Understanding FedRAMP

- What it is
- FedRAMP's primary objectives
- Changes are a-comin!!

Importance of FedRAMP in Cloud Security

- Cloud Security Landscape
- Risks mitigated by FedRAMP
- The value of standardization

Stakeholder Roles and Contributions - Overview

- List of Key Stakeholders:
  - General Services Administration
  - Cloud Service Provider (CSP)
  - Third-Party Assessment Organization (3PAO)
  - Federal Agencies

Role of the Cloud Service Provider (CSP)

- Offering cloud solutions to federal agencies
  - Can be tailored to specific agencies
- Ensuring solutions meet FedRAMP security standards
- Responsible for Continuous monitoring and updates

Role of the Third-Party Assessment Organization (3PAO)

- Perform an objective evaluation of CSPs
  - SAP (who, what, where, when and how)
- Validation of security practices (the assessment!)
  - Examine (documents, processes)
  - Interview (CSP stakeholders)
  - Test (pen test, scans)
- Produce a SAR
- Importance in the FedRAMP authorization process – impartiality & consistency

Preparing for Audits and Reviews

- Types of audits and reviews
- Documentation requirements
- Best practices for audit preparation

Factors Affecting Assessment Depth

- System classification (L,M,H, LI-SaaS)
- Data sensitivity
- Operational complexity
- Compliance requirements

The Importance of Readiness: Setting the Stage

- Why readiness matters
- Impact on assessment success
- Role in reducing delays and costs
- CSP’s role in ensuring readiness

Overview of the FedRAMP Authorization Process

- CSP Steps in the Authorization Process
  - Prepare (for an assessment)
  - Engage (with a 3PAO)
  - Conduct (3PAO conducts the assessment)
  - Report (SAR and POAMS go to AO)

- Interplay between stakeholders during assessment & authorization (Agency & CSP)

Breaking Down the Security Assessment Report (SAR)

- What is a SAR?
  - Report produced by 3PAO at end of assessment
- Objective of SAR
  - outlines any findings/gaps
  - contains a CRITICALITY, a balanced risk discussion, recommends (or not) any remediation
- Key Components
  - Executive Summary
  - Details
  - Recommendations

Common CSP Pitfalls

- Pitfall 1: Inadequate preparation on CSP's part
- Pitfall 2: Poor communication
- Pitfall 3: Ignoring risk management

- How to avoid these pitfalls
  - Prepare, - stay ready so you don't have to get ready!
  - Stay engaged
  - Follow through on recommended actions
  - Con mon!

The Importance of Speed in the Agency Path

- Time-to-market advantages
- Reduced wait time for authorization
- Impact on project timeline

Relationship Building: A Cornerstone of Agency Path

- Importance of networking
- Building trust with agencies
- How relationships impact the authorization process

CPSs: Interacting with Agencies

- Effective communication strategies
  - Before (SAP)
  - After (SAR)
  - Con Mon
- Mistakes to avoid
  - Ignoring requests! BAD CSP!
- How to engage constructively
  - Monthly tag ups
  - Ad hoc emails/phone calls/tag ups

The ATO (Authorization to Operate)

- Time bound
- Event bound

} ATO with conditions

- Legal and Regulatory Implications (FISMA)

Pitfalls?
Too short – e.g. 6 months - increases workload on the Agency (number of reviews, documentation etc)

Ongoing Authorization – OMB mandate, increased emphasis on continuous monitoring

Roles and Responsibilities Post-ATO

- Compliance Monitoring
- Reporting Requirements
- Periodic Re-assessment

Continuous Monitoring in FedRAMP

- Definition and importance
  - A ‘near real time’ knowledge of the security posture of a system
  - FedRAMP outlines activities for daily, weekly, monthly annual monitoring
- Role in ensuring up-to-date security
  - Required monthly summary of status and events to partner Agency,
  - Notification of any significant changes
- Collaboration between CSPs and federal agencies
  - Tagups , ongoing communication

Collaborating with the PMO: Best Practices

- Communication Channels
- Project Milestones and Tracking
- Documentation and Record-keeping

FedRAMP and the Future of Federal Cloud Security

- Evolution of FedRAMP
  - EO 14028 is revamping and modernizing FedRAMP
  - Prioritizing use of Cloud
- Emerging trends and challenges
  - Multi-cloud, hybrid, edge computing, AI

FedRAMP and a whole lot to LOVE

- OMB draft memo released for public comment Oct 2023
- Modernizing the Federal Risk Authorization Management Program (FedRAMP)

- WHAT'S IN IT??? TELL US, TELL US!

FedRAMP and a whole lot to LOVE

- Acknowledgement that FedRAMP is IaaS biased
- Reorientation of the program to better serve SaaS products
- Reorientation of the PMO as a consultant, expertise driven partner

FedRAMP and a whole lot to LOVE

- New pathways to authorization
- Staying ahead of the curve
  - Multi-Agency panel replacing the reviewing documentation role of the JAB
  - ‘Joint –Agency authorization’ where any group of 2 or more agencies sign off in an ATO together
  - PMO encouraged to find agencies and support this effort
  - PMO continue to oversee the process for all authorizations

FedRAMP and a whole lot to LOVE

COMMON SENSE!!

- The authorization to use without FR ATO (a clearer than ever articulation of what kinds of cloud services are exempt from FedRAMP)
- Ex: ‘Ancillary services’ where compromise poses ‘negligible risk’ to govt data (web stats/page views etc from agencies’ public web sites)
- Recognizing the value of newer industry practices that offer improved security (and helping agencies benefit from newer approaches)

FedRAMP and a whole lot to LOVE

AUTOMATION!

- FedRAMP to start implementing receiving documents in machine readable format! (OSCAL)
- The Good? HOLEY HANNAH! No more word docs and spreadsheets!
- The Bad? CSPs had better become proficient in OSCAL and getting their documents into an acceptable format.

FedRAMP and a whole lot to LOVE

Say WHAT?!?!

“In general, to promote both security and agility, Federal Agencies should be using the same infrastructure relied on by the rest of the CSP’s customer base”.

Most SaaS CSPs already do this… It makes little business or economic sense to have a separate gov environment.

.

FedRAMP and a whole lot to LOVE

PMO encouraged to ‘increase agency reuse, drive more authorizations, and reduce the burden and cost’ of authorization.

What we’ve already seen?

- PMO adding staff to help alleviate the backlog of systems ‘in the pipeline’
- FedRAMP holding monthly ‘Office Hours’ to help meet the needs of CSPs and 3PAOs.
- Single responses from CSPs WRT to emergency directives

.

FedRAMP and a whole lot to LOVE

What CSPs would like to see?

- Just as it's counterproductive to support 2 environments, it is inefficient for a CSP with a global presence to have variable restrictions on non-US staff preventing them from bringing their expertise and talent to the problems the govt faces.
- The acceptance of other industry standards/certifications (SOC2, ISO27001) as an overlay to controls – many overlap. Let's put effort into answering and assessing these once.

Takeaways

- Importance of standardized cloud security
- Collective effort of stakeholders
- The future-proof nature of FedRAMP

All document templates for FedRAMP documentation can be found on https://www.fedramp.gov/documents-templates/

Contact Ann Marie Keim at:
annmarie.keim@fitsi.org or aa4gov1@gmail.com
M 334-224-0359
linkedin.com/in/ann-marie-keim-507108a