CLOUDSEC2019

PICTURE THIS!

SEE. SECURE. GO FURTHER.


CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
Katie Lewin
FedRAMP and its impact on cloud security
Federal Director CSA
www.cloudsec.com
#cloudsec

FedRAMP Background

Need

- Federal agencies reluctant to use cloud technology: security, cost
- No consistent application of security controls

Goals

- Ensure the use of cloud services **protects** US Federal Government information
- Enable **reuse** of security certifications across the Federal government wherever possible to save money and time

FedRAMP Background

Solution

- Do once, use many times – Establish a process, Do it right, Reuse results across US Federal government
- Transparency – Share information, encourage and address input, builds trust among CSPs and US Federal government
- Validate Security Certification - FedRAMP authorization process promotes uniformity and trust in the results
- Centralized, secure repository – where agencies can access security packages for expedient authorizations

FedRAMP by the Numbers

CLOUDSEC2019
PICTURE THIS!

We cover more than

5 MILLION assets available for Federal use

&

1/3 of the world's internet traffic through our program

4 security baselines to match government use to risk

- HIGH *(421 controls)*
- MODERATE *(325 controls)*
- LOW *(125 controls)*
- LI SAAS *(36 controls*)*

143
Authorized Cloud Services

1000+
Agency Reuses of Authorized Services

156
Participating Agencies

220+
Participating Industry Partners

POINTS OF CONNECTION

750+
Annual meetings with agencies and vendors

4,100+
Followers on Twitter

11,000+
Stakeholders on listserv

20,000+
Questions answered through info@fedramp.gov

#cloudsec

Success Factors

- **Identify program authority – FISMA**
- **Get high level sponsor- Federal CIO**
- **Begin with Technical – address what (controls) and how (processes, procedures) not who**
- **Provide means for feedback from government and industry**
- **Roll out processes/procedures for comment often – while there is time to incorporate comments**
- **Publish as much information as possible – guides, FAQs, templates, tips&tricks**
- **Remain flexible – allow changes to the program**

Lessons Learned

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Begin with moderate security level – 70% of systems at moderate level

Don’t leave CSP to navigate the process unaided - Work with CSP to determine readiness:

- Tailor the authorization to type of product: IaaS, PaaS, SaaS
- Start with basic penetration test - key indicator of security maturity
- Review key documentation after test results
- Look at vulnerabilities and risks identified in test results and documentation

Lessons Learned

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Authorization Process

- Tailor test cases for unique architectural design
- Information security is a business issue
- Technology is easy
    - Business processes and procedures understood by staff make security work
- Risks are not all externally generated – internal risks must be addressed

Continuous Monitoring

- Same tools used for testing and on-going continuous monitoring
- Locking down the system critical to successful testing
- Planning significant change in advance
- Alignment of scanning, patching and testing schedules

FedRAMP Now

- **More Clouds to Choose From**
  - Increase Authorized Cloud Services
  - Increase Re-used Authorizations
  - Move FedRAMP-Ready CSPs to In-Process or Authorized CSPs
- **Transform Security Authorizations**
  - Automate the Authorization Process
  - Continue to push FedRAMP Tailored Authorizations
- **Strengthen FedRAMP Community**
  - Connect the Community Through Industry and Agency Days
  - Enhance 3PAO Resources with Updated 3PAO Requirements
  - Promote Better Understanding of FedRAMP and the Authorization Process

FedSTAR– Case for Change

- Secure environment - vital to any deployment of cloud technology
- Security concerns – always a major challenge to any cloud implementation
- 30+ certification systems world wide
- CSPs forced to spend resources to implement and to monitor compliance with multiple certification systems
- Multiple security systems - Barrier to market entry
- Need for commonly accepted certification system used across customer bases

Proliferation of Security Certifications

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Fig1. Compliance Templates Provided By Microsoft

Goals

- **Build a foundation for mutual recognition between national, international and sector specific security certification, attestations and accreditations**
- **Grant a trusted certification**
- **Reduce the compliance cost for CSPs that want to meet requirements of both industry and government**
- **Use a common framework for deployment**
- **Support requirements for continuous monitoring**

Solution

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- **DO NOT develop a new certification system**
- **Address need for secure environment with common security assessment system(s)**
- **Start with security assessment systems that have common authority/approach/level of review – Don't boil the ocean**
- **Establish areas of mutual recognition among systems**
- **Build frameworks that can be used across systems**
- **Where to start:**
  - **FedRAMP and STAR are among the most used cloud certifications worldwide**
  - **Not compatible as deployed, but have basic elements in common:**
    - **Rely on established standards**
    - **Used control-based reviews**
    - **Require independent 3rd party assessments**

Why STAR & FedRAMP?

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- **FedRAMP and STAR are among the most used cloud certifications worldwide**
- **Not compatible as deployed, but have basic elements in common:**
  - **Rely on established standards**
  - **Used control-based reviews**
  - **Require independent 3rd party assessments**
- **Allow CSPs to leverage the areas of overlap between the FedRAMP Moderate and CSA CCM**
- **Reduce level of effort required to get FedRAMP-STAR or STAR-FedRAMP certifications**
  - **Establish a framework to facilitate security accreditation from FedRAMP to STAR – first step**
  - **Establish a framework to facilitate security accreditation from STAR to FedRAMP**
- **Develop processes that facilitate CSPs with a FedRAMP moderate accreditation to obtain STAR certification through audit of the compensating controls**

Measures - examples

- Readiness/Preparation Time - effort required to prepare for a STAR Certification audit starting from a position of FedRAMP Moderate compliance
- Audit Time – after documentation is submitted for STAR Certification, how much time does it take to get the STAR certification
- Skills Base - required to complete a FedRAMP audit.
- Accuracy of Mapping and Gap Analysis - qualitative measures the level of accuracy in the "CCM-FedRAMP Mapping and Gap Analysis".

Next Steps

- Ongoing meetings with pilot CSPs and 3PAOs
- First pilot scheduled for late summer 2019
- Provide "CCM-FedRAMP Mapping and Gap Analysis" document including FedRAMP – CCM gap analysis
- Begin to collect data from pilots
- Establish a Focus Group
  - Recruit members from across cloud security community:
    - STAR Certification auditors
    - Independent 3rd party assessors for FedRAMP
    - CSA DC Chapter Advisory Group
    - CSA Members

Legislation

- GSA announced the FedRAMP Ideation Challenge requesting all stakeholders submit ideas on how to improve FedRAMP.
- Bill to codify FedRAMP introduced in this Congress –FedRAMP Authorization Act
  - Codifies compliance with FedRAMP processes
  - Establishes a presumption of adequacy security assessments conducted under FedRAMP
  - Requires reporting of metrics on the length and quality of assessments
  - Requires FedRAMP PMO to find ways to automate their process


CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
THANK YOU
Katie Lewin
Federal Director, CSA
www.cloudsec.com
#cloudsec