Improving Security Posture in the Public Sector

Recommendations for Deploying FedRAMP Authorized Enterprise Service Management with NIST-Compliant Workflows

White Paper

Table of Contents

Introduction

Meeting a Higher Level of Security Precautions

Whether experiencing an outage, needing a password reset, or opening any other help desk ticket, end users depend on timely responses from IT teams. Similarly, organizations depend on timely responses from IT to maintain user productivity. Nothing controversial here. There is nothing "wrong" with commercial-grade IT products. However, when government agencies are involved—whether federal, state, or local level—there are additional procedural and security requirements that help ensure compliance and reduce risk. Through the Federal Risk and Authorization Management Program (FedRAMP), IT vendors have the option to deliver cloud-based products to the federal government, its agencies, and contractors, while meeting a higher level of security precautions.

A major focus of the FedRAMP assessment is on the National Institute of Standards and Technology (NIST) Special Publication 800-53. Having a technical architecture compliant with NIST SP 800-53 includes requirements such as multi-factor authentication, continuous monitoring, FIPS140-2 crypto-modules, among other security controls. These may or may not be independent of a vendor's commercial-grade offering (some may include these capabilities by design). Federal agencies need to incorporate NIST-compliant workflows into their operations, placing FedRAMP Authorized solutions at the top of the list for helping them meet these workflow mandates.

This white paper helps guide you through some of the nuances of FedRAMP Authorized service management, matching NIST SP 800-53 (Rev. 4) Moderate Impact Controls to the stages of deploying Enterprise Service Management in a federal agency environment. You'll notice the white paper also references a number of security and privacy controls—audit control, training, access control, etc. To provide some context, NIST Special Publication 800-53 (Rev. 4) "Security and Privacy Controls for Federal Information Systems and Organizations," organizes these controls into the following "Control Families":

AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification & Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS - Personnel Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

Security Measures

Privacy

With dramatic changes in privacy legislation happening across the world, maintaining the privacy of customer data is a more urgent priority than ever. A Privacy Impact Assessment (PIA) must be done whenever an agency starts a new program. The PIA examines how citizen privacy may be impacted by the commencing program, ensuring appropriate data protection is maintained throughout.

> Privacy-impact assessments, comprehensive audit reports, and cybersecurity training (complete with alerts and reminders when training is missed) help agencies maintain a strong security posture.

Auditing

Auditing is all about checking and re-checking. Making sure that the expected workflows and outcomes are realized is part of the “regular scheduled maintenance” to keep your system at peak operational performance, but also at the optimal security posture. Audit control AU-6 requires organizations to review audit records and, when necessary, report findings to accountable departments (help desk, information security, etc.) along with any assignable actions. Modern service management solutions employ automation to facilitate the auditing and reporting processes.

Training

When it comes to cybersecurity, every employee is a member of the threat prevention team. Making sure everyone is educated to recognize and report risks is discussed in Control AT-2, and really is something every organization (whether public sector or commercial) should provide. Complementary to training all associates, Control AT-3 describes how agencies need to provide supplemental training dependent on individual roles and responsibilities, including agency contractors. Access to system-level software should be aligned with each role and supported by role-specific training.

Assessments

Regular, thorough, and comprehensive assessments of the security landscape is the cyber equivalent of having sentries regularly patrolling the perimeter of a physical property. The CA- control group outlines policies for assessments and authorization controls. Assessments must not only include personnel and access measures, but also the security provided in the service management solutions. As an example, control SC-7 covers Boundary control, and requires all connections into and out of the environment to be secured by default. This is one example when a FedRAMP Authorized solution may differ from its commercial-grade equivalent.

> NIST SP 800-53 requires all connection into and out of the environment to be secure by default—prudent but not required for commercial deployments.

Access Management

Access Control

Who has access to what systems? At what level? Why? These are among the core details of access control, and it may be for more than alphabetical sorting purposes that NIST SP 800-53 lists the Access Control security and privacy controls first. While control AC-1 discusses the access control policy, AC-2 supplements this with details regarding system account types (individual, group, guest, temporary, etc.), and the definition of workflows when additional reviews are necessary. Then there's exception handling, discussed in AC-14, such as situations where access to specific information doesn't require authentication. This workflow may support a permanent exception, or one defined by circumstantial parameters that allow authentication to be bypassed.

> New access requests, and the associated approval workflows, should be documented within the agency's service management solution.

Authentication and Identification

The IA- control set addresses the “ins-and-outs” of making sure users accessing systems are truly who they claim to be. Multi-Factor Authentication (MFA) is a required workflow and is intended to minimize the risk compromising credentials by requiring validation on a separate device. Think of the situation when a laptop is left in a coffeeshop or rental car. When login requires authentication on the laptop (in the form of a password) but also on a mobile device (SMS text code or permission app), unauthorized access becomes significantly more difficult. While control IA-2 describes the requirements for MFA, IA-5 is noteworthy for control enhancements ranging from password complexity to guidance on the use of encrypted versus unencrypted authenticators.

Physical Access Security

Where are confidential documents being printed, and who can retrieve them? How is maintenance performed? Physical output devices such as office printers are often overlooked targets of insider and intrusion breaches. Classified documents need to be printed to physically secured printers to prevent unauthorized access to printed content, for example. Output devices in secured rooms accessible by authorized badges or other individually identifiable means are among the guidelines offered in control PE-5. A separate control group for information-system maintenance describes how internal or outside entities obtain system access, and controls such as MA-2 advise on workflows for approving, monitoring, and keeping records of all maintenance performed.

Risk Assessment

“What could go wrong?” It’s hard to imagine the countless scenarios that could impact your agency, but understanding the risks and having procedural safeguards in place are essential to your security plan.

Control RA-2 provides the framework for categorizing risks based on the severity of potential adverse impact and escalation procedures. Whereas RA-5 requires the use of vulnerability scanning tools to maintain compliance. It's imperative that vulnerability scanning workflows be readily updated as new vulnerabilities are discovered and announced, and as methods for scanning are developed. Automated workflows compare vulnerability scans over time, helping identify trends in information-system vulnerabilities. This regular analysis aids the continuous updating of risk-assessment initiatives.

Automated vulnerability scanning workflows enable trend analysis, contributing over time to stronger risk assessments and threat prevention.

Vendor Risk Management

Agencies must protect themselves from supplier error. The NIST SP 800-53 System and Services Acquisition control set is designed to help reduce the risk to agency reputation. Workflows for onboarding and performing risk assessments on vendors need to be incorporated to protect public sector entities. Commercial-grade products may include these workflows and may be well documented, but FedRAMP Authorized solutions adhere to the strict requirements and standards required for US government implementation.

FedRAMP Authorized service-management solutions should include workflows for a strong vendor risk-management program, including onboarding and risk assessment.

Effective Change Management

From scoping a system update through implementation and testing of upgrades and modifications, the configuration management controls are designed to maintain stability and offer best practices to minimize risk throughout deployment. Whenever an outage occurs, the first question help desk teams often ask is "What changed?". The CM-2 control covers the establishment of baseline configurations

(which may also aid agency compliance with USGCB mandates). These are documented, formally reviewed and agreed upon specifications serving as the basis for future builds, releases, and/or changes.

Control CM-5 is designed to restrict access to systems for the purpose of making changes, along with recordkeeping to help identify any unauthorized changes. Following a templatized process for change implementation as the framework's CM-9 control describes should not only be part of the configuration management plan, but also forces responsible team members to consider what would need to be "backed out" if a change gone bad needed to be rescinded to return the system to a stable state.

Establishing a Change Review Board compliant with NIST SP 800-53 control CM-3 is prudent – expanding workflow approval especially as more work is being performed outside the office.

Incident Management and Response

Security incidents cannot be handled by automated defenses, so the NIST 800-53 Incident Response controls frame out who gets notified based on a security incident—and also the plans for handling these, particularly in IR-8, with reporting requirements in IR-6 applying to federal agencies and supporting vendors and contractors.

Being prepared for such incidents, as the frequency is ever-increasing, requires regular testing. IR-3 control requires the testing of incident response capabilities, as well as the documentation of test results. Ideally, testing is where an agency finds areas for improvement, and this is where workflows for flaw remediation come in, such as control SI-2. Vulnerability management assessments may seem to not be significantly different from commercial-grade products, but FedRAMP solutions are more extensively scrutinized than commercial-grade options—particularly in the area of security alerts.

Commercial-grade service management products may have periodic vulnerability monitoring. FedRAMP Authorized solutions should have continuous monitoring, with robust quality in line with NIST 800-53 control SI-5.

Contingency Planning

Situations like COVID-19 are all the proof necessary for why contingency plans are essential. Agencies are finding they need more information—and varying kinds of information—that hadn't been relevant before so many staffers began teleworking. It started with understanding employees' ability to connect from home but has expanded to collecting health information.

Agencies must be able to quickly build workflows that help them keep up as the situation evolves. Trying to match the office experience and resource access as best as possible is key for associates to work from anywhere—on corporate or personal devices. How do agencies prepare for what's next? Going back to the planning at the beginning of this paper, it's extremely important to have development environments so contingency scenarios can be rehearsed and refined. Like a traditional fire drill, ongoing contingency training and testing offer the best ways to ensure plans are realistic and adaptable. Agencies need to achieve continuity of operations for business functions, and performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency.

Trust Beyond Commercial-Grade

FedRAMP Authorized Ivanti Service Manager

Commercial-grade is designed to meet commercial-grade demands, but the requirements of public sector agencies level up from there. Whether a federal agency following compliance mandates, or a state or local governing body aiming for better security, rest assured that Ivanti Service Manager has been through the rigorous FedRAMP Authorization process. With over 25 NIST Special Publication 800-53-compliant workflows built into it, our FedRAMP Authorized solution offers public agencies and government contractors a validated and proven choice for their cloud-based Enterprise Service Management deployments.

Learn More

ivanti.com/FedRAMP
1 800 982 2130
sales@ivanti.com