* **73 of 81** confirmed registrants attended the FedRAMP ISSO Training
* We received **67** evaluation forms from **93% of participants**

**August 2018 Results**

|  |  |  |
| --- | --- | --- |
| **ID** | **Question** | **Score** |
| 1 | The objectives of the session were clearly defined | 4.71 |
| 2 | The session was well-organized | 4.66 |
| 3 | The learning topics were relevant | 4.73 |
| 4 | The content was organized and easy to follow | 4.70 |
| 5 | I will be able to apply what I learned quickly and easily | 4.43 |
| 6 | The session was a worthwhile investment of my time | 4.73 |
| 7 | The session met my overall expectations | 4.66 |
|  | **Session Average** | **4.66** |

**August 2018 - Participant Feedback**

**Question 1: What was the most effective part of the training?**

* All of it (7x)
  + I didn't really know much about the FedRAMP process prior to today's training
  + Really impressive
  + The whole training was very interesting
  + Everything that I heard was critical of the success of my organization. It would be nice if there was something something in place for organizations that are new to this process
  + All was informative
* Continuous monitoring approach (5x)
  + Authorization deep dive. Post-authorization + CM review
* FedRAMP JAB-ATO & Agency ATO information
  + JAB (4x)
    - I thought it was helpful that the P-ATO was explained for JAB authorizations
    - Getting a better understanding of the JAB and the procedures
    - Process review role of JAB
  + Agency (4x)
    - The requirement that if a CSP is FedRAMP Authorized the agency still has to have an agency ATO. Also, filled in a lot of blanks that I had
    - Approach/Agency Roles & during authorization topics
    - Authorizations Deep Dive
* Session Content (5x)
  + The presentation was tailored to those already familiar with FedRAMP, so the language used was very easy to understand and 100% relevant to what we do daily
  + Great overview, handling of materials & challenges
  + Understanding the process
  + Content is relevant and useful in an ongoing way. (i.e. used to refer to next time). Content is rich
  + Everything was well organized
* Session Materials (5x)
  + It was helpful having hard copies of the slides for note taking (of late, it has become common place to have soft copies on a website)
  + The session provided detailed information with slides to augment the session to ensure all information is communicated
  + Presentation of slides
  + Print outs + corresponding commentary
  + The presentation slides
* Panels & Presenters (14x)
  + Questions from audiences; Panel
  + The panels were very effective
  + Question and answer segments
  + The FedRAMP process, panel board very good. Helped a lot
  + Speakers & materials
  + Educating ISSOs on use of FedRAMP resources - primarily experience from personnel of their implementations at Agencies
  + The presenters were very knowledgeable concerning each topic
  + Delivery of the content, all presenters were very knowledgeable and able to answer questions
  + Individuals were well informed
  + Lesson learned from previously deployments. Question answer sessions with panels. Presentations and exercises
  + The Q&A session with the panel & the group exercise was very informative Understanding that the agency need 2 have a continuous lines of communication open with CSP + FedRAMP PMO + 3PAO
  + The GSA team getting "the feedback" from cabinet-level agency workers
  + Hearing from various SMEs that have been through FedRAMP process
  + Expertise of all stuff to take on questions & provide viable information & guidance
* Exercises (6x)
  + Going through the examples; Going through the steps individually
  + The exercises
  + Exercise with Laurie and Jenny
  + The exercise were helpful. It was great to step through them with the group
  + Practical/real-world examples
  + Break out sessions
* Overall clarifications
* Not straying off topic
* Found new resources to help our cloud security program

**Question 2: What suggestions do you have for improving a future training session?**

* Nothing! (6x)
  + This was great. Please have more of it.
  + I loved how you stayed on task, great training!
* OMB MAX (1x)
  + Include more info on OMB Max and how it can be utilized
* Q&A (9x)
  + Extent time to include longer Q&A sessions
  + The session and information presented were adequate. There is not much to change other than maybe adding more time for Q&A
  + None Q&A time
  + Time boxing the Q&A better to stay on schedule
  + May help to build in Q&A between topics to allow more interactions
  + Restrict the questions for the end of each section
  + Document questions from audience and distribute as FAQs for participants
  + Reduce the time on audience questions to allow for a deeper dive into the material
  + Repeat the questions that people ask before giving the answer
* Exercises (4x)
  + More exercises; if more exercises stretch training to 1.5 or 2 days
  + Exercises on overall process. Workflow from beginning to end
  + More teamwork exercises
  + Additional collaborative exercises with colleagues
* Process Materials and Content (10x)
  + Have an opening flow chart that shows the basics: (JAB ATO, Other Agency ATO, systems that can leverage the results of the ATOs
  + Add few use cases of Agency issues
  + Would also like to go through the materials more in depth.
  + It will be great to see a FedRAMP ATO class
  + Send handouts prior by email. Spell out acronyms when starting with them.
  + Less acronyms
  + Who are the "Big 3PAOs"? Mention that FedRAMP does not offer ATO'S, rather P-ATO, and the Agency offer the ATO.
  + Reporting & change management
  + More discussion of how GSA FedRAMP +DHS CDM Program align or relate to each other
  + More basic on training
* Presenters / Panels (3x)
  + Speakers don't talk over each other / finish each other's sentences
  + More actual AO's from other agencies
  + Having this training for CIO / CISOs from the different agencies. Have some CSPs security personnel at the training
* Logistics (10x)
  + Something was not working with the sound system. Some people could be easily heard, some people could not be heard.
  + Don't bleed activities into Break/Lunch periods
  + 2 days - deep dive
  + Longer training to allow more time for questions
  + More or increase to two days; virtual training
  + Training certificate should be provided to participants
  + Training should be provided for CSPs
  + It was a lot of material to cover in one day -> possibly expand to two days
  + Hard to hear at times - especially questions from audience. Maybe more speakers, great handout package (suggest to a page of links and contacts)
  + Agency specific telecon / webinar options
* Demonstrations of some of the system FedRAMP uses for its internal processes may provide deeper insight

**Question 3: What topic or activity would you like to see in a future training session?**

* JAB ATO vs. Agency ATO details (3x)
  + Roles of initial reviewers of JAB & agency ATO
  + Specific to agency responsibilities for JAB ATO (not agency sponsored). It was touched on but it would be good (1/2 day session) for new ISSO's on what to do and how to handle CSPs.
* FedRAMP and DHS CDM / FISMA (3x)
  + How FedRAMP fits into the picture with CDM, FISMA
  + CDM
  + Relationship between GSA/DHS/NIST (how to navigate at an agency)
* The money aspect. We are an asking a lot of CSPs and other companies, when does the money start. We talked about a kick off meeting, but it doesn't seem like they would do any work without knowing that they are getting the contract and approved for said portion of time.
* Interagency Communications & Collaboration (3x)
  + The presenters emphasised collaboration. Adding small group activities with a diverse group representing different agencies would help facilitate this.
  + An overall view of all the interagencies communications (weekly, monthly dial- in calls) so others can join in
  + Deep dive on agency collaboration for ConMon
* Additional Types of Trainings (14x)
  + Have to go through all the materials. Application of privacy.
  + I hope you have more of these, we have more people in our dept. that would benefit from this
  + FAQs / Tips of the trade. Ex) Just because a vendor says they are FedRAMP Authorized, they may not be. Always check the dashboard site for verification
  + Duties of system owners / program manager for IT systems. Acquisition - what the COR and other specialists must look for prior to procuring cloud services.
  + Separate training should be provided for ISSOs that support CSPs
  + Specific breakouts and going over A&A High levels, OMB MAX, FedRAMP's site
  + More on tailoring & agency/ csp interactions (what worked, what doesn't)
  + How to prepare for the first cloud migration for the Agency?
  + Creating effective security briefing for CX level
  + How to achieve greater visibility into a CSP data center. Real time monitoring of audit processes
  + Reporting to Agency SOC
  + Deep dive into what capabilities (products authorized for the big cloud vendors (AZURE or AWS)). Overview of types and categories of ATO capabilities that are available to leverage
  + Devops! Managing and transforming Devops
  + Would recommend incorporating the "navigating FedRAMP.gov" website into the agenda (15 mins) instead of a working lunch topic
* Additional Levels of Detail (13x)
  + Deeper illustrations, transitioning, scenarios from a standard host platform to cloud
  + Session on reviewing sample SAP, SAR, etc. and pointing out flaws
  + ATO packages that are Customer, Contractor, CSP
  + Significant Changes & Deviation Requests
  + Common order POA&Ms / challenges from CSPs
  + Discuss future changes to FedRAMP
  + SLAs with CSPs in-depth
  + Deep dive into the OMB max for all
  + Continuous monitoring - scans and reviews
  + Any procedures documentation for this process?
  + Exiting or cancelling (revocation) acceptance of CSP risks
  + More on continuous monitoring
  + Leadership inclusion

**Question 4: Based on what you’ve learned today, how likely are you to leverage what you learned and undertake a FedRAMP Agency Authorization?**

* FedRAMP Authorized CSP in-use already
  + We already have 2 systems of FedRAMP approved CSPs. This will let me go into a deeper dive into these packages.
* Immediately (2x)
* Likely / Very Likely / Extremely Likely (27x)
  + I realized I have additional tasks for some of the FedRAMP systems I inherited
  + It's a lot of work but we will continue to document
  + I will use what I have learnt to make sure my Agency is FedRAMP compliant
  + This has assisted with lessons learned and red flags to look for when providing doc prep services for customers
  + I will leverage the marketplace and incident management repository mentioned in class
  + Feel much more comfortable with the FedRAMP process
  + Not impossible - difficult- still getting the concepts clear in mind
  + My agency has dozens of non-ATO'ed systems. Current process is cumbersome, unwieldy, and high inefficient
  + For contacting the other Government Agency that processes / grants an ATO for the SaaS and setting up a joint review.
  + Look at level of cloud services that are ready to be used (SAAS IAAS). Look into what ATO's have been used by my agency.
* More focus to ensuring consistency between SSP, SAP, SAR, POA&M
* If the request is made-immediate; will still create process procedures.
* This information presented solidified the knowledge of the A&A process. The FedRAMP tailored info makes it very easy to implement within our agency. We will definitely leverage what we learned today

**Question 5: What was the biggest myth debunked during today’s session?**

* Relationship between JAB-ATO / Agency ATO (6x)
  + FedRAMP JAB-approved ATO means a system that inherits from the FedRAMP system does need to review all controls. The Agency AO has to accept the risk.
  + JAB P-ATO does not require an agency ATO was properly debunked.  
    POA&M review
  + P-ATO is not an Authorization for Agencies. It is the agencies responsibility to accept risk
  + The P-ATO. I now have a much better definition of it
  + Agencies have to provide a JAB like internal review
  + FedRAMP P-ATO is the ATO that is needed to use the CSP
* Agency ATO Process (10x)
  + The simplicity
  + At the beginning we were told that on average, each cloud ATO is "reused" 7 times. Then we were basically told to not trust the CSPs and to check everything. Where is the time savings?
  + The usual FedRAMP Ready vs. Approved
  + That some providers are certified. The site will give you the skinny.
  + FedRAMP is hard!
  + It's possible to get FedRAMP certifications in a shorter timeframe
  + The misconception some individuals have that obtaining a FedRAMP authorization does not require significant involvement on their part
  + Leveraging agencies don't have to review risks for themselves
  + That partnering or sponsoring vendor is extremely challenging.
  + That agencies don't have to take such an integral role in FedRAMP ATO process
* FedRAMP Requirements (2x)
  + That FedRAMP prohibits data outside the US
  + CM
* Claims to CSP FedRAMP Authorization (2x)
  + How many cloud providers are FedRAMP certified
  + The authorized vendor must be on the FedRAMP site to be officially authorized
* Different entities within the agency are leveraging CSPs that are not FedRAMP
* CSPs are not all "created equal"
* That the FedRAMP process and and offices/programs that manage the processes are some sort of black hole, there are actual people you can contact and they will assist you.
* FedRAMP deployment is complex
* FIPS compliance does not mean FIPS validated. Just because vendor claims they are FedRAMP doesn't mean they are. They are not if they are not listed under FedRAMP marketplace.
* Buy-in by the entire agency
* Maria Roat is coming back to GSA
* Ability to work in the cloud!

**Question 6: What is the biggest roadblock that still exists at your Agency regarding FedRAMP authorization?**

* Leadership Involvement & Direction (3x)
  + Agency leadership acceptance of another agency's issuance of an ATO
  + AOs participating in Continuous Monitoring
  + Misinformation from vendor's to agency executives. Executive lack of knowledge around FedRAMP. DHS TIC reference architecture. A lack of clarity moving forward.
* Policies & Guidance (2x)
  + Agency level guidance is lacking. Some IT Opps/Security do not understand the requirements for A & A
  + We must coordinate with another agency for Enterprise solutions. They don't understand Agency specific requirements
* Knowledge of the Authorization process (11x)
  + Lack of knowledge of the process. There are many combinations and permutations to deal with
  + Understanding that just because a provider is FedRAMP doesn't mean they can automatically use it
  + Education + lack of "evangelist"
  + Clear understanding of stakeholders roles + responsibilities
  + Agency & organisational cooperation & acceptance for roles & responsibilities
  + Lack of understanding between JAB & Agency ATO and requirements of both.
  + Lack of understanding about Agency ATO once inherited. Inheritance remains unclear
  + Difference in quality standards between Agencies in acceptance of FedRAMP ATO
  + FedRAMP-ready (inclusion of an IaaS) - not FedRAMP Authorized
  + All necessary roles obtaining and maintaining OMB Max access
  + Monitoring the closure of open POA&Ms which are long overdue
* Lack of Cloud Computing Knowledge (4x)
  + Lack of cloud knowledge RE: "Lift and Shift" misconception (cloud busting)
  + Lack of expertise at Agency with cloud process, still no solid procedures in place at my agency
  + Decision to deploy cloud as a solution
  + Since we fell under a bigger Agency we normally use their contracts and stuff as we go for new solutions. This provides an issue because we don't always get to be at the meetings for this type of projects as they handle it
* Industry Misconceptions / Miscommunication (6x)
  + People (esp. vendors) say they are FedRAMP...something, but are not approved
  + Getting the information from the CSPs (e.g. annual test plans)
  + Managing the professional service providers
  + Visibility to assets that exists in authorization boundaries
  + Consistent availability of CSP as we're going through the process
  + Responsiveness often not there
  + Obtaining monthly ConMon data / reports
* Resources and Funding (9x)
  + Man power to sponsor ATO's
  + We haven't fully stood up our cloud systems management group and / or processes
  + The workload of internal responsibilities, OIG Audits, shadow IT and other tasks
  + Document review and updates
  + The necessary resources to ensure FedRAMP requirements (e.g. POA&M mitigation, etc.) are met
  + Funding, Architecture
  + Resources + knowledge based on what it is + how to leverage
  + Budget
  + Devops, funding, legacy applications with not funding

**Question 7: How can we improve? Any other comments?**

* Create program. Should be expanded to run more than just quarterly
* Recommend adding like CSP point of contact for the POA&M in the monthly ConMon summary
* What happens to POA&Ms that are long overdue per FedRAMP remediation time frames
* Need the answers about the DHS CDM Program and how that will affect the FedRAMP Process along with are these going to be approved since its a mandate
* Make this available via a webex type technology. There are ISSOs that need this training but cannot travel to Denver or DC for 1 day. Or, record this session and make available via the MAX.gov
* Is there a way to create a workgroup for agencies to collaborate (maybe a forum)? It would be useful to know when new CSP Kickoffs occur. VA is trying to get an understanding of what is required (assessments/testing/reporting) for onboarding CSP
* Address when CSPs we ask the questions ""You are the only agency asking these questions, if you want the info go to the JAB because they have already done the review and approved the deviations""
  + What results do we have if we don't agree? Or if their timeline is too far out?
* Do you allow agencies participate in JAB reviews? Or listen in?
  + HHS has allowed other agencies to listen during their monthly ConMon meetings
* How long are ORs permitted to go? 3 years, more? Can these be worked at? It's hard to address when JAB accepts ORs for years. What can we do? Seems CSPs ask for an OR or Risk Reduction if they don't want to address
* Looking forward to the virtual FedRAMP ISSO Training
* Monthly outreach if it won't be too challenging. Wider knowledge and collaboration with Agency / IG Questions and CIO / CISOs
* I enjoyed the expert panels. Good way to break up and enhance training
* Really would be helpful if GSA could approach FedRAMP the way DHS has with CDM. We need funded tools and services to transform the codebase to help us migrate apps / services to cloud