TEVORA™

FedRAMP Authorization Guide

2020 Tevora Whitepaper

Kevin Liang
Taiba Zadran
with guidance and revisions from
Kaitlyn Bestenheider
Troy Dahlin

July 15, 2020

Table of Contents

FedRAMP Overview

The Federal Risk and Authorization Management Program (FedRAMP) is a United States government-based program that provides a standardized approach to security assessments, authorization, and continuous monitoring for cloud products and services.

FedRAMP Requirements

FedRAMP is mandatory for federal agencies implementing cloud deployments for service models at the Low, Moderate, and High levels. Private cloud deployments may be the only exception if they are intended for single organizations and are implemented in federal facilities.

FedRAMP is based on the National Institute Standards of Technology (NIST) Special Publication 800-53 Revision 4 (NIST 800-53 (Rev. 4)) baselines and adds controls above the baseline that specifically address elements of cloud computing. These additional controls ensure all federal data is secure in cloud environments.

The FedRAMP Marketplace

The FedRAMP Marketplace (marketplace.fedramp.gov) is an online repository providing information about cloud service offerings (CSOs) that have achieved a FedRAMP designation, federal agencies that leverage FedRAMP compliant CSOs, and certified Third-Party Assessment Organizations (3PAOs) as accredited auditors for FedRAMP assessment. The FedRAMP Marketplace is one of the primary resources that any federal agency can reference to seek compliant CSOs. This enables more opportunities for Cloud Service Providers (CSP) to obtain subsequent federal contracts with federal agencies.

Cloud Service Provider

Cloud Service Provider (CSP) organizations provide and maintain network services, including data storage and computing infrastructure, hosted in the cloud. They provide on-demand availability of computer system resources which can be accessed without on-premise physical servers.

The Cloud Smart Strategy provides guidance surrounding security, procurement, and the necessary workforce skills needed to foster cloud adaptation and implementation. To address the Cloud Smart Strategy, federal agencies are incentivized to increase computing demands that requires the flexibility and availability of the on-demand infrastructure of cloud services. Some CSPs have extended their services to be compliant with federal regulations to fulfill those demands. However, all federal agency contractors are required under FedRAMP regulations to operate using authorized CSOs when seeking cloud services. Therefore, CSPs must obtain FedRAMP Authority to Operate (ATO) to offer their services to any federal agency. Once a CSP has obtained their first FedRAMP ATO, they will be published onto the FedRAMP Marketplace.

Federal Agency

Federal agencies are government organizations which carry out national goals including resource management, financial oversight, and security issues such as the Department of Defense, the Department of Education, and the Department of Health and Human Services. Federal Agencies are adopting cloud solutions that provide scalable and demand services creating a more efficient and cost-effective program. Since becoming FISMA and FedRAMP compliant can be a long-term project, many federal agencies use the FedRAMP Marketplace to identify potential services that have already been approved for use by the federal government to meet their needs.

Third-Party Assessment Organization

Third-Party Assessment Organizations (3PAO) are the certified independent organizations that help both CSPs and federal agencies meet FedRAMP compliance regulations. Once certified, they will be included in the FedRAMP Marketplace as a resource to help agencies complete their missions related to FedRAMP. They offer both necessary FedRAMP on-going and continuous assessments services, including executing the Security Assessment Plan (SAP) and the Continuous Monitoring Plan assessments. Essentially, their services extend throughout the entire FedRAMP process including the initial gap assessments conducted prior to the FedRAMP process and the continual annual assessments post-FedRAMP ATO.

Overview of FedRAMP Authorization

While required to work with federal agencies, the process to reach FedRAMP authorization can be a long one. In the early adaptation stages of obtaining FedRAMP accreditation, the security authorization process took most organizations 12-24 months to complete. In the summer of 2015, FedRAMP made their process more efficient, but most organizations still need six months or more to obtain authorization. Below is a description of the three main phases of the FedRAMP authorization process: Pre-Authorization, Authorization, and Post Authorization.

Phase One: Pre-Authorization

In phase one of the FedRAMP authorization process, federal agencies will establish partnerships with a service provider. All necessary documentation, planning, and communication pathways must be defined.

Pre-FedRAMP Planning and Partnership Establishment

The Partnership Establishment phase is when federal agencies select a CSO that will meet the agency’s mission needs and to establish a working relationship with the CSP, FedRAMP Program Management Office (PMO), and other relevant agencies. Once a CSO has been selected, the CSP formalizes a partnership with the requesting agency.

The CSP must also establish their system is fully built and functional, display a satisfactory level of commitment, and exhibit an understanding of the entire FedRAMP authorization process to ensure sufficient success rate in obtaining FedRAMP accreditation. The primary evidence that demonstrates this includes a developed system security plan (SSP) with a well-documented Authorization Boundary, system certifications such as Capability Maturity Model Integration (CMMI) and International Organization for Standardization (ISO), Federal Information Processing Standard 140 Revision 2 (FIPS 140 (Rev. 2)) security implementations, and established policies and procedures. A Readiness Assessment Report (RAR) should be developed to exhibit all evidence necessary to demonstrate acceptable success in completing the FedRAMP process.

FedRAMP Planning

The FedRAMP Planning phase is used to prepare documentation necessary to organize the tests and assessments that verify implementation of controls needed to meet FedRAMP compliance. All strategies and agendas will be included in the Security Assessment Plan (SAP). The FedRAMP Planning phase also establishes communication channels and mutual storage to maintain documentation to be viewable by all parties, including the federal agency, CSP, and 3PAO. The FedRAMP PMO provides documentation storage called the FedRAMP Office of Management and Budget MAX (OMB MAX) where all parties will be able to coordinate test results, updated documentation, and plans.

Phase Two: Authorization

Full Security Assessment

The Full Security Assessment phase begins testing and assessing the CSO against security controls as outlined in the SAP. This will verify whether the CSP has implemented FedRAMP controls on CSO-related systems and is then further validated by 3PAO. The testing and feedback process will repeat between the CSP and the 3PAO until all remediation actions establish an agreement to acceptable implementation of controls. If a Plan of Actions and Milestones (POA&M) has not already been established, it will be created here to document all remediation items from the assessment. During the assessment, the results will be updated to the POA&M and Security Assessment Report (SAR). Once all results have been addressed and documented, the 3PAO will develop the final SAR and indicate the CSP is ready for the Authorization Process.

Authorization Process

The Authorization Process phase is used to verify all documentation is ready for the agency to sign off on the CSP ATO. The Post-Authorization plans will also be developed, including the finalized POA&M and Continuous Monitoring Plan, ensuring acceptable risk after being granted authorization. The CSP will compile all documentation into the Authorization Package for the agency’s Final Review.

The Authorization package will contain:

- System Security Plan (SSP) (and attachments)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of Actions & Milestones (POA&M)
- Continuous Monitoring Plan
- Signed Authority to Operate (ATO) Letter for agency Authorizations

The agency will submit the Authorization Package to the FedRAMP PMO for review. If approved by the FedRAMP PMO, the status of FedRAMP Authorized will be granted to the CSP to recognize the CSO as compliant with an agency ATO. The CSP will then be published in the FedRAMP Marketplace and will be eligible to provide services to any subsequent federal agency.

Phase Three: Post Authorization

The FedRAMP Authorization process does not end with Authorization. Organizations must continue to monitor their services' quality, maintain alignment to the NIST 800-53 (Rev. 4) controls, and address potential development of risks.

Continuous Monitoring

The Continuous Monitoring phase ensures ongoing quality assurance and addresses additional risks after a CSO has been granted an ATO. To accomplish this, the 3PAO conducts annual assessments to validate any significant deviations and changes to the system. Along with the annual assessments, the CSP will perform monthly scans and assessments. The results of both activities should be well documented to ensure consensus between the agency, the CSP, and the FedRAMP PMO on the development of acceptable risks that occur
after ATO.

Challenges

The FedRAMP Authorization process requires extensive scheduling and strong commitment from the CSP and federal agency. Many obstacles that CSPs and agencies encounter exists prior to engaging in the FedRAMP process. The obstacles will continue to develop into subsequent activities after obtaining FedRAMP authorization. Some of the challenges include the lack of existing system requirements, failures in executing successful security assessments, and the lack of continued commitment after authorization has been granted.

However, the greatest consideration for approaching FedRAMP challenges is to be focused in planning and scheduling activities prior to the engagement of the FedRAMP accreditation process. To be considered a successful candidate for FedRAMP, the process requires considerable amount commitment and dedication from the candidate. One of the specific obstacles is the lack of existing documentation and minimum system security requirements. The most essential piece of documentation is the composition of a fully developed System Security Plan (SSP). The process to completing an SSP can be found in Addendum A – Composing a System Security Plan. A completed SSP is a strong indicator that the system has overcome one of the initial challenges and is likely to be successful in crossing subsequent obstacles.

Conclusion

The FedRAMP’s standardized approach is an essential process to ensure cloud security allowing government operations within the cloud. Because the cloud provides high scalability and availability, agencies are increasingly incentivized to migrate into using cloud computing services as part of their system. FedRAMP provides the answer to the migration process. The assurance provided by its authorization process allows for safe operations to adopt innovative solutions that were not capable by traditional means.

The FedRAMP Authorization process is an extensive development to the system. It requires significant efforts in planning, scheduling, and execution from the system’s organization to be considered successful. The organization’s commitment must also begin prior to engaging the process to increase the probability of success. The commitment is realized by developing the exhaustive procurement of the system’s initial supporting minimum-security requirements documentation and establishing partners who are also dedicated to the success of the accreditation process. Ultimately, to address innovative solutions using cloud services, agencies and their partners must be dedicated to the extensive and comprehensive process of FedRAMP.

Appendix: Glossary

- **3PAO** – Third Party Assessment Organization
- **Agency** – Federal agency that grants ATO to CSP for its CSO
- **ATO** - Authorization to Operate
- **Authorization Package** – Package containing evidence for Authorization including SSP, SAP, SAR, POA&M, Continuous Monitoring Plan, ATO Letter
- **CMMI-** Capability Maturity Model Integration
- **CSO** – Cloud Service Offering
- **CSP** – Cloud Service Provider
- **FedRAMP** - Federal Risk and Authorization Management Program
- **FedRAMP Authorized** – Status granted by FedRAMP PMO that a CSO is compliant with FedRAMP.
- **FedRAMP Ready** – Status granted by FedRAMP PMO that a CSO is ready for FedRAMP security assessment process.
- **FIPS -** Federal Information Processing Standards
- **FIPS 140-2 -** Security Requirements for Cryptographic Modules
- **Gap Assessment** – Pre-FedRAMP tests conducted by a third-party consultant to identify any missing security implementations that is necessary to start the FedRAMP process.
- **NIST** - National Institute Standards of Technology
- **ISO -** International Organization for Standardization
- **OMB MAX** – Information system that acts as a repository for FedRAMP documentation.
- Package Request Form -
- **POA&M** - Plan of Actions and Milestones
- **PMO** - Program Management Office
- **RAR** – Readiness Assessment Plan
- **SAP** – Security Assessment Plan
- **SAR** – Security Assessment Report
- **SSP** – System Security Plan

Appendix: References

- Cloud Smart Strategy (April 2020) found on the U.S, Department of the Interior website's Foundation Cloud Hosting Services
- FedRAMP Moderate Readiness Assessment Report (RAR) Template (August 2018) found on the FedRAMP website's Template Repository.
- FedRAMP System Security Plan (SSP) Moderate Baseline Template (August 2018) found on the FedRAMP website's Template Repository.
- FedRAMP Initial Authorization Package Checklist (March 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 4 - FedRAMP Privacy Impact Assessment (PIA) Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 5 - FedRAMP Rules of Behavior (RoB) Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 6 - FedRAMP Information System Contingency Plan (ISCP) Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 9 - FedRAMP High Control Implementation Summary (CIS) Workbook Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 12 - FedRAMP Laws and Regulations Template (Aug 2018) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 13 - FedRAMP Integrated Inventory Workbook Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Security Assessment Plan (SAP) Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Security Assessment Report (SAR) Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Plan of Action and Milestones (POA&M) Template (March 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Agency Authorization Review Report Sample Template (June 2019) found on the FedRAMP website's Template Repository.
- FedRAMP ATO Letter Template (June 2019) found on the FedRAMP website's Template Repository.
- FedRAMP Annual Security Assessment Plan (SAP) Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Annual Security Assessment Report (SAR) Template (June 2017) found on the FedRAMP website's Template Repository.
- NIST Special Publication 800-53 (Rev. 4 January 2015) found on the NIST website's Computer Security Resource Center.
- NIST Special Publication 800-60 (Rev. 1 June 2004) found on the NIST website's Computer Security Resource Center.
- FIPS PUB 199 (February 2004) found on the NIST website's Computer Security Resource Center.

Kevin Liang, Federal Consultant Development Program

Primary Role

Kevin was a part of the Consultant Development Program at Tevora and was responsible for providing supporting work during assessments and the report writing process.

Notable Accomplishments

Kevin developed multiple personal projects using his established private virtual home lab containing resources and platforms to conduct tests and experiments. The experiments include White-hat hacking projects to breach his personal network and another experiment engaging in available cloud computing services. His objective is to obtain hands-on experience from subsequent research on modern cybersecurity topics.

Certification and Training

Kevin earned his Bachelor of Science in information technology from George Mason University and holds certificate to the NSA/DHA National CAE in Information Assurance/Cyber Defense. He also holds his CompTIA Security+ certification.

Tenure

Kevin was with Tevora from January 2020 until April 2020.

Taiba Zadran, Information Security Associate

Primary Role

Taiba is an Information Security Associate at Tevora and is responsible for providing supporting work during assessments and the report writing process.

Notable Accomplishments

Taiba was previously a part of the Consultant Development Program at Tevora. Before that, she interned at Symantec Corporation through the Year Up program in 2019.

Certification and Training

Taiba is currently attending George Mason University, pursuing a bachelor’s degree in information technology and cyber security. She is currently part of AllCyber, a non-profit organization aiming to advance students’ cyber security skills. Taiba also holds her CompTIA Security+ certification and has completed a CCNA Cyber Ops training program with Per Scholas and was a participant in the National Cyber League competition.

Tenure

Taiba has been with Tevora since January 2020.

Kaitlyn Bestenheider, Senior Information Security Analyst

Primary Role

Kaitlyn is an Information Security Analyst at Tevora and is responsible for providing supporting work during assessments and the report writing process.

Notable Accomplishments

Kaitlyn has served as a high school cybersecurity instructor at Rockland County BOCES Career and Technical School in Nyack, NY, where she helped second year students prepare for their CompTIA Security+. Kaitlyn has also worked as a Digital Marketing Specialist for Silver Tips Tea, where she provided in-house technical support, developed a web loyalty program, and developed a Google AdWords initiative.

She actively contributes to the information security community and has served as a volunteer for the Grace Hopper Women in Computing Celebration (2017) and the Pace University GenCyber Program (2017-2018), has presented at r00tz Asylum at DEFCON25 (2017) and DEFCON26 (2018), Women in Cyber Security Conference (2017-2020), the Community College Cyber Summit (2018), and has guest lectured at multiple colleges and universities all across the country. Since 2017, Kaitlyn has served as the Chief Player Ambassador for the National Cyber League. She runs and regularly appears on their Thursday Night Live Coaching Sessions to encourage students nationwide to participate in CTF competitions to achieve their cybersecurity academic and career goals.

Kaitlyn was also the grateful recipient of the Women in Cyber Security Conference 2019 Rising Leadership Award.

Certification and Training

Kaitlyn earned a Master of Science in information systems from Pace University in Pleasantville, NY in May of 2018 and holds a Certificate in Cybersecurity from Westchester Community College in Valhalla, NY. Kaitlyn also holds her CompTIA Security+ certification.

Tenure

Kaitlyn has been with Tevora since June 2018.

Troy Dahlin, Senior Consultant Federal and Third-Party Risk

Primary Role

As Tevora’s Senior Consultant for Federal and Third-Party Risk practice areas. The Federal practice area provides clients with FISMA, FedRAMP, DFARS, NIST CSF and other related standards. Troy mentors consultants, manages client relationships, assists with pre and post sales activities, and oversees projects from the inception to the closeout presentation to ensure that every project exceeds client expectations.

Notable Accomplishments

Troy started in the Information Assurance field as a US Navy Information Systems Security Manager in 2001, responsible for the configuration and hardening of US Navy IT Assets meeting FISMA regulations and DITSCAP Accreditation process.

Troy retired from the US Navy Reserve after 24 years of combined Active and Reserve duty as an IT Chief Petty Officer having performed as the Senior Enlisted Leader for two different units (Inshore Boat Unit 25 and Beach Master Unit 2). Troy’s last duty station was Commander Navy Cyber Command (US Tenth Fleet) in Ft. Meade, MD.

In 2017 he started work as the Corporate ISSM implementing and managing the RMF implementation within the company and supporting DoD and Federal customers. Also, with the implementation of the DFARS/ CMMC within the Corporate network he was the primary expert on implementation activities. As the Corporate ISSM, he was also responsible for incident handling, insider threat mitigation, investigations, self-assessments and managing COMSEC transfers.

Certification and Training

Troy holds the Certified Information Systems Security Professional (CISSP), CompTIA Security+, GIAC Certified Incident Handler (GCIH) certifications and earned a Bachelor of Science degree in computer networks and security from University of Maryland University College (2017).

Tenure

Troy has been with Tevora since the beginning of 2020.

TEVORA™

Go forward. We’ve got your back.

Compliance – Enterprise Risk Management – Data Privacy – Security Solutions – Threat Management