

Summary of the Major Revisions to the NIST SP 800-53 rev.2

NIST has released an Initial Public Draft (IPD) of NIST Special Publication 800-53 Revision 3, as part of the joint effort between the Defense, Intelligence, and Civil communities to create a common information security framework discussed in DRAFT NIST Special Publication 800-37 Revision 1. NIST SP 800-53 Revision 3 includes updates and changes intended to harmonize security control specifications across the federal government and incorporate the newly simplified, six-step Risk Management Framework. This document provides a high-level summary of some of these changes.

Cosmetic Changes:

- Consistent with NIST SP 800-37 Revision 1, the C&A Process is now referred to as the “security authorization process” and systems will now receive “security authorizations” instead of “security accreditations.”
- Security controls are now documented in bullet form with specific control requirements versus the previous paragraph format.
- The CA family is no longer “Certification, Accreditation and Security Assessments” and is now “Security Assessment and Authorization.”
- The step of “Selecting and Tailoring the Initial Baseline” has been renamed to “Selecting Security Controls.” “Selecting the Initial Baseline Security Controls” and “Tailoring the Baseline Security Controls,” have been added to this step as sub-steps.

Significant/General Changes:

- Security controls now include specific requirements previously stated as Supplemental Guidance.
- Security control/control enhancement requirements were reevaluated for the Low, Moderate, and High security control baselines.
- Redundant or unnecessary security controls and control enhancements were eliminated.
- Selected controls were reinforced by adding new security control enhancements.
- New security controls were added to address specific areas of growing concern:
 - *Cyber threats*
 - *Supply chain threats*
 - *Capital planning and budgeting*
 - *Enterprise architecture*
 - *Risk management*
- These revisions provide a crosswalk between NIST SP 800-53 controls and the international standard, ISO/IEC 27001.
- Furthermore, the revisions include additional guidance for the management of common controls:
 - *Common controls are defined as security controls that are inheritable by one or more organizational information systems.*
 - *The process of documenting common controls is specifically defined. The guidance highlights the flexibility of referencing organization-wide policy as long as the document is provided as an attachment to the System Authorization Package.*

1515 N. Courthouse Road
Suite 310
Arlington, VA 22201

703.841.5500 tel
703.841.5501 fax

www.onpointcorp.com