Federal Risk and Authorization Management Program (FedRAMP) Security Controls

Overview

This document lists the security controls and corresponding enhancements that Federal Agencies and Cloud Service Providers (CSPs) must implement within a cloud computing environment to satisfy FedRAMP requirements. The security controls and enhancements have been selected from the NIST SP 800-53 Revision 3 catalog of controls. The selected controls and enhancements are for systems designated at the low and moderate impact information systems as defined in the Federal Information Processing Standards (FIPS) Publication 199.

Selection of Security Controls

The FedRAMP Joint Authorization Board (JAB) began the selection of security controls with the 800-53 defined baseline for low and moderate impact systems. The JAB then selected additional controls and enhancements from the 800-53 catalog of controls. The controls were selected to address the unique risks of cloud computing environments, including but not limited to: multi-tenancy, visibility, control/responsibility, shared resource pooling, and trust.

Security Control Review Process

FedRAMP released documentation including the initial FedRAMP security controls and enhancements for public comment in November of 2010. Over 1,000 comments were received from Industry and Federal Agencies. Of these comments approximately 350 addressed the security controls and enhancements proposed by the FedRAMP JAB.

To address these comments, the FedRAMP Program Management Office (PMO) created Tiger Teams with representatives from across the Federal Government to review, analyze, and make recommendations for actions based on each comment. The FedRAMP JAB then reviewed and adjudicated these recommendations to create the FedRAMP security controls and enhancements presented in this document.

The FedRAMP JAB has defined in their governance structure a process and method for the FedRAMP security controls to be updated and refined through agency input, updates to NIST 800-53, and regular reviews of the controls. This process and method will be detailed in the JAB Charter in a forthcoming release.

Verification of Security Control Implementation

The implementation of the FedRAMP security controls on a cloud computing environment will be detailed in the following documents (in alignment with the NIST SP 800-37 Risk Management Framework). The templates and specific guidance on the creation of these documents will be released prior to the Initial Operating Capability of FedRAMP.

System Security Plan (SSP): This document will detail how the requirements of each security control will be met within a cloud computing environment. Within the plan, each control must detail:

1. What is the solution being employed? e.g. device, document, process, plan.
2. Who is responsible for the implementation? e.g. CSP, customer, or hybrid.
3. When is the solution implemented? e.g. once, periodic, continual.
4. How does the solution satisfy the control or requirement? e.g. how the solution correlates to the requirements of the control.

Security Assessment Plan (SAP): This document details how each control implementation will be assessed and tested to ensure it meets the requirements.

Security Assessment Report (SAR): This document details the issues, findings, and recommendations from the security control assessments detailed in the SAP.

Third Party Assessment:

In order to receive a FedRAMP JAB provisional authorization, the FedRAMP security control implementations must be independently verified and validated by a FedRAMP-accredited Third Party Assessment Organization (3PAO). The process for CSPs to use 3PAOs will be detailed in the FedRAMP Concept of Operations (CONOPS) to be released by February 7, 2012.

Organization of FedRAMP Security Controls

The Security Controls document is designed to accompany the NIST SP 800-53 Revision 3 catalog of security controls. The document lists the FedRAMP security controls and has 4 fields associated with each control. Organization of these fields is as follows:

Control Number and Name

- The FedRAMP security controls are numbered, named, and grouped by family designations in alignment with the 800-53 organization.

Control Baseline

- All controls and enhancements for low and moderate systems that have been selected by the FedRAMP JAB are designated in their respective columns.
- All controls and enhancements that are FedRAMP requirements above the baselines defined in the 800-53 baseline are denoted in **bold**.

Control Parameter Requirements

- Required parameter values for the variable parts of security controls and control enhancements are designated by the *assignment* and *selection* statements.

Additional Requirements and Guidance

- Any additional requirements beyond the scope of the security controls and control enhancements described in Special Publication 800-53 as well as additional guidance for interpreting and implementing controls and control enhancements are provided.