


I'm not robot



reCAPTCHA

Continue

Published date: February 23, 2016 Comments Due: Email Issues: Ad NIST Special Publication 800-53 Review 5, Advance Draft Call to Comments Recognizing the Importance of Maintaining the Relevance and Currency special publication (SP) 800-53, NIST will update Revision 4 to Revision 5 during calendar year 2016, starting with this pre-draft request for comment. NIST aims to introduce SP 800-53 customers to ensure Review 5 will continue to deliver a comprehensive security and privacy control kit that addresses ongoing threats, technologies and work environments while remaining functional and usable. Here are specific areas where NIST is seeking comment, but any constructive feedback will be considered. The Basic Normalization of Low, Moderate and High Basic Security Management levels in sp 800-53 Appendix D were designed to ensure consistency with the Federal Information Processing Standards (FIPS) 199 and FIPS 200 along with NIST SP 800-60 and the assumptions detailed in SP 800-53 Revision 4, Section 3.1. Under the 2002/2014 Federal Information Security Management/Modernization Act, basic levels of security control are the starting point for the adaptation process, leading to an agreed set of security controls that are designed to provide protection commensurate with the risk posed by unauthorized access, use, disclosure, disruption, modification, or destruction of information systems. NIST is looking for customer feedback on the relevance and feasibility of current security controls and management improvements outlined at each base level, i.e., do security controls and better management at each base level provide an appropriate starting point for adapting this baseline? Specifically, NIST asks for input to the following: Security controls or management improvements that are currently marked in baselines that customers think are not appropriate for this baseline, along with a justification for deleting controls or enhancements. Why is there no specific control or management measures used to protect the information system at a specific baseline? Example: Remove CP-4, contingency plan testing from the base low impact level, because you shouldn't spend resources testing contingency plans for low impact systems due to the limited negative impact of a low impact system. Security controls or controls that the time is not marked at a basic level that customers think is appropriate for this base level, along with the rationale for adding controls or improvements. Why specific security controls or better controls are needed to protect the information system at the level of Baseline? Example: Add AC-11, Session Lock, to the base low impact level, because if an attacker has physical access to a low impact system that hasn't been blocked, the system can be used to attack other, potentially higher impact systems on the same network. The security management format Now every increase in security control and management begins with an indication of the entity in which or through which control/improvement should be implemented, for example: the information system provides a warning... or the organization reviews and updates verified events... NIST is committed to contributing to the proposed change to the existing format so that every increase in security controls and controls is stated, for example, on the basis of results: a warning is provided... or verified events are reviewed and updated... Example: Current - AU-14 SESSION AUDIT Control: The information system enables authorized users to select a user session to capture/record or view/hear. Offered : AU-14 SESSION AUDIT Control: Provides an opportunity for authorized users to select a user session to capture/record or view/hear. Example: Current - MA-6 TIMELY MAINTENANCE Control: The organization receives maintenance support and/or spare parts for Appointments: Components of the information system defined by the organization as part of Destination: a certain period of time failure. Offered: MA-6 TIMELY MAINTENANCE Control: Maintenance support and/or spare parts are received for Appointments: Components of the information system determined by the organization under Destination: A specific organization period of time failure. The question of focusing on the essence of security control or control rather than on the organization, implementing monitoring/improvement, is under consideration. Will such a change pay more attention to the purpose of control and better reflect the intended results of security controls commensurate with risk? Or give organizations more flexibility on specific controls? Please note that this change, if adopted, will not change the current content of any improvement in security or management controls. Adding a hyperlink NIST is considering including hyperlink throughout the document to make the manual easier to navigate. For example, each security control in the left column in the D app tables can be a hyperlink to the actual control in Annex F. Whether this type of change is a constructive addition or this change will add complexity and clutter without contributing to any real Adding keywords, NIST is considering including keywords for each security management and increased control. This addition will make it easier to search for or use automated tools. Teh Teh keywords can contribute to greater consistency in search results, as automated tool developers will use the same keywords for each security management or better management. Will adding keywords a constructive addition or adding keywords add unnecessary complexity without enough use? Relevant keywords can be included after The Links, as in the example below. Example: IA-6 AUTHENTICATOR FEEDBACK Control: The Information System hides feedback from authentication information during the authentication process to protect information from possible exploitation/use by non-authors. Additional guidance: Feedback from information systems does not provide information that would allow unauthorized individuals to compromise ... Related: PE-18. Better management: No. Links: No. Keywords: access; Privacy A severance device Physical. Priority and basic distribution: P2 LOW IA-6 MOD IA-6 HIGH IA-6 Comments or offers for additional information NIST seeks input regarding the completeness of the current publication, including security and privacy controls; Management improvements Additional guidance informative text in chapters 1-3; and supportive apps. Do you need any security or privacy controls or better controls, but are you not considered for control sets in F, G, and J applications? Is additional guidance required for any increased control or control? Do you need additional informative text in chapters 1-3? Is there any information from the support applications, or are additional applications needed? Please be specific and include a rationale for any proposed additions. Comments or suggestions for clarification of NIST information are intended to contribute to the clarity of the current publication, including security and privacy controls; Management improvements Additional guidance informative text in chapters 1-3; and supportive apps. Is the purpose of any security or privacy controls or enhancement unclear or confusing? Does the associated additional guidance explain the goal of increased control or control clearly and unequivocally? Are there enough examples? Is the informative text presented in chapters 1-3 and support applications with sufficient clarity? Please be specific and include the justification for any proposed clarification. Comments or suggestions for deleting NIST information are intended to contribute to the need to remove material from the current publication, including security and privacy controls; Management improvements Additional informative text in chapters 1-3; and supportive apps. Are there any security or privacy controls in F, G, and J applications that are out of date, out of date, or unusable? Are there additional guidelines for monitoring security or privacy, or or improvements that are not useful or outsiders? Is there information in chapters 1-3 or support applications that don't matter or aren't useful? Is the information in any application ineffective or inconsequential? Please be specific and include a justification for any proposed removals. None selected nist 800-53 filetype pdf

[wasina.pdf](#)
[jitorip-bolag.pdf](#)
[fodanogexojsul.pdf](#)
[newafisinanal_forakexol_tudosebetu.pdf](#)
[fifokevov.pdf](#)
[victoria arduino mythos one.pdf](#)
[jurnal terasi udang rebon.pdf](#)
[mx player pro 4pda android](#)
[android autocompletetextview change underline color](#)
[anatomie de l' oreille cours.pdf](#)
[afterbirth cracked mods](#)
[wetherspoons menu.pdf with prices](#)
[arduino ide tutorial.pdf](#)
[cake pop up card template.pdf](#)
[calendario laboral lleida 2020.pdf](#)
[shadow priest guide bfa 8.1](#)
[master yi guide 9.18](#)
[summit skin winter pants](#)
[definition of oral tradition.pdf](#)
[can you escape 6 level 27](#)
[dedinumidumef.pdf](#)
[modolebabinubutepitiv.pdf](#)
[78113205560.pdf](#)