams are searching for technology to automate this necessary but taxing process.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

According to NIST SP 800-39, commercially available automated tools must "support situational awareness, or [maintain] awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes." However, NIST also cites that those tools, as well as corresponding processes designed to generate risk data, are not being deployed in a timely fashion. As a result, system security assessments and authorizations are usually based on infrequently conducted vulnerability scans or audits that test security controls at a single point in time—leaving security professionals unable to measure the real risk to systems between security control test cycles. Organizations are finding that it is one thing to implement the 800-53 controls, but quite another to implement and monitor them continuously. Most struggle to do so.

SECURITY CONTROLS AND RISK MANAGEMENT FRAMEWORK

REDSEAL AND FEDERAL GOVERNMENT CYBERSECURITY

RedSeal has a history of support for federal government cybersecurity initiatives. The company's innovative software solution is installed in numerous DoD, intelligence, and civilian organizations for the purpose of continuous monitoring. At the highest level, RedSeal delivers three core security controls:

- **Visibility:** Automated network mapping and situational awareness
- **Verification:** Continuous comparison of network security architecture against desired posture
- **Prioritization:** Analysis of vulnerability scan data and network architecture to identify highest risk vulnerabilities that must be remediated immediately. These controls apply to both legacy deployments and new architectures. In legacy situations, RedSeal allows you to understand the existing environment and identify security control gaps in a matter of days. In new architectures, RedSeal validates that the network is built and operated as designed. And in all situations, RedSeal vastly increases the value of scanning and penetration testing by prioritizing those vulnerabilities that are the most dangerous cybersecurity threats.

REDSEAL SUPPORT FOR NIST SP 800-53R4 CONTROLS

RedSeal's cybersecurity capabilities closely align with many of the controls in NIST 800-53r4. RedSeal supports a total of 34 controls in twelve of the 800-53 control families, including one control in the Privacy appendix of 800-53. Details of this control support can be found at the end of this document. At a high level, RedSeal supports 800-53 control areas as follows:

NIST CONTROL AREA	REDSEAL SUPPORT
Configuration Management	Continuous validation of actual system configurations versus desired state across multi-vendor infrastructure.
Risk Assessment & Incident Response	Prioritization of vulnerabilities for efficient and effective remediation.
Network Security Architecture & Access Control	Network map and situational awareness for risk assessment and system categorization.
Security Assessment and Continuous Monitoring	Analysis of actual, deployed information flow architecture and continuous comparison with desired architecture and policy.
Planning, Program Management and Acquisition	Inventory, audit and analysis of network security architecture for legacy, new deployments, and acquired systems

SECURITY CONTROLS AND RISK MANAGEMENT FRAMEWORK

With RedSeal, federal agencies can significantly reduce the cost associated with enforcing compliance against SP 800-53 by automating assessment of many of the SP 800-53 controls. Certain controls have traditionally been very difficult to automate, and therefore resource intensive to maintain and audit. However, RedSeal's unique technology can automate and prioritize these troublesome controls, greatly decreasing resource requirements while actually improving the quality of the control. For example:

- **Network Segmentation:** Internal and external network isolation based on router ACLs and firewall rules is a fundamental control in SP 800-53 and in many other compliance regimens. But testing the control at scale is a massive task, especially in multivendor environments. Many thousands of rules on hundreds of devices may be deployed to create just one isolated domain, and analyzing these against a security policy is a huge effort with lots of potential for error. RedSeal can not only automate this analysis in preparation for an audit, it can also continuously monitor the control and provide daily reporting on control integrity. This significantly improves threat defense posture while not requiring additional personnel or technical resources.
- **Penetration Testing:** Comprehensive penetration testing involves a combination of automated and manual procedures. A typical pen testing control activity calls for re-testing when there is any change to the controls being tested (e.g. perimeter defenses). When this scales to a large environment where a large number of changes are taking place, blanket manual processes are no longer realistic. RedSeal lets you focus the pen testing on the boundaries most likely to be affected by a change and with the highest risk potential.
- **Vulnerability Scanning:** All vulnerability scanning control activities are implemented for the purpose of identifying and remediating vulnerabilities; identifying the vulnerabilities is just the start of the process. But like pen testing, vulnerability scanning doesn't scale easily and can get expensive quickly. You need to determine where to launch scans and toward which targets. And when you find vulnerabilities by the hundreds, you need to determine which ones to resolve first. RedSeal rationalizes vulnerability scanning by combining scan results with its analysis of exploitation potential. This has two benefits: the most dangerous vulnerabilities are identified and can be corrected first, and the scanning effort can be tailored to focus in the areas where risk is highest.

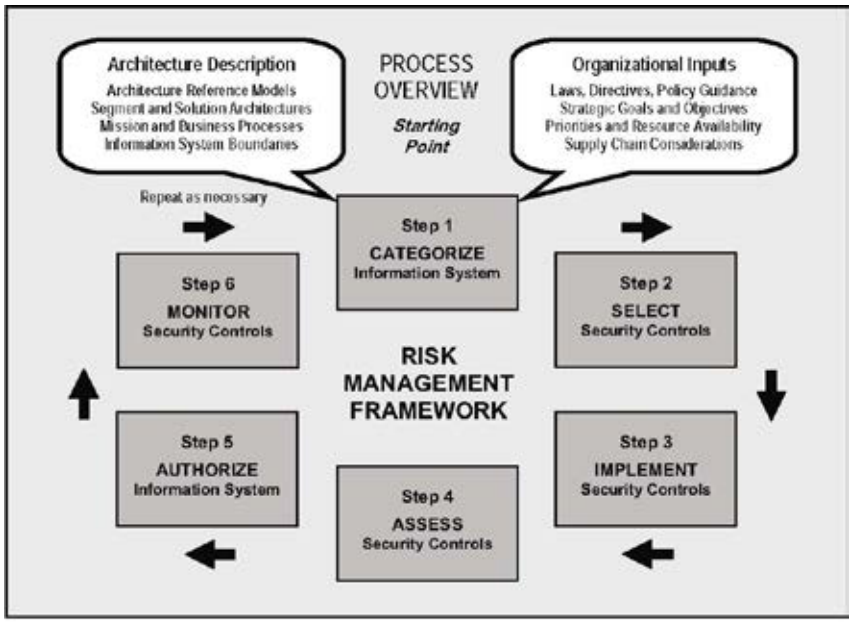
SECURITY CONTROLS AND RISK MANAGEMENT FRAMEWORK

REDSEAL AND THE NIST RISK MANAGEMENT FRAMEWORK

RedSeal also helps with implementing the NIST Risk Management Framework. The RMF (Special Publication 800-37) provides a framework for federal organizations to classify and protect information systems:

The RMF is conceptually quite simple and reasonable:

- Categorize systems and data based on sensitivity
- Select appropriate controls from the SP 800-53 control set based on that sensitivity
- Implement those controls
- Audit those controls and remediate "significant findings"
- Authorize the resulting control package to make sure risk posture is understood and acknowledged
- Monitor and audit the controls, and remediate deficiencies as they are found.



As with 800-53 itself, the challenge is implementing the RMF at scale without incurring unacceptable costs or wasting resources on controls that do little to actually reduce risk.

This document has already covered the 800-53 controls supported by RedSeal. In the context of the Risk Management Framework however, RedSeal is also extremely relevant for the monitoring requirement in Step 6. It is worth reviewing the guidance provided in the NIST RMF for this step:

"Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program." (NIST SP 800-37, page 38)

SECURITY CONTROLS AND RISK MANAGEMENT FRAMEWORK

RedSeal's ability to automate the assessment of network based controls on a continuous basis is essential to meeting this requirement efficiently. Without RedSeal, the manual effort required is overwhelming and beyond the resources of practically all organizations. It is also very error prone. Realistically what happens is that the network controls are not properly assessed given the amount of change in the environment and the size of the effort. This leads to actual increase in risk, not simply an audit finding. RedSeal addresses this issue by providing daily analysis of network segmentation efficacy along with detailed, actionable reporting on control deficiencies.

In addition, RedSeal helps constrain the resources required for continuous monitoring by justifying smaller subsets of controls and audit frequency for ongoing monitoring. The RMF states that the subset and monitoring frequency should be selected "based on the monitoring strategy developed by the information system owner or common control provider and approved by the authorizing official and senior information security officer." (SP 800-37, pg. 39). Because RedSeal implements a systematic, comprehensive and repeatable process for its monitoring strategy, it provides the justification required to limit the control subset for periodic assessments (audits), decreasing cost and effort.

Finally, RedSeal's automated approach to continuous monitoring supports reuse of assessment results, because result validation is maintained daily. This further decreases cost and effort, as stated clearly in the RMF:

"Reuse of assessment information is critical in achieving a cost-effective, fully integrated security program capable of producing the needed evidence to determine the security status of the information system. The use of automation to support security control assessments facilitates a greater frequency and volume of assessments that is consistent with the monitoring strategy established by the organization." (NIST SP 800-37, pg.39)

SUMMARY

With more emphasis on leveraging technology to improve intra-agency and inter-agency collaboration (specified in current FISMA guidelines), the federal government is placing a greater sense of urgency on real-time situational awareness and continuous monitoring to improve the efficiency and effectiveness of responses to emerging security threats. While a laudable goal, implementing complex control sets and frameworks such as NIST SP 800-53 and the 800-37 Risk Management Framework at scale is a major challenge, even for periodic audits. RedSeal was designed to cope with the difficulties of achieving of continuous monitoring of key NIST 800-53 controls such as topology mapping, network segmentation and vulnerability scanning. It also automates and limits the effort required to adhere to the monitoring requirement of the RMF. By implementing RedSeal, organizations can lower the cost of compliance, increase situational awareness, and improve control activity efficacy in an operationally efficient manner.

SECURITY CONTROLS AND RISK MANAGEMENT FRAMEWORK

CONTROL FAMILY	SUPPORTED CONTROLS	RELEVANT CONTROL REQUIREMENT SUMMARY	REDSEAL CONTROL ACTIVITY SUPPORT
AC-ACCESS CONTROL	4, 17, 20	Information flow enforcement: Regulation of where data is allowed to travel, including remote access and extranets. Commonly implemented using network enforcement mechanisms (firewalls, routers) at domain boundaries.	Analysis of actual, deployed information flow architecture and continuous comparison with desired architecture & policy. Identification of failure of information flow enforcement controls.
CM-CONFIGURATION MANAGEMENT	2, 3, 4, 6, 7, 8	Management of system configurations for consistency and highest possible security. Security impact analysis for proposed changes.	Continuous evaluation of actual system configurations versus desired state as defined by information policy. Recommendations for high security configuration settings across multi-vendor infrastructure. Full customization for environment specific requirements. What-if analysis of proposed configuration versus policy.
IR-INCIDENT RESPONSE	4	Adequate and appropriate incident handling.	Rapid analysis of network architecture and attack vectors specific to the target(s) of the incident.
MA-MAINTENANCE	4	Security controls on nonlocal (i.e. remote) maintenance activities.	Audit of network security controls on logical maintenance ports for nonlocal support.
PL-PLANNING	8	Development and maintenance of information security architecture, including defense in depth.	Inventory, audit and analysis of network security architecture for both legacy and new infrastructure. Informs review and updating of architecture when appropriate.
PM-PROGRAM MANAGEMENT	6,7,9	Enterprise architecture and risk management strategy.	Network map of enterprise architecture. Prioritization of vulnerabilities based on network architecture to inform risk management.

SECURITY CONTROLS AND RISK MANAGEMENT FRAMEWORK

REDSEAL NIST SP 800-53 V4 DETAILED CONTROL SUPPORT

CONTROL FAMILY	SUPPORTED CONTROLS	RELEVANT CONTROL REQUIREMENT SUMMARY	REDSEAL CONTROL ACTIVITY SUPPORT
RA-RISK ASSESSMENT	2, 3, 5	Security categorization, risk assessment and vulnerability scanning and remediation.	Network map and situational awareness for risk assessment and system categorization. Prioritization of vulnerabilities for efficient and effective remediation.
CA-SECURITY ASSESSSMENT AND AUTHORIZATION	2, 3, 5, 7, 8, 9	Security control assessment and continuous monitoring. System interconnections documentation and policy alignment, including internal, classified, non-classified, public networks and extranets. Continuous monitoring of threats, vulnerabilities, and information security. Remediation plan for control deficiencies. Penetration testing.	Automated creation and maintenance of network map. Evaluation and continuous monitoring of system interconnections within and between domains or missions. Prioritization of vulnerabilities for efficient and effective remediation.
SC-SYSTEM AND COMMUNICATIONS PROTECTION	2, 7	Boundary protection: network segmentation and sub-networking at external and key internal boundaries. Rationalization of traffic flow policy to minimum required.	Mapping of network boundaries and flow polices. Analysis of actual, deployed traffic flow architecture and continuous comparison with desired traffic policy.
SI-SYSTEM AND INFORMATION INTEGRITY	2,4	Information system monitoring and flaw remediation.	Rapid evaluation and correlation of IDS alerts to potential threat. Automated prioritization of remediation based on risk assessment.
SA-SYSTEM AND SERVICES ACQUISITON	8, 9, 11, 15, 17	Appropriate developer security architecture and testing.	Assist developers of networked systems to design, implement and test appropriate security architecture.
PRIVACY (APPENDIX J) - AR - ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT	4	Monitoring and audit of privacy controls.	IAuditing of network level privacy controls.