FedRAMP Accelerated Feedback

Workstream #1: Capability Readiness Assessment

Cloud Community of Interest (COI)

Date Released: April 22, 2016

Synopsis

The FedRAMP Program Management Office (PMO) at GSA is revamping FedRAMP Ready to include a FedRAMP Readiness Capabilities Assessment. FedRAMP released a draft of the FedRAMP Readiness Assessment Report Template and a companion document, the FedRAMP Readiness Assessment Guidance for CSPs and 3PAOs, for public comment.

The content in this report is in response to the draft FedRAMP Readiness Assessment Report feedback request. The Cloud COI members engaged in active participation to present comments in the form of feedback to the PMO. The COI facilitated collaboration of Government, 3PAOs, and CSPs to provide the feedback and input to FedRAMP on the new process. Input and practical suggestions are provided to further enhance FedRAMP Capability Readiness Assessment.

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology (ACT) is a non-profit educational organization established to create a more effective and innovative government. ACT-IAC provides a unique, objective and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communications between government and industry, collaborative and innovative problem solving and a more professional and qualified workforce.

The information, conclusions and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over thirty years of experience, to produce outcomes that are consensus-based. The findings and recommendations contained in this report are based on consensus and do not represent the views of any particular individual or organization.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC does not accept government funding. This report and other ACT-IAC activities are underwritten by AT&T, ACT-IAC's strategic mission partner, and a number of private sector organizations who share the ACT-IAC commitment to better government. ACT-IAC is greatly appreciative of this support and a complete list of sponsors can be found on the ACT-IAC website.

ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of IT. For additional information, visit the ACT-IAC website at www.actiac.org.

Cloud Community of Interest

The ACT-IAC Cloud community of Interest (COI) mission is to collaborate with federal CXOs and other government executives responsible for assessing, acquiring, deploying and maturing cloud technologies to become a major component of the IT & business strategy.

We leverage the expertise of the IT community to support the Government's cloud computing initiatives:

- Coordinate ACT-IAC related activities on Cloud Computing.
- Eliminate redundant efforts across ACT-IAC program areas and to promote cross pollination of ideas and activities.

- Align the efforts of ACT-IAC on cloud computing with the needs and requirements of the federal government.
- Provide a mechanism and platform for ACT-IAC members to collaborate and communicate effectively on the topic of cloud computing.

Disclaimer

This document has been prepared to contribute to a more effective, efficient and innovative government. The information contained in this report is the result of a collaborative process in which a number of individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

Further Information

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or www.actiac.org.

Contents

Introduction

The FedRAMP Program Management Office (PMO) at GSA is revamping FedRAMP Ready to include a FedRAMP Readiness Capabilities Assessment. The goal of this is to allow vendors to demonstrate their capabilities faster through an assessment by a Third Party Assessment Organization (3PAO) than through documentation reviews by the FedRAMP PMO. This will in turn enable Cloud Service Providers (CSPs) and Agencies to achieve FedRAMP authorizations faster without negatively impacting risk and quality of security packages.

In order to achieve FedRAMP Ready, an accredited Third Party Assessment Organization (3PAO) must perform an onsite assessment of a Cloud Service Provider's (CSP's) system based on required FedRAMP Readiness Capabilities. The results of the assessment will be documented in a FedRAMP Readiness Assessment Report.

FedRAMP released a draft of the FedRAMP Readiness Assessment Report Template and a companion document, the FedRAMP Readiness Assessment Guidance for CSPs and 3PAOs, for public comment. The documents were released to CSPs and 3PAOs to solicit their feedback and recommendations for improving these documents.

ACT-IAC Cloud COI facilitated accelerated feedback and collected comments from government leaders, 3PAOs, CSPs and System Integrators to further enhance FedRAMP. Specific workstream and feedback areas are:

1. Capability Readiness Assessment
2. Templates & Methods of Completion
3. JAB Prioritization
4. Open Forum

This "whitepaper" reports on findings from the first workstream, Capability Readiness Assessment. The other workstream areas are in progress in the remaining three subcommittees and are forthcoming as reports are due in late June 2016.

FedRAMP Capability Readiness Assessment Feedback

The following matrix provides specific comments regarding FedRAMP Capability Readiness Assessment. The instructions provided to the team is below:

How to populate the Comment Matrix:

Please use this template to provide comments and suggestions on improving the FedRAMP Readiness Assessment Report.

1. First, double-click on the header on p. 2 and provide the following information:
    a. Date – provide numeric month, day, and year.
    b. Provide your organization's name.
    c. Provide the name, email address, and phone number for a point of contact (POC) if we have any questions on the comments.

2. First column provides the comment line number; it is greyed out as it is automatically generated by Microsoft Word.

3. Second column identifies the comment author.

4. The third column identifies the location in the document on which you want to comment. Enter the line number of the document text to be commented on.

5. For the fourth column, identify the type of comment. The responses are:

Code	Change Type	Example
E	Editorial	Typos, grammar, format
G	General	Structure, cohesion, accuracy, consistency, clarity
T	Technical	The third check in Configuration Management should be XYZ.

6. The fifth column identifies the document contents that you believe should be updated and the reason for this change, e.g., review time period is not correct.

7. The sixth column, Proposed Change, documents the way you would like to see the document information changed, e.g., review the document every six hours.

8. The seventh column, FedRAMP Comment Resolution, is for internal FedRAMP use and should not be filled in.

Also embedded here is the summary presentation deck:

ACT-IAC Cloud COI
- FedRAMP accelerat

ID #	Author of Comment	Line # or Table No.	Type of Comment (E-G-T)	Comment (Justification for Change)	Proposed Change	FedRAMP Comment Resolution
1.	KCG	1	T	Minimum acceptable Capability level missing	Should contain guidance stating the minimum acceptable capability level for matrices within each family and the overall capability level determination to be certified as FedRAMP ready.	
2.	KCG	1	T	This document is more a set of instructions than a guidance from FedRAMP.	Change the name and language to state the contents are instructions.	
3.	BRMi	1	G	Make the Readiness Report easier to complete	Consider combining CSP & 3PAO Guidance with Report Template so 3PAO does not need to jump back and forth between two documents when reading guidance on how perform assessment.	
4.	BRMi	12	E	Change wording so they provide instructions to the 3PAO rather than describe the document. Current text: "This section provides a quick summary"	Proposed text: "Update this section so it provides a quick summary	
5.	KCG	15	T	CSPs receive P-ATOs not ATOs Current text: "should describe that CSP system and its Authorization To Operate (ATO) status."	Proposed text: "should describe that CSP system and its Provisional Authorization to Operate (P-ATO) status."	

ID #	Author of Comment	Line # or Table No.	Type of Comment (E-G-T)	Comment (Justification for Change)	Proposed Change	FedRAMP Comment Resolution
6.	NASA	67	T	Many FedRAMP/NIST requirements call for automated and centralized management.	Add this text: "Identify which process are automated and centralized."	
7.	NASA	83	T	Justification: Health system in California had major PII breach because truck cargo carrying backup tapes including HIPAA info was stolen.	Demonstrate protection of audit & backup information stored on removable media.	
8.	NASA	81	G	Not just suspicious events should be notified. Current text: "Have alerts and notifications based on suspicious events."	Proposed text: Have alerts and notifications based on suspicious events, and system or audit events (e.g., logs full or logs changed).	
9.	NASA	100	T	Can anyone make changes? No way to determine.	Add a bullet to explain how personnel who can make configuration changes are identified	
10.	BRMi	106	E	Provide instructions from the perspective of the 3PAO, not the CSP. Current text: "your system"	Proposed text: "the CSP's system"	
11.	BRMi	113	E	Provide instructions from the perspective of the 3PAO, not the CSP. Current text: "do you test"	Proposed text: "does the CSP test"	

ID #	Author of Comment	Line # or Table No.	Type of Comment (E-G-T)	Comment (Justification for Change)	Proposed Change	FedRAMP Comment Resolution
12.	NASA	148	T	Justification: Health system in California had major PII breach because truck cargo carrying backup tapes including HIPAA info was stolen.	Add this bullet: "Address media transport if applicable (Is media encrypted? Is there a point-to-point chain of custody?)	
13.	NASA	156	G	Ensure passwords are changed whenever an administrator leaves the CSP	Add this bullet: "Verify the CPS has procedures to ensure accounts are updated as a result of personnel transfers and terminations."	
14.	KCG	150, 158	G	Missing capability levels	Create capability levels for PS and PE families.	
15.	NASA	164	T	Physical protections other than entrance not addressed	Add the following bullet: "Describe the infrastructure protections that are currently in place? (e.g. fire suppression, emergency power, water shutoff)"	
16.	NASA	175	T	Credentialed scans reveal much more information than non-credentialed	Add this text: "Verify that vulnerability scans credentialed."	

ID #	Author of Comment	Line # or Table No.	Type of Comment (E-G-T)	Comment (Justification for Change)	Proposed Change	FedRAMP Comment Resolution
17.	KCG	184	T	Level designations for "Weakness Remediation"	The descriptions for the levels should be revised as follows for better understanding of capability level expectation: I - Ad Hoc II - Tracked via POA&M III - Consistent resources and funding for remediation IV - 75% > remediated within FedRAMP defined timeframes V - 90%> remediated within FedRAMP defined timeframes	
18.	KCG	215	T	Clarify guidance for permitting Alternative Implementations and Not Applicable controls. The guidance states that this section is for "describing" the Alternative Implementations and Not Applicable controls. If the intent is that the 3PAO should also state whether or not the 3PAO is in agreement with these control designations.	Add this text: "3PAO should indicate whether or not they agree with the CSP designation for all Alternative Implementations and controls marked as Not Applicable."	

ID #	Author of Comment	Line # or Table No.	Type of Comment (E-G-T)	Comment (Justification for Change)	Proposed Change	FedRAMP Comment Resolution
19.	Microsoft, Google, Amazon, Salesforce	215-220	G	Alternative Control Implementations and Not Applicable controls do not fit into the model of a capabilities assessment. These controls should be validated and tested using the traditional testing approaches specified by the PMO as part of the full/annual assessment.	Remove section 2.13 and focus on the 20 capability questions proposed in the following embedded document: (Also in Appendix)  Capability_Criteria.docx	
20.	KCG	225 – 281	T	These definitions are too IaaS and PaaS focused.	Will be better interpreted and received if written using similar theory and language used for CMMI maturity levels. • Level I – Initial/Ad Hoc • Level II – Managed • Level III – Defined • Level IV – Quantitatively Managed • Level V -- Optimized	
21.	Microsoft, Google, Amazon, Salesforce	All Tables	G	Capability level selections need to be defined to prevent misinterpretation by CSP/3PAO and ensure standard interpretations across government/Industry.	See document embedded above (Item 19) for table with definitions/recommended updates to include 20 capability questions in place of a 5-level model.	
22.	Microsoft, Google, Amazon, Salesforce	All	G	Capability levels do not map directly to the statements in Appendix A.	Remove Appendix A and shift to a capability focused set of 20 evaluation criteria. See document embedded above (Item 19)	

ID #	Author of Comment	Line # or Table No.	Type of Comment (E-G-T)	Comment (Justification for Change)	Proposed Change	FedRAMP Comment Resolution
23.	Microsoft, Google, Amazon, Salesforce	Appendix A	G	Capability level descriptions are generic and do not map directly to individual capabilities. A capability level does not map directly to individual control family capabilities.	Recommend removing Appendix A as part of the capabilities question shift from maturity model (5 levels) to capability questions answered by the 3PAO. See document embedded above (Item 19)	
24.	Microsoft, Google, Amazon, Salesforce	All	G	The addition of the maturity ratings adds unnecessary ambiguity to the readiness assessment. The maturity model creates an additional evaluation scheme (e.g., Moderate Level IV) that further complicates the work by the 3PAO without any clear benefit to the CSP.	We strongly suggest that the PMO remove the maturity model and focus only on the capabilities described by the CSP and validated by the 3PAO as meeting the NIST 800-53 Rev.4 requirements and any FedRAMP specific guidance. If the intent is to streamline and accelerate FedRAMP certification, the readiness assessment should focus solely on the capability of the CSP to meet the stated NIST requirements, including consideration of any alternative implementations and risk acceptance.	
25.	Microsoft, Google, Amazon, Salesforce	All	G	The capability levels are not aligned with an industry standard and are not presented in increasing order of maturity. For example, CSPs could meet capabilities in higher levels without meeting the lower level capabilities.	We strongly suggest that if the PMO wants to adopt a maturity framework is leverages existing industry practices such as the NIST Cybersecurity Framework instead of creating a FedRAMP specific methodology.	
26.	Microsoft, Google, Amazon, Salesforce	All Tables	G	Capability level selections need to be defined to prevent misinterpretation by CSP/3PAO and ensure standard interpretations across government/Industry.	See document embedded above (Item 19) for table with definitions/recommended updates to include 20 capability questions in place of a 5-level model.	

Contributors

The following individuals contributed to the feedback provided herein:

Erik Boxhoorn, Google

Bill Burns, Google

Stacy Cleveland, HP Enterprise (HPE)

Kathleen Fischer, Vencore

Elizabeth Fitzgerald, Salesforce

Jenn Gray, Amazon Web Services

Marilyn Hays, HP Enterprise (HPE)

Jenifer Heimbach, HP Enterprise (HPE)

Kyle Hendrickson, Battle Resource Management Inc. (BRMi)

Min Hyun, Microsoft Corporation

Nate Johnson, Microsoft Corporation

Roopangi Kadakia, National Aeronautics and Space Administration (NASA)

Drew Kahle, Salesforce

Ann Marie Keim, National Aeronautics and Space Administration (NASA)

Daniel Hae-Dong Lee, Censeo Consulting Group

Ted Steffan, Amazon Web Services

Kathleen Whalen, ManTech International Corporation

Appendix: Proposed Initial Capability Criteria

	Initial Capability Questions	Applicable NIST Cybersecurity Framework
1	Does the CSP have the capability to restrict access to resources to authorized personnel?	Protect
2	Does the CSP restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system?	Protect
3	Does the CSP have the capability to restrict the flow of data across internal and external boundaries?	Protect
4	Does the CSP have the capability to detect, contain, and eradicate malicious software?	Detect
5	Does the CSP have the capability to transmit and store customer data using sufficiently strong encryption?	Protect

6	Does the CSP have the capability to detect and remediate system flaws in a timely manner based on risk posed to the system?	Detect
7	Does the CSP have the capability to identify and authorize users in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation?	Protect
8	Does the CSP have the capability to store audit data in a tamper resistant manner which meets chain of custody and any e-discovery requirements?	Protect
9	Does the CSP have the capability to perform after the fact, forensic investigations of suspected security incidents?	Recover
10	Does the CSP have the capability to detect unauthorized or malicious use of the system, including insider threat & external intrusions?	Detect
11	Does the CSP have the capability to train personnel on security awareness and role-based security responsibilities?	Protect
12	Does the CSP have the capability to account for the critical components - hardware and software - that comprise the system?	Identify

13	Does the CSP have the capability to ensure that ongoing maintenance and operation of the system does not degrade the system security posture?	Protect
14	Does the CSP have the capability to recover the system to a known and functional state following an outage, breach, or disaster?	Recover
15	Does the CSP have the capability to assess risk, track ongoing risk/remediation, and report risk posture on a regular basis?	Identify
16	Does the CSP have the capability to restrict physical system access to only authorized personnel?	Protect
17	Does the CSP have the capability to classify positions by risk and screen personnel based on those risk ratings?	Protect
18	Does the CSP have the capability to sanitize or destroy physical media prior to removal from the authorization boundary?	Protect
19	Does the CSP have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations?	Respond

20	Does the CSP have the capability to investigate and remediate suspected incident detections in a timely manner?	Recover