Possibilities

#CiscoLive

Building and Running FedRAMP System at Cisco

(Federal Risk and Authorization Management Program)

Troy Sherman
Principal Engineer
Information System Security Officer

DGTL-BRKSEC-2005

Agenda

- Introduction
- What is FedRAMP?
- Why Do it?
- Things that affect FedRAMP
- Getting an ATO (Having the Baby)
- Passing the 3PAO Audit
- Keeping your ATO (Care and Feeding)
- Running the Business
- Conclusion

Introduction

Introduction

- 23 years on Halloween at Cisco
- Security for over 15 years
- FedRAMP Background
  - First Authority to Operate (ATO) at Cisco – FedRAMP Moderate
  - Have worked on 3 separate ATO's
  - I am the Information Systems Security Officer (ISSO) for 2 ATO'ed Systems
    - Webex Meetings and Collaboration
  - Worked with the FedRAMP Program Management Office (PMO) on FedRAMP security requirements
  - Part of team that created many of the standards used at Cisco for FedRAMP

What is FedRAMP?

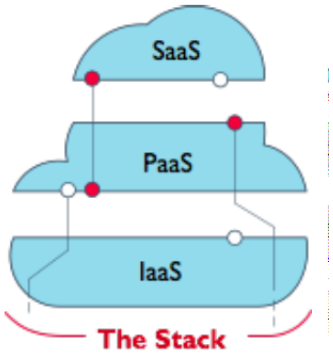
What is FedRAMP

- **Fed**eral **R**isk and **A**uthorization **M**anagement **P**rogram
  - Standard allows agencies to purchase approved cloud systems
  - US Government-wide standard for Cloud Service Providers (CSP)
- Allows agencies to purchase approved cloud systems
  - IaaS, PaaS, SaaS, etc
  - Each level needs an ATO
    - IaaS
    - PaaS
    - SaaS

https://www.fedramp.gov/

What is FedRAMP

- Example – AWS has FedRAMP Moderate ATO
- If we run our SaaS in AWS we will have a FedRAMP ATO
  - Incorrect
- Each level needs an ATO – IaaS or PaaS ATO does not equal a SaaS ATO



https://www.fedramp.gov/

What is FedRAMP

- 2 types of sponsorships – Agency and JAB (Joint Authorization Board)
  - JAB is DHS, GSA and DoD
    - Department of Homeland Security, General Services Administration, Department of Defense
- Cisco has only received Agency sponsorships
  - Easier to get an agency to sponsor a product – JAB only takes a limited number of new sponsorships each year
- There are many more agencies than the JAB
  - Increases the ability to get an ATO

NIST is your Friend

- FedRAMP has 4 different levels based on NIST 800-53 (only thing you need to remember from this presentation)
  - Tailored – Self Audit
  - Low – Some of NIST 800-53
  - Moderate – More of NIST 800-53
  - High – All of NIST 800-53
- Took me a year to figure out that NIST is the root of all FedRAMP
  - Learn the controls and you will be a FedRAMP expert

System Security Plan (SSP) is Root

- SSP is the main document that a system is audited against
- Has all the answers to the NIST 800-53
- Has the boundary diagrams defining your system – Section 9
  - Section 9 is very important – sponsor needs to understand the system based on that section
  - Shows the boundary diagrams – the **Boundary is King**
    - From the old days – hard and crusty on the outside is the boundary
    - Everything that flows in and out of the boundary needs to be controlled
    - Most controls are in and around the FedRAMP boundary
- Checked into max.gov for all agencies to download

SLA's for FedRAMP Security

- FedRAMP requirements
  - Security vulnerabilities to be fixed within the SLA's
- There are 3 security levels for FedRAMP
  - High
  - Moderate
  - Low
- SLA for each is
  - High – 30 days remediation
  - Moderate – 90 days remediation
  - Low – 180 days remediation

Missing the SLA's for FedRAMP

- FedRAMP and the Sponsor or JAB take the SLA's very seriously
- There are 2 things that can happen when an SLA is missed
  - Detailed Finding Review – first step to losing an ATO
  - Corrective Action Plan – CAP – last notice before losing an ATO
- Missing SLA's means
  - Detailed Finding Review –
    - 5 or more highs 30 days late - 10 or more moderates 90 days late
  - Corrective Action Plan –
    - 5 or more highs 60 days late – 10 or more moderates 120 days late

https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Performance_Management_Guide.pdf

Why Do It?

Why Do FedRAMP

- Customer list includes
  - Federal Governments
  - State Governments
  - Local Governments
  - Native American Nations
  - Research Centers
  - Critical Infrastructure

Why Do FedRAMP

- Critical Infrastructure is usually defined as:
  - All non .mil or .gov agencies
  - Commercial customers that produce items the US government buys
  - Commercial customers to do not have access to max.gov and the “package”
    - Will talk more about that later

Why Do FedRAMP

- Many FedRAMP products take more work to manage, audit, and staff
  - Monthly meetings
  - US Staffing usually
  - Paying for annual audit
- Usually means the product can charge more for the service

Things that affect FedRAMP

Things to include/think about/issues

- Timing of your ATO
  - Federal budgets are complete in October
    - Get your ATO in December there could be no budget to buy your FedRAMP system until next budget
- Speed of sales can be slow vs. a commercial product
  - Sponsor could be involved with a sale
  - Many government agencies have an additional ATO in addition to FedRAMP ATO
    - Agencies had cloud requirements before FedRAMP that still apply
    - Agencies have additional controls they might add to the FedRAMP system
      - Can and has included more NIST controls to qualify to be used

Things to include/think about/issues

- Sizing of your system
  - How large do you need to build to?
    - Our first build to support 50k active users
- One large agency could be larger
  - Department Health and Human Services 79k employees
  - Department of Homeland Security 240k employees
  - Department Veterans Affairs 380K
- Be prepared to scale quickly if one large agency is added to the a FedRAMP system

Getting the Authority to Operate (ATO)

Having the Baby

Getting the ATO

- Sponsor/Program Management Office (PMO)
- How long and hard it is to get an ATO
- How hard is it to get an ATO?
- What is a corporate service?
- Interconnect Security Agreement (ISA)
- Full Audit of all NIST controls for your ATO
  - High, Moderate, Low
- System Security Plan (SSP)

Getting the ATO – Sponsor

- What an Authority To Operate (ATO) really means
  - You have the *Authority to Operate*
    - the Federal Government's Software
  - They approve all changes to the system
  - Any major changes need to be approved (More detail later)
- Sponsor or JAB
  - Sponsor is a Federal Agency or the JAB
  - How vested in the process your sponsor is controls some of the speed to ATO
- FedRAMP PMO
  - Not needed if part of the JAB, they will be included
  - If you have an agency sponsor you will have to get PMO approval to get an ATO

Getting the ATO – How Long for an ATO?

- If you have no processes in place it is going to take a while
- If you have certifications like Cisco does, things will go faster
  - SOC, HiTrust, Secure Development Lifecycle, etc.
  - Each of those fills in some detail on the NIST controls
- Corporate Services – The more you have the better it can be
  - Services that help complete more of the NIST controls
    - PSIRT (Product Security Incident Response Team)
    - CISRT (Cisco Incident Security Response Team)
    - InfoSec
    - Crypto Team
    - Absorbed all of them you can for your System Security Plan (SSP)

Getting the ATO – How Hard?

- If your cloud system does not have good processes in place
  - Getting an ATO could be difficult
  - Can take quite a bit of time
  - What will it take to create all the processes?
  - Do all your engineering teams handle security issues the same way?
    - If not, systems will have to change to an approved system, or each system must be documented
      - This can make the overall system very cumbersome to manage if there are multiple processes for just one task

Getting the ATO – Corporate Services

- Supporting systems or processes
  - That are outside the boundary
- Not normally part of the audit
- People have used Corporate Services incorrectly
  - Gets a great deal of scrutiny from Sponsors and Auditors
- Does allow PII outside the boundary
  - Example – we would never build a billing system so the commercial billing system is used
  - Name, number, email, etc. to track system for billing

Getting the ATO – Corporate Services

- Cisco's "Secret Sauce"
- Things that did not need to be created
- Systems were already fully documented
  - Systems processes need to be ported to the SSP
  - Match processes to appropriate NIST controls
- Security teams understood audits and how to respond to auditors
  - PSIRT (Product Security Incident Response Team)
  - CISRT (Cisco Incident Security Response Team)
  - InfoSec
- Absorbed all you can for your System Security Plan (SSP)

Getting the ATO – Corporate Services

- Product Incident Response Team
  - Has all the processes posted externally
    - Vulnerability Policy
    - Vendor Vulnerably Reporting and Discloser Policy
    - Trust and Transparency Center
    - Cisco Security Development Lifecycle (CSDL)
    - Security Advisories
    - Notification Registration
      - RSS Feeds
      - Security Blog
      - My Notifications
      - ETC…
- https://tools.cisco.com/security/center/home.x

Getting the ATO – Corporate Services

- CISRT (Cisco Incident Security Response Team)
  - Monitors all data in and out of the building for Cisco
  - Includes the multi billion-dollar e-commerce site
  - Creates the postmortem of any event
    - Also creates the action items from any event to prevent it from happening again.
- Systems are fully documented
  - Great for passing the audit from the Third-Party Auditor (3PAO)

Getting the ATO – Corporate Services

- InfoSec / CollabSec – Our Group – Collaborations InfoSec
  - Outside of our chain of command
  - Sponsor and agencies believe they are impartial
  - They are the trusted entity for all Continuous Monitoring Meetings (ConMon)
  - They have the final say on ALL security issues in FedRAMP
    - What level they are – High, Moderate or Low
  - They track all the security issues in their system
    - They have their own security Data Center
    - They have all the SLA's for security issues
    - Their system is the Root of all data for the Plan of Action and Milestones (POA&M)

Getting the ATO – Corporate Services

- Cryptography Team
  - Cisco Crypto team manages over 15 million keys a quarter for all of Cisco
  - Have all the policies written down for the SSP
  - Understand how to do audits, FedRAMP is nothing new to the team
  - Manages the Key Management Systems (KMS) in the FedRAMP boundary

We are Lucky

- Cisco's corporate services have been audited many times
- Webex and other groups that use these parts of Cisco do not have to staff or create them from scratch
- This makes getting an ATO for the second ATO group at Cisco easier
  - Webex Meetings had to figure this out all by themselves the first time
- The more of these services you can use, the faster you will get an ATO
- If you do it incorrectly, the 3PAO could call them out as a risk
  - Could slow down the ATO if that happens
  - Be careful, choose wisely

Interconnections

- First rule of FedRAMP (Fight Club) is
  - 2 clouds that talk to each other need to both have ATO's
- They should be on the same FedRAMP level – low to low, moderate to moderate, high to high
- There are cases where there is "Low to High" Connection
  - Our ticketing system is in a FedRAMP high ATO cloud
  - In this case we have more security than required
  - This makes approval very easy
- Not all interconnects are equal
  - Some sponsors do not like the risks from other sponsors

Passing the 3PAO Audit

Third Party Auditor (3PAO)

- The “Big Kahuna” – it is a given you must pass the audit
- They enact the current security concerns for all FedRAMP systems
  - The 3PAO gets direction from the JAB and PMO on what to focus on during an audit
  - That focus pushes a system to meet the audit requirements
  - Does change from year to year
- The 3PAO also has input back to the JAB and PMO
  - What they see that bothers them is communicated to the JAB/PMO
  - They are the eyes and ears of the FedRAMP program

System Security Plan (SSP) is Root

- SSP is the main document that a system is **audited** against
- Has all the answers to the NIST 800-53
- Has the boundary diagrams defining your system – Section 9
  - Section 9 is very important – sponsor understands the system from that section
  - Shows the boundary diagrams – the Boundary is King
    - From the old days – hard and crusty on the outside is the boundary
    - Everything that flows in and out of the boundary needs to be controlled
    - Most controls are in and round the FedRAMP boundary
- Checked into max.gov for all agencies to download

During the Audit

- Treat it like any other audit
  - If you don’t know, say so
  - Phone a friend
  - Be prepared, review your section of the SSP
- Do Not Lie
  - An incorrect answer is better – you can correct the error in the future
- A negative finding in the audit is not the end of the world
  - The finding will stay
  - It can be resolved before the sponsor sees the results

Reacting to The Audit

- The 3PAO will work with you to achieve a “clean audit”
- I have seen this process last up to 6 months after the audit
- Will help the vendor clean up the Security Assessment Report (SAR)
- Staff up for the reply to fix before the SAR is presented to the sponsor

Security Assessment Report (SAR) Readout

- The 3PAO created document to present to the sponsor
- The sponsor will get a readout of the SAR from the 3PAO
- It is a very good idea to invite the FedRAMP Program Management Office (PMO)
  - They will receive a copy of the SAR and SSP
  - You will get all the feedback at once
  - Saves a great deal of time in the long run
- If all goes well, and ATO is granted

FedRAMP Program Management Office (PMO)

- PMO is not the bad guy
- They are your advocate to the JAB to get your ATO
- Involving them early will mean a quicker ATO
  - If you wait until the end, they will not know the history of the ATO
  - They will have to ask questions that have been answered without their knowledge
  - Should be involved with the SAR

Joint Authorization Board – JAB

- The “Big Big Kahuna”
- They give the final stamp of approval
- Once the sponsor and PMO agree, ATO goes to the JAB
- They could have input to any ATO but not something that would be unusual

Keeping your ATO (Care and Feeding The Baby)

Keeping the ATO

- Sponsor
- Continuous Monitoring (ConMon)
- Plan of Action and Monthly Milestones (POA&M)
- Package
- Inventory
- Next Audit Planning

Sponsor

- The single source of truth
- Have a good relationship with them
- They control the product's destiny
- Can accept risks for the product
  - Pre-Audit
  - Significant Changes
- Everything is based on the risk that a product creates for a government agency

ConMon

- Monthly communications meeting with the Sponsor
  - Plan of Action and Monthly Milestones (POA&M)
- Time to talk about security and Risks
  - Everything is based on the Risks of a system
  - New features to be added
  - New deployment models
  - Significant changes
  - Operational Requirements

Plan of Action and Monthly Milestones (POA&M)

- What is presented at the ConMon
- Usually a document that the sponsor defines
- Includes all the data for the sponsor and agencies that can use your system
  - Security Scans
  - Open and closed security issues
  - Changes to the systems
  - Future changes and new parts of the the system that is sponsored

Package

- The most important monthly document about an ATO
- Everyone that has a .mil or .gov email address can download this
- The main form of communication to any potential customer
  - They get your package and you do not have to talk to them
  - They will ask questions usually and that is how you find out they are interested in your product
  - Includes all the data from the POAM
  - Is available on max.gov and allows agencies to download all ATO data

Inventory

- Sponsors and agencies are very interested in the asset inventory
- Changes in inventory without any reason will lead to questions
- This data is in the FedRAMP Package
  - Keeping questions down will assist in sales
- Will make things much easier if the inventory and security scans are EXACTLY the same

Next Audit Planning

- Because things added to the system can create audits
  - Planning starts right after the audit
  - All changes are mapped out in advance
  - Changes in the SSP
  - Changes in the inventory
  - Changes in the POA&M
- Sponsor and customers like to know these things in advance

Running the Business

Keeping the ATO

- Instill discipline
- Cadence
- Annual Audit
- Significant Change
- Speed of new features
- Operational Requirement (OR)
- Vendor Dependency
- Redacted SSP

Instill discipline

- FedRAMP is very regimented
- FedRAMP happens on key milestones
  - Monthly – ConMon, Significant changes, Inventory, Security Scans
  - Yearly – Audit, SAR Review, ATO renewal

Cadence

- Setup that cadence
- When is are the security scans checked in
- When is the ConMon
- Creates problems
  - If the security fixes are focused on the ComMon the sponsor will see late issues
  - The security scans are checked into max.gov 2 weeks before the ConMon
    - The real date for security fixes is the security scan date

Annual Audit

- The sooner you start planning the better
- Some changes are over a year in advance
- Significant changes related to features can require an audit prior to the annual
  - Might only have to audit the change itself
- What happens to the SSP for the next audit
  - How many changes in a 700+ page document
  - 300+ controls
  - Corporate Services need to be reviewed

Significant Change – SC

- What FedRAMP has determined is a major change
- Basically 3 types
  - Document the SC
  - Document and audit the SC
  - Document and audit the entire system for the SC (usually the annual)

Significant Change

- List of SC from the FedRAMP documents

Changes Likely Considered Significant or Major	
Adding/Removing security controls	New cryptographic modules or services or changes to existing modules/services
Changing alternative (or compensating) security control(s)	New data center or moving to new facility
New interconnection or changes to existing	Scanning tool changes
Upgrade of OS	New system monitoring capabilities or replacement of system monitoring capabilities
New Virtual Server(s)	New/upgrade of DBMS (MS SQL, Oracle, etc.)
New Code Release	New authentication mechanisms or changes to existing mechanisms
New boundary protection mechanisms or changes to existing mechanisms; changes to routing rules	Change in cloud service ownership that would result in major changes (e.g. change to contingency planning or incident response processes/capabilities)
Changed or updated backup mechanisms and processes	Movement of information system data to a different system boundary

https://www.fedramp.gov/assets/resources/documents/CSP_Significant_Change_Policies_and_Procedures.docx

Speed of New Features

- What is a new feature and what is an enhancement?
- You can enhance something that is in the boundary
- If something new is added – I could be a SC
  - Can slow down new feature adoption
- Put something in early just to have it audited
  - Allows you to plan around the cadence

Operational Requirement – OR

- Some security issues cannot be fixed
- The system requires something to be configured in a way that is less secure
- FedRAMP views these issues as Operational Requirements
- They allow the system to be run in a state that could be considered less secure
  - Other controls can offset the security issue
- OR's are reviewed every year at the annual
  - If you don't need them anymore, remove them, they can be a pain

Vendor Dependency

- Many we wait for a security fix from a vendor
- When this happens you can be late on your security SLA's
- If this happens you can do a "Vendor Dependency"
- This allows you to track that security issue outside of being late
- The Sponsor and the PMO can help push the vendor to fix issues that are late

Redacted SSP

- Companies, such as contractors, vendors, etc.
  - They do not have access to max.gov
  - Will not get a copy of the full SSP
  - They will get a redacted version of the SSP
- They will require an SSP that is redacted without some key information
  - Ports, protocols, special sauce that makes that product unique
  - This can be a great deal of work – there may be more demand for a product from commercial customers supporting the government then from the government

Conclusions

Conclusion

- Get a sponsor – this will speed things along
- The SSP is root
  - What customers will see about your system
- Corporate Services will allow you to increase speed of the ATO
  - Make sure they are well defined
- Hire the expertise if you do not have it
  - FedRAMP is a learning cliff
  - Easy to get confused and spend time recovering

Conclusion

- Getting an ATO can be a challenge, or very hard
- 18 months is possible
  - Well documented system
  - Good security practices
  - Have defined corporate controls
  - Executive management support
  - A good sponsor
- Missing any of the thing listed above, add additional time

Conclusion

- https://fedramp.gov
- https://www.fedramp.gov/documents/
- https://www.fedramp.gov/assets/resources/documents/CSP_A_FedRAMP_Authorization_Boundary_Guidance.pdf
  - Best 3 page doc every created about FedRAMP
- https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf
  - Good playbook

Thank you

Possibilities

#CiscoLive