TEVORA™

NIST SP 800-53 Revision 5 Updates

Luke Mueller and Jeana Cosenza

August 19, 2019

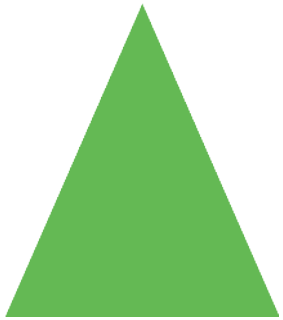

Table of Contents

What is NIST SP 800-53?

NIST Special Publication 800-53 is a publication by the National Institute of Standards and Technology (NIST) to set an information security standard for the federal government. Specifically, NIST SP 800-53 (also known as NIST 800-53) establishes security and privacy controls for all federal information systems and organizations excluding systems involved with national security. The goal of NIST 800-53 is to protect operations, assets, individuals, other organizations, and the nation from a diverse set of threats such as hostile attacks, human error, and natural disasters. These controls are written to be flexible and customizable to assist organizations in implementation.

NIST 800-53 Revision 5 (Rev. 5) creates a baseline of safeguarding measures for all types of computing platforms for both public and private sector organizations. The intention of Rev. 5 is to develop a next generation of security and privacy controls that to protect critical and essential systems for operation along with personal privacy of individuals.

How does this relate to FISMA and FedRAMP?

The Federal Information Security Modernization Act (FISMA) was passed in 2002 and updated in 2014. FISMA requires the implementation of information security controls that employ a risk-based approach. It applies to all federal government agencies, state agencies with federal programs, and private-sector firms that support, sell to, or receive services from the government. The framework of FISMA is NIST 800-53 and organizations that are FISMA-compliant are awarded an Authority to Operate (ATO). A FISMA ATO only applies to one combination of agency and organization. If an organization wants to work with multiple agencies, multiple ATOs are required, each with its own independent certification process.

The Federal Risk and Authorization Management Program (FedRAMP) was designed to enable easier contracting for federal agencies with cloud service providers (CSP). Like FISMA, the controls outlined in FedRAMP are based off the controls in NIST 800-53. The process of a FedRAMP certification requires a third-party assessment organization (3PAO) to assess security controls of the CSP's service by completing a Security Assessment Plan (SAP), performing initial and periodic assessments of the CSP's security controls, and producing a Security Assessment Report (SAR). The SAP, SAR, and the CSP's System Security Plan are then submitted to the Joint Authorization Board (JAB) or an agency for review. If authorized, the CSP's services are placed on the FedRAMP Marketplace for other agencies to find services that meet their needs as well as meet security requirements. After an authorization is granted to the CSP, the 3PAO performs annual testing and assists in any deviation requests, significant changes, or monthly assessments. The acquisition of an ATO requires a rigorous certification process compared to FISMA. FedRAMP is only applicable to CSPs and any agency planning to employ CSP systems.

Baselines

Federal Information Processing Standards Publication 199 (FIPS 199), published by NIST, establishes the standard for the security baseline categorization of all federal information and information systems. FISMA requires that all information and information systems are categorized according to risk levels.

FIPS 199 categorizes information and information systems into three potential impact baselines:

- **Low** – loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate** – loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.
- **High** – loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.

FIPS 200 establishes the minimum security requirements and related areas for federal information and information systems. The related security areas stated in FIPS 200 coincide with the control family categories of NIST 800-53.

Based off FIPS 199 and 200, NIST 800-53 determines which controls and control enhancements are required to be implemented to meet the minimum requirements for each baseline impact level.

Since FIPS documentation only establishes baseline requirements for security controls, privacy controls in NIST 800-53 are not included in the baseline requirements. Any privacy control that NIST determines as required must be implemented regardless of baseline levels.

Important Changes in Revision 5

Changes in the Title

In Rev. 5, NIST has removed 'Federal' from the title of SP 800-53; the new title is "**Security and Privacy Controls for Information Systems and Organizations**." While the framework is only required for federal systems, NIST believes the document will be more accessible to non-federal and private organizations and encourage organizations to use the standards and guidelines in the creation, modification, or updating of their systems.

Emphasis on Privacy

Rev. 5 places a much larger focus on privacy than its predecessor, Rev. 4, and aims to bring privacy to the forefront of the system design and implementation process. In Rev. 4, a separate appendix existed solely for privacy controls and they were not incorporated into security controls. In the new revision, NIST incorporated the privacy control families into the existing security controls to create joint security and privacy controls.

Table F-1 of *Appendix F: Consolidated View of Privacy Controls* in Rev. 5 distinguishes joint security and privacy controls from those controls only related to privacy. *Table F-1* also classifies each of the controls and enhancements as required (R), situationally required (S), or discretionary (D). If any privacy-related controls are being implemented, they must be implemented for any baseline level. NIST 800-53 offers guidance for tailoring controls for specific needs in *Appendix G: Tailoring Considerations*. Privacy-related controls exist outside of the FIPS**-199** baselines because the document only establishes those baselines for security controls. *Appendix D: Control Baselines* states which security controls and enhancements are required for each baseline in *Table D-1*. If a control is classified as a joint control, organizations can decide whether they want to do a joint implementation of the control or implement the security and privacy aspects of the control separately. Therefore, *Table D-1* also includes the implementation requirements for joint controls, even though they are classified as privacy-related.

While most of the privacy control family titles were eliminated during incorporation, **Individual Participation (IP)** was left as its own control and expanded upon as a main control. In total, IP contains six controls and five controls enhancement to address:

- User-facing privacy controls (including consent)
- Redress (regarding data accuracy and corrections to inaccurate data)
- Access to an individual's information that is maintained record systems
- The need for and distribution of privacy notices

While IP is not a completely new control family, its incorporation into the security controls is new.

Since compliance to IP is strictly privacy-related, privacy programs have the sole authority to select and oversee this control family, resulting in the need to be compliant with the privacy control requirements. In *Appendix F: Consolidated View of Privacy Controls;* only IP-1 is required while IP-2 through IP-6 are noted as situationally required. On top of the controls, the control enhancements IP-3 (1) and (2) are situationally required. Privacy programs must evaluate these controls and the enhancements to determine if they should be selected and implemented.

There is another new control family that also addresses privacy concerns called **Privacy Authorization (PA)**. PA uses four total controls and two control enhancements to address:
Verifying legal authority to collect, use, maintain, and share Personally Identifiable Information (PII)
Supporting documentation for uses cases of PII
Developing guidelines for sharing PII
Developing and communicating privacy notices
The privacy control compliance only requires PA-1 to be implemented by all organizations. PA-2 through PA-4 are situationally required for review along with control enhancement PA-3 (1) if PA-3 is selected to be implemented.

Increases in Program Management

The revision of the Program Management (PM) control family includes 16 new controls, doubling the number of controls in PM. These new controls aid with developing privacy programs to utilize the newly required privacy controls. There is also additional guidance for developing security programs where existing security controls were revised. Since this family is for developing and managing programs, it is deployed organization-wide and is independent of any system. This family is not directly associated with the security baselines. Implementation of PM controls is done through the same process as privacy-related controls stated above.

Changes to the First Control of All Control Families

XX-1 is the shorthand reference for the first control in all control families. Apart from Program Management (PM), there are several changes to the XX-1 controls. The first addition is that all policies must be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Since NIST wants private and non-federal organizations to use the NIST 800-53 framework as a guideline for their systems, this specification will most likely not apply to those organizations; therefore, the language was removed from Rev. 5.

Organizations must now assign a senior management official responsibility for an entire control family. While this change may help some organizations that are disorganized, other organizations may struggle, because there may currently be multiple people taking responsibility for the individual controls within a control family. Going forward, one person will be held responsible for making sure the control family is in place but will be permitted to delegate responsibilities to individual controls to multiple people.

NIST also specifies that organizations must ensure that the procedures implement the policies and controls. The addition of the term “ensure” implies that organizations must be able to prove that policies and controls are implemented.

The final change to the XX-1 controls involves the development, documentation, and implementation of remediation actions for violations to policies. In Rev. 4, remediation actions were placed on an individual control basis, but by placing them within the XX-1 controls, NIST is emphasizing the importance of following entire policies.

Changes in Language

NIST made changes to the language used throughout NIST 800-53. Throughout the document, the term "information systems" is replaced with "systems" to expand guidelines to be applicable to all types of systems, such as industrial or process control systems, cyber physical systems, weapons systems, and internet of things (IoT) devices that may not have been included through previous language.

NIST removed all introductory phrases within the controls to make the controls more outcome-based, rather than responsibility-based.

For all joint controls that were security controls in previous revisions, language is altered in the controls, changing "security" to "security and privacy" to emphasize the switch to joint controls.

Furthermore, there are additional assignment statements throughout the controls to reduce ambiguity during implementation.

Overall, more concise language is being used throughout Rev. 5 to improve understanding of the controls.

Compliance Deadline Estimation

For Rev. 1 and Rev. 2, NIST set compliance deadlines within one year from publication. However, for Rev. 3 and all subsequent revisions, compliance scheduling for NIST standards and guidelines have been established by the Office of Management and Budget (OMB).

The OMB decided on a one-year compliance schedule for implementation of Rev. 3. For Rev. 4, the OMB decided on a June 2014 deadline, giving agencies a compliance deadline of 14 months since publication in April 2013. There may have been two reasons for this extended deadline:

1. There were more changes in Rev. 4 than there had been in any previous revisions; or
2. OMB chose to make the compliance deadline at the end of a quarter rather than the middle of a quarter.

No one can precisely estimate a publication date for Rev. 5 at this time because the OMB has not yet given NIST their review of the final draft of the publication. Tevora estimates that organizations will have one year from Rev. 5's publication date to implement all new controls and be compliant with the new standard.

NIST is behind on their intended publication deadline for Rev. 5, which was originally scheduled for December 29, 2017. The deadline was pushed to December 2018 and rescheduled again to March 2019. As of January 2019, NIST has submitted the document to the OMB and Office of Information and Regulatory Affairs (OIRA) for review and approval. As of August 2019, the OMB and OIRA have not completed the review and will not permit NIST to publish.

Family Control Changes and Impact

Access Control (AC)

AC determines and limits access to systems and information stored on those systems.

There are not many changes in AC that will have an impact on organizations, because many of the control enhancements that have been updated or added are not included in any of the baseline configurations.

One control enhancement that will likely have an impact is AC-2 (3). The control changed from only requiring inactive accounts to be disabled and added four new conditions under which accounts can be disabled. Organizations will likely have to update policies and procedures that pertain to this particular control.

Additionally, several controls have been switched to joint controls; organizations will likely need to update their standards to include privacy in addition to security.

The baseline changes for the AC family are AC-2, AC-4, AC-6, AC-18. Several of these controls added control enhancements to further allow organizations to secure their systems. These enhancements focus on information flow enforcement, implementation of the principle of least privilege, and reviews of user privileges.

Awareness and Training (AT)

AT emphasizes the training and awareness policy and procedures of an organization.

The awareness training is updated in AT-2 to include privacy awareness, now that NIST is creating a combination of security and privacy training. AT-2 added the implementation recommendation of using practice modules to help with awareness and training. While **Insider Threat** was required in Rev. 4, **Social Engineering** and **Mining** have been added as required curriculum for Rev. 5. Training for indicators and precursors of insider threat and social engineering can help prevent compromises of system information.

AT-3 ensures role-specific training for new hires and maintaining training for current employees. The biggest change to the AT control family is the inclusion of privacy awareness and training on protecting privacy as well as security of the organization.

The most significant baseline change for AT is the addition of training policies for all baselines. AT-2 is the only control that contains significant changes, primarily focusing on adding privacy and security training for Low baseline organizations. Additionally, Moderate and High baseline organizations are required to add concepts of social engineering and mining training to their current programs.

Assessment, Authorization, and Monitoring (CA)

The biggest changes for the CA control family are the addition of "*Monitoring*" to and the removal of "*Security*" from the title, and the addition of privacy assessments.

Continuous monitoring was already included in the control family, so it has logically been added to the title. Security was removed from the title to reflect that it is now a joint security and privacy control.

The changes to CA that will have the most impact for organizations are the addition of privacy assessments and the addition of risk monitoring, which is now a required control enhancement for all baselines. Organizations will likely need to add procedures for privacy assessments to accommodate the joint control. Risk monitoring is a now a requirement, so organizations may need to add statements for risk monitoring policies and procedures since they can no longer be ignored.

It is now required in CA-2 for the assessment plan to be reviewed by an authorized individual before the assessment is done.

The addition of CA-3 (6) ensures that secondary and tertiary connections are identified and severed when security and privacy controls on those connections cannot be verified/validated.

CA-6 adds the need for an authorizing official for controls that are inherited by a system, along with 2 new control families that allow for joint authorization where needed.

The addition of CA-7 (4) ensures that the system is being monitored for risks and that it includes monitoring for effectiveness, compliance, and change.

The addition of CA-8 (3) requires that penetration testing be done on physical access points into a facility.

Baseline changes for CA involve CA-3, CA-7, and CA-8. The new required baselines add control enhancements to each control. CA-3 and CA-8 involve additional enhancements to the High baseline regarding identification of secondary and tertiary systems and employment of an independent penetration agent or team. CA-7 is a key change to note since it now requires all organizations to perform risk monitoring to ensure that organizations risk response measures are effective, compliant, and account for any changes in a system or environment.

Configuration Management (CM)

There are minimal changes to Configuration Management, but the changes that will probably have organizational impact are the addition of reviewing and updating the baseline configuration and the addition of CM-12, which requires that locations of information be identified. These changes will require organizations to regularly check and keep track of what is happening within their systems, which increases the organization's responsibility for maintenance of their systems.

Baseline changes for the CM control family are CM-2, CM-3, CM-4, CM-7, CM-8, CM-12. Control enhancements primarily focus on the implementation of security personnel within Moderate or High baseline organizations. All control enhancements primarily focus on the configuration of information storage locations and how an organization can use the controls to enhance the security of the system.

Contingency Planning (CP)

CP focuses on contingency planning and the ability to respond effectively to a significant future event or situation that may or may not happen.

CP-1 discusses the changes that pertain to assigning responsibility and the use of consequences to enforce the policies.

CP-9 (8) is a control enhancement that brings cryptographic protection for back-up information for an organization. Baseline changes for CP only consist of additions of control enhancements to CP-9 for Moderate and High baselines. This control enhancement ensures that organizations implement cryptographic protections for system backups.

Overall, the changes in the CP control family places emphasis on maintenance and ensuring that all contingency planning policies and controls are carried out effectively and efficiently.

Identification and Authentication (IA)

IA establishes the policies and procedures to ensure that organizational users or processes are uniquely identified and authenticated.

IA-2 (3), (4), (6), (7), (11), (13) are incorporated into IA-2 (1) and IA-2 (2) to simplify the control enhancements into the multi-factor authentication (MFA) enhancements.

IA-4 contributes control enhancement (8) to help assist in identifying and verifying parties for communication.
IA-5 enhances password protection and policies by adding a list of previously compromised passwords, commonly used, or expected password to reduce the likelihood of passwords being compromised. New control enhancements for IA-5, IA-5 (16) and IA-5 (17), can help reduce the costs by outsourcing password and party authentication issuance to ensure that partnerships with organizations are authenticated to reduce the likelihood of unwanted access. Additionally, the increase of use of biometric authenticators led to a control enhancement to reduce the likelihood of these authenticators becoming compromised.

IA-8 added a new control enhancement, IA-8 (6), to reduce privacy risk of user information from being compromised by blinding service providers and relying parties.

IA-12 was added to address proof of identity to collect, validate, and verify a user's identity before issuing credentials for system access. IA-12 was established to mitigate the risk to these new users and the creation of their accounts.

The baselines for this control family involve the controls IA-2, IA-4, IA-5, IA-8, IA-11, IA-12. IA-11 and IA-12 are new controls added to the baseline and require organizations to implement re-authentication when organizationally defined events occur, as well as identity-proofing current and incoming employees. The overall impact of IA is the authentication of user identities for access to organizations systems and protection of information of those users who are in the process of being authorized.

Individual Participation (IP)

IP is a new control family that focuses on privacy for an organization.

IP-2 allows individual to understand the risks that are being accepted when providing consent for an organization to their personal information.

IP-2 (1) allows users to select in certain cases how they will allow their information to be used beyond the originally intended use. IP-2 (2) allows users to re-give consent if the circumstances under which they gave original consent have changed or if a significant amount of time has passed.

IP-3 allows individuals to have personal information corrected if the organization is storing inaccurate information and creates a process for corrected information to be delivered to users authorized to use this personal information. IP-3 (1) ensures that the individual associated with the information and all authorized users of the information are notified when changes are made. IP-3 (2) allows individuals to appeal the organization's decision not to allow them to change their personal information.

IP-4 ensures that individuals are given the organizations privacy notice the first time they interact with the organization, and at organization specified frequency intervals. It also ensures that information about the processing of personally identifiable information is written in clear language that is easy for anyone to understand. IP-4 (1) allows users to re-give consent if the circumstances under which they gave original consent have changed or if a significant amount of time has passed.

IP-5 ensures that organizations include a Privacy Act Statement with any forms that collect personal information, or provide the Privacy Act Statement on a separate form that the individual can keep for their records. IP-5 also ensures that the Privacy Act Statement is read out loud if PII is being collected verbally.

IP-6 allows individuals to review the information that an organization is storing about them, while ensuring that individuals only have access to the appropriate information.

The main impact to organizations is that they are required to have policies and procedures in place for PII regarding how it is being stored and used, and the processes being used to inform individuals and receive consent to use their PII. IP is not allocated to baselines since it is a privacy control and is selected and implemented based on guidance in *Appendix F: Consolidated View of Privacy Controls* of Rev. 5.

Incident Response (IR)

IR family controls focus on the incident response of any incidents.

IR-8 explicitly updates the incident response plan to focus on the roles and responsibilities of the incident response team. This allows a team to effectively manage all incident responses to ensure the damage is mitigated and the problem is resolved.

Baseline requirements for the IR control family now call for implementing control enhancements to improve supply chain coordination. Also, the new implementation of IR-10 for organizations with high baseline classification, instructs the creation of a new integrated team of forensic and malicious code analysts, tools, developers and real-time operators to handle incidents. This may require organizations to hire qualified individuals to fulfill this requirement.

Protecting PII is a huge point of emphasis in Rev. 5; the incident response plan was also updated to include how to handle incidents regarding this type of information.

Maintenance (MA)

There were very few changes to MA, so most organizations likely won't be impacted by these changes. One change regarding MA-3 now requires frequency-based reviewal of organizational tools to ensure they are still being used under the same conditions that they were approved under. All the other changes involve filling-in gaps that were present in Rev. 4.

MA-2 and MA-2 (2) now include replacement as one of the maintenance options for system components, rather than just maintenance and repair, if a system component cannot be repaired and needs to be fully replaced.

MA-3 now requires a review of previously-approved maintenance tools to ensure that they remove tools that are outdated, unsupported, irrelevant, or not in use.

MA-4 (2) was withdrawn from Rev. 5 most likely because there were already controls in-place for documentation of nonlocal maintenance, making MA-4 (2) redundant.

The addition of MA-6 (4) ensures that there is a reasonable supply of critical system components available for use, while ensuring that there are safeguards in place to provide this supply of components.

MA had minor changes to the baselines, resulting in several already-required control enhancements being implemented into the control itself. MA-3 was the only control that had an additional control enhancement for the moderate baseline to improve the maintenance tools of an organization.

Media Protection (MP)

MP ensures that access to system media, both digital and non-digital, is restricted to ensure the integrity, availability, and confidentiality of a system. Media Protection covers the use of media to collect and analyze data to enhance an organization. These policies help protect information and the organizational from risks that may occur with the interconnectedness of the media.

MP-6 added a new control enhancement MA-6 (9) involving personally identifiable information and its deletion.

Baseline changes in MP have no impact in implementation in any level organization. The controls enhancements changes are incorporated into the controls themselves resulting in minimal impact for organizations going forward.

Privacy Authorization (PA)

PA is a new control family that places controls on the privacy of data.

The PA control family places a huge focus on privacy and PII. As systems continually become more interconnected, PA will be vital to protecting the privacy of users.

PA-1 aligns with all the XX-1 controls and requires organizations to establish the policies and procedures along with the new updates of consequences and a designated role for the control.

PA-2 requires organization to determine, collect, and document the legal authority to collect the information that they are collecting, especially PII.

PA-3 requires the organizations to provide reasoning to why they need access to the PII and to create privacy notices for the user's information. The control adds several control enhancements to restrict usage of PII and automate mechanisms to support records management.

PA-4 involves sharing PII with external parties. It requires an organization to develop, document and disseminate certain roles or personnel to handle the sharing of PII with external parties with checks and balances in place to ensure that the sharing of such information is permitted and acceptable.

PA is not allocated to baselines since it is a privacy control and is selected and implemented based on guidance in Appendix F: Consolidated View of Privacy Controls of Rev. 5.

Physical and Environmental Protection (PE)

PE focuses on the physical access and environmental protection policies to protect the organizations assets. The physical access controls in-place can reduce the likelihood of unauthorized access. The biggest impact on PE is the controls that are in place to address new physical attacks that may compromise the physical and environmental safety of an organization.

PE-3 (7) added a list of physical barriers that could be used to help restrict asset to an organization's assets and systems.

With the rise of Electromagnetic Pulse (EMP) attacks and the availability of equipment to perform these attacks, certain organizations may need to have the preparations to address potential EMP attacks. PE-21 was added to address this issue.

Control baselines for PE include control enhancements to protect the environment in which an organization operates. The new changes in the baseline controls involve PE-13 (1) and (2) to enhance fire protection to protect personnel and organizational assets. The control enhancements were implemented for the Moderate baseline to reduce risk of the damages caused by potential fires.

Planning (PL)

The main change for PL is the addition of privacy to all controls to reflect the switch to joint controls within Rev. 5. Organizations will need to ensure that they have adequate privacy plans for their systems.

Planning was also added to baseline selection and tagging for Rev. 5 to remove the control selection process from the actual controls, which allows the controls to be used by different communities of interest. This addition will have little impact to organizations that are updating documentation to reflect changes between Rev. 4 and Rev. 5, other than having two new controls to fill out in their SSP. This will likely apply to the private and non-federal organizations that are using NIST 800-53, to give them more flexibility of how they are implementing the controls.

Program Management (PM)

The Program Management control family was moved to be included within the main controls, rather than being in its own appendix. For further details, see Increases in Program Management in Important Changes in Revision 5.

Key privacy-only baselines to note are PM-18, PM-19, PM-23, PM-29, and PM-30. These baselines are required to be implemented for all organizations going forward.

PM-18 requires organizations to develop and implement a privacy program plan along with six parts to be included.

PM-19 calls for organizations to appoint a Senior Agency Official for Privacy to have various responsibilities to meet privacy requirements and managing privacy risks.

Organizations are required to setting up proper data quality management for PII. This policy is established in PM-23.

Inventory of PII is key for any organization and provides the guidelines for properly management in PM-29.

PM-30 requires organizations to create privacy reports to OMB, Congress, and other oversight bodies to show accountability for the privacy program.

Personnel Security (PS)

PS focuses on the security of an organization's personnel, their information, and the risks that are associated with them. The biggest change to personnel security is the verification process of citizenship and ensuring that they are legalized citizens of countries that are friendly to the Nation

PS-3 added a control enhancement that addresses citizenship requirements of personnel are verified and permitted to access a system.

Baselines for the PS control family have no additions or removals, so there is no impact to any system baselines.

Risk Assessment (RA)

RA focuses on the risk assessments of an organizations and looks for ways to mitigate risk and allocate an organizations resources to effectively protect its operations.

RA-2 created a control enhancement RA-2 (2) to add a second level of categorization for more granularity to the impact levels. This will enhance the risk assessments and assist in the process of prioritization of the multitude of risks an organization faces.

RA-5 added RA-5 (f) to include vulnerability scanning tools that readily update the vulnerabilities scanned to ensure that patching and repair of accessible vulnerabilities are addressed immediately.

RA also added three new controls to assist in progressing the Risk Assessment control family. RA-7 refers to responding to the findings from security and privacy assessments. RA-8 responds to the findings of privacy impact assessments. RA-9 addresses the categorization of criticality. All systems and their components may not need significant protection. The ability to find mission-critical function and components is key for the allowing organizations to have protection in the worst-case scenario. This analysis should be performed as the architecture and design is developed, modified or updated. The reduction of the amount of highly critical systems can mitigate risk that could be extremely costly to an organization.

RA control family requires new control enhancements and controls to assist organizations with risk assessments. RA-3 and RA-5 added control enhancements to assist with mitigating supply chain risks as well as vulnerability scanning. RA-7 is required for all baselines and requires organizations to respond to any findings and show proper documentation of implementing changes. RA-9 is required for Moderate and High baselines and enables organizations to make specific, critical risk mitigation decisions.

System and Services Acquisition (SA)

Many of these controls now include the need for privacy protection measures to be in-place in addition to security. SA-3 (System Development Life Cycle) added three new control enhancements, SA-3 (1), SA-3 (2), and SA-3 (3), to manage the development environment, define the proper way to use live data in the development environment, and to plan and implement a schedule for technology updates throughout the development life cycle.

SA-9 (6) and SA-9 (7) ensure that additional steps are being taken to protect security and privacy.

Changes to wording in SA-11 ensure that testing and evaluation are happening at specified frequencies.

The change of SA-12 from "*Supply Chain Protection*" to "*Supply Chain Risk Management*" ensure that not only are there safeguards in place, but that there is proper documentation of these safeguards. SA-12(16) was added to ensure that the chronology of system, system components, and associated data ownership is maintained.

Baseline changes for SA address the requirement to implement systems security engineering principles to develop trustworthy, secure systems and components. The new control baseline using SA-12 uses supply chain management plan to mitigate risks and consists of 6 components.

Rev. 5 added two new controls into the baseline requirements for SA. SA-21 requires High baseline organizations to use stricter screening processes when hiring external developers. SA-22 requires all organizations to replace components no longer supported by developers, vendors, or manufacturing organizations.

There are several places where control/control enhancements were withdrawn and moved to different controls/control enhancements where the information is more relevant. The biggest takeaway for SA is that it is now a joint control so organizations will have to ensure that any systems and services they use will also protect privacy and make any necessary changes when becoming compliant with Rev. 5.

System and Communication Protection (SC)

SC is the way that organizations can protect their communication and their systems that are all interconnected together. Like other control families, SC focuses on PII.

SC-7 added a SC-7 (24) for processing, storage and transmission of PII. The guidelines given enable the organization to properly manage this information.

SC-11 added a new requirement to provide a trusted communications path for users to establish communications with trusted components of a system. SC-11 (1) (b) was added to enhance the system with permissions to initiate a trusted path to ensure the user system unmistakably recognizes the source as trusted system component.

SC-28 added a control enhancement by allowing an organization to take an organization-defined action to respond to faults, errors, or compromise.

SC-42 discusses sensor capability and data, and added two new control enhancements. SC-42 (4) discusses on the notice of collection and allowing the users to be made aware of sensors that are on and collecting data and information. This alert will enable users to prevent any unwanted tracking of information. SC-42 (5) focuses on collection minimization that focuses on minimizing the amount of information that is collected at the entry point into a system. In the case of a breach, the less amount of data that is in the system would reduce the damages that result.

Baselines for this control family use control enhancements to further secure organizational systems and the boundary protection policies they should already have in place.

SC places significant emphasis on the management of communication of PII and the importance of protecting this information at rest and in-transit.

System and Information Integrity (SI)

While several changes were made to include control enhancements for handling PII, none of them are selected in the baseline control requirements so many organizations most likely won't be impacted by those changes.

SI control baselines include six new control enhancements. System monitoring is a key aspect of system security and the control enhancements enhance the protection and process of system monitoring for organizations.

Cryptographic authentication mechanisms are required for high baseline organizations to ensure malicious code is not located in hardware or software components.

Three new controls were also added along with several control enhancements, but these were also not included in the baseline control requirements, so they will most likely not impact organizations unless they relate to a system and need to be tailored into the system documentation. The controls that these new controls and enhancements are related to are also not selected in the control baselines, so there should be minimal impact regarding SI.

Conclusion

Key Impacts

The key impact for organizations within the new revision is the emphasis on privacy. The controls have shifted from a security-only focus to incorporating security and privacy.

Various changes in the baselines for each control family will require organizations to update or create new policies or procedures to become compliant with the controls. Once the document is approved for publication, organizations will most likely be required to fully incorporated within a year.

Rev. 5 requires the baselines and the family controls to be applicable to all systems regardless of if it belongs to government or private organization; these controls provide a customizable and applicable foundation for everyone. As a result, the structure and operational security for all organizations are enabled meet new threats, vulnerabilities, or changes in the operational environment to mitigate risk.

New controls in this revision provide the needed instructions and control steps to ensure that protection against new attacks as well as new approaches to security are used when becoming compliant to the framework.

Impact on Tevora

Actions

Consultants can advise clients to make proactive changes to reduce the workload required when Rev. 5 is published. Proactive changes increase the efficiency of the process of adjusting to the new controls and baselines.

Consultants could use NIST 800-53 as a foundation for recommendations on potential implementation for non-federal clients wanting to improve system security or create their own framework. The critical need for protecting internal information is applicable to all organizations. With Rev. 5, organizations can be up to date with any new technologies, threats, or changes in the environment that potentially have significant impact on their current operations and mitigate any risks associated with these changes.

Services

Tevora can offer the following services revolving around NIST 800-53:

- SSP Updates based on Rev. 5
- Gap Assessments
- Remediation
- Rev 4. Compliance Assessments with Notes and Feedback on Rev. 5
- Policy/Procedure Creation/Revisions

Resources

Bennett, Sese. "What You Need to Know About NIST-800-53-Rev-5." *LBMC Family of Companies*, LBMC, 27 June 2019, www.lbmc.com/blog/what-you-need-to-know-about-nist-800-53-rev-5/.

Brisson, Mark. "NIST 800-53 Rev 5 Draft - Major Changes and Important Dates." *NuHarbor Security*, 25 Feb. 2019, www.nuharborsecurity.com/nist-800-53-rev-5-draft/.

Cassidy, Susan B., and Covington Team. "NIST Releases Fifth Revision of Special Publication 800-53." *Inside Government Contracts*, Covington, 17 Aug. 2017, www.insidegovernmentcontracts.com/2017/08/nist-releases-fifth-revision-special-publication-800-53/.

FedRAMP. "Third Party Assessment Organizations." *FedRAMP.gov*, www.fedramp.gov/assessors/.

Joint Task Force. "Draft NIST Special Publication 800-53 Revision 5." *National Institute of Standards and Technology*, Aug. 2017, https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

Joint Task Force Transformation Initiative. "NIST Special Publication 800-53 Revision 3." *National Institute of Standards and Technology*, Aug. 2009, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r2.pdf.

Joint Task Force Transformation Initiative. "NIST Special Publication 800-53 Revision 4." *National Institute of Standards and Technology*, April 2013, https://nvlpubs.nist.gov/nistpubs/Legacy /SP/nistspecialpublication800-53r4.pdf

Ogden, Mike. "NIST SP 800-53 Rev. 5 Coming This Summer." *Lockpath*, 30 Apr. 2019, www.lockpath.com/blog/it-risk-management/nist-sp-800-53-rev-5-coming/.

Ross, Ron, et al. "NIST Special Publication 800-53 Revision 1." *National Institute of Standards and Technology*, Dec. 2006, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r1.pdf.

Ross, Ron, et al. "NIST Special Publication 800-53 Revision 2." *National Institute of Standards and Technology*, Dec. 2007, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r2.pdf.

Rouse, Margaret. "What Is Federal Information Security Management Act (FISMA)?." *SearchSecurity*, TechTarget, May 2013, searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act.

Sparks, John. "NIST 800-53 Rev. 5 Is Coming—Are You Compliant?" *Jazz Networks*, 7 Jan. 2019, www.jazznetworks.com/blog/nist-800-53/.

Symanovich, Steve. "Privacy vs. Security: What's the Difference?" *Norton*, Symantec, us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html.

Yakencheck, Jason. "Adopting the NIST 800-53 Control Framework? Learn More About the Anticipated Changes in 2019." *Security Intelligence*, 25 Mar. 2019, securityintelligence.com/adopting-the-nist-800-53-control-framework-learn-more-about-the-anticipated-changes-in-2019/.

Appendix

Appendix A – Terms and Definitions

Authority to Operate (ATO)- Official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations, assets, individuals, other organizations, the Nation based on the implementation of an agreed-upon set of controls.
Cloud Service Provider (CSP)- refers to organizations that offer network services, infrastructure, or business applications in the cloud.
Control Family – series of controls pertaining to a particular security and/or privacy topic designed to help organizations select controls that are best suited to their systems to become compliant with FISMA laws
Electromagnetic Pulse (EMP) – an intense burst of electromagnetic (EM) energy caused by an abrupt, rapid acceleration of charge particles. These bursts can give rise to large electrical currents in nearby wires. Attacks using this method, typically wipe out the availability of the system with surges with electricity.
Joint Authorization Board (JAB)- Primary decision-making body that reviews and provides authorizations for the FedRAMP Program. The Chief Information Officers from the Department of Defense, the Department of Homeland Security, and the General Services Administration serve on the board.
Multi-factor authentication (MFA) – A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Typically, uses something a user knows (i.e. password) and something a user has (i.e. token, or phone for a code).
Office of Information and Regulatory Affairs (OIRA) – A statutory part of the OMB. This is the United States Government's central authority for the review of Executive Branch regulations, approval of Government information collections, establishment of Government statistical practices, and coordination of Federal privacy policy. That are also a part of the approval process for each NIST 800-53 revision.
Office of Management and Budget (OMB) – A business division of the Executive Office of the President of the United States. It administers the US federal budget and oversees the performance of federal agencies. They are a part of the approval process for each NIST 800-53 revision.
Privacy – refers to any rights an individual possesses regarding their personal information and how it is used
Security – refers to how personal information is protected

Appendix B – Control Markup

For in depth changes to the control families, see Draft SP 800-53 Rev. 5 Controls Markup (pdf).

Appendix C- Baselines Markup

For in depth changes to the control baselines, see Draft SP 800-53 Rev. 5 Baseline Markup (pdf).

Appendix D – Baseline Changes Impact

For the impact of baseline changes, see Attachment 1 – Appendix D Baseline Changes Impact.