GOVREADY

The FedRAMP IDEATION CHALLENGE

Who Is Responding

GovReady PBC is a Virginia based business whose mission is to lower the cost of innovation in digital services to citizens. We are pleased to submit our FedRAMP Challenge Response to the FedRAMP Ideation Challenge.

Proposed Initiative: FedCHAMP

We propose FedRAMP establish open working groups associated with each of the NIST RMF Control Families to promote vendor-neutral evidence collection and standards for the security controls within that family. Dubbed **FedCHAMP** for **Fed**eral **C**ontrol **H**armonization **A**ssessment and **M**anagement **P**artnership,this initiative will reduce the guesswork of what information is required to verify the capabilities of a system.

Whether or not a security capability is enabled or not enabled is non-competitive and could be standardized for many controls. Under **FedCHAMP**, vendors in the audit and log management sectors along with CSPs and experts would collaborate on what evidence would best validate that content of an audit log contains sufficient information (AU-3) and could propose and promote a standard for how software products should alert when an audit processing failure (AU-5). The impetus behind the FedRAMP Readiness Assessment was to prepare vendors for FedRAMP by putting together a preliminary package of information before vendors even start the process. Through FedCHAMP, FedRAMP will be able to facilitate standardization of documentation and assessments while making the Readiness Assessment even better.

Existing Challenges FedCHAMP Addresses

FedRAMP Accelerated identified that the FedRAMP process has been historically challenged by the difficulty of technical writing, the difficulty of validating controls, and duplicative processes. Standardizing evidence collection related to security controls by vendors addresses these challenges. The compliance community has always invested in automation and with infrastructure as code is moving towards even more self-reporting by the system. FedRAMP can accelerate the OSCAL and OpenControl efforts by putting people invested in individual controls families together.

Management Approach to Implementing FedCHAMP

FedRAMP enjoys a unique position of authority in the community that they can use to facilitate standardization on non-competitive aspects of security like visibility and attribution. In the same way FedRAMP has set up 3PAOs to support the assessment of entire systems, third party stakeholders can contribute to the assessment and validation of component configuration and controls. FedCHAMP could model itself after the successful example of the Internet Engineering Task Force and Request for Comments.

Resources Required for Implementation & Metrics to Monitor & Manage Post Implementation

FedCHAMP necessitates the addition of community liaison staff to organize the 20 (800-53r5) working groups, possible one or two FedRAMP staff for every working group handling three working groups each. FedRAMP would also benefit from more website team members to provide information resources into the community. Measuring success of Working Groups could be measured by the ratio of participating vendors in the groups and the time to create documentation. The number of controls for which fully automated evidence collection and assessment exists would be a healthy metric as well.

Intended Outcomes of Implementing FedCHAMP

FedCHAMP would fundamentally improve and deepen the continuous monitoring environment that FedRAMP operates in today. Facilitating discussion and tangible steps towards self-assessment, increasing reusable content, and cutting down on writing cumbersome technical documentation all serves the greater purpose of increasing the efficiency of the FedRAMP process.

Contact: Greg Elin, CEO, GovReady PBC.
Phone: 202-505-1050.

Email: gregelin@govready.com
Web: http://www.govready.com