
Leveraging FedRAMP® as a Transformative Tool

From Checkbox to Culture

Presentation for the OpenSSL Conference, Prague 2025
Bernie Leung, Bron Torres, Sapna Paul



Agenda

1. FedRAMP Fundamentals
2. Why FedRAMP Matters
3. Encryption
4. Vulnerability Management
5. Continuous Monitoring / Improvement
6. Implementation
7. Challenges/Solutions



Transformation

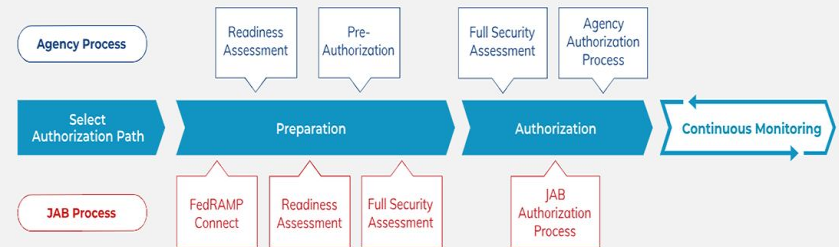


FedRAMP

- Purpose & scope
 - . Government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services
- . Impact levels (Low/Mod/High)
Based on FIPS 199 Categorization of the CUI processed. *CUI- Controlled Unclassified Information.
- . 3rd Party Assessor 3PAO as independent auditor

FedRAMP Authorization Process

There are two ways to authorize a Cloud Service Offering (CSO) through FedRAMP, through an individual agency or the Joint Authorization Board (JAB).



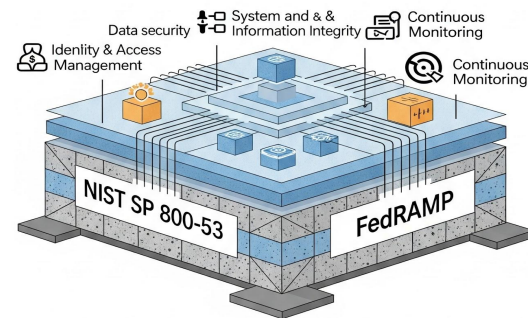
Note: Readiness Assessment is required for the JAB Process and is optional but highly recommended for the Agency Process.

Why FedRAMP Matters

A common Security Baseline based on SP800-53 that

Both agencies and service providers understand.

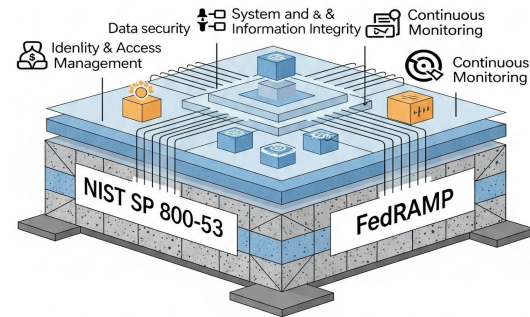
Business Benefits	Security Benefits
- Faster adoption - Cost savings - Market access	- Risk reduction - Compliance credibility - Trust building



Role of the 3PAO

**An Independent Certified 3rd Party Auditing
Organization that Brings Conformity to Security
Baseline.**

3PAO -
*independent
auditor*



A horizontal line with a teal-to-orange gradient, located above the 'Project objective' text.

Project objective

Getting Started to FedRAMP Authorization

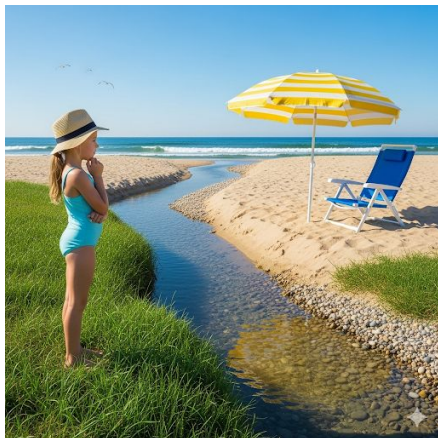
FedRAMP

Key Security Indicators

FedRAMP 20X Key Security Indicators	Summary of Controls
Cloud Native Architecture	- ** Boundary Protection and Manage Access Control Points - ** Internal System Connections - ** Immutable Infrastructure
Service Configuration and Encryption	- ** Harden configurations, encrypt traffic and data at rest. - ** Centralized config management, - ** Cryptographic integrity. - ** Automated key management, patching strategy.
Identity and Access Management	- ** Protect user data, - ** Control access, and apply zero trust principles.
Monitoring and Logging	- ** Continuous Monitoring (SIEM) - ** Vulnerability Scanning and Patching (within H30, M90, L180 days) - ** Maintain System Inventory
Change Management	- ** Log and monitor changes - ** Automated testing before deployment. - ** Documented procedures and risk evaluation.
3rd Party Risk Management	- ** Identify 3rd Party Resources, Monitor Supply Chain Risks
Cybersecurity Education	- ** Awareness training on Insider Threats, Social Engineering

FedRAMP Readiness Assessment

Step 1 – Gap Analysis



Top Challenges	Findings
1. Encryption	- ** All traffic within and crossing <i>Authorization Boundary</i> must be encrypted with FIPS 140-2/3 (validated algorithm).
2. Vulnerability Scanning and Remediation	- ** All systems within Authorization Boundary must be scanned. - ** Vulnerabilities must be remediated (High 30days, Medium 90days, Low180days) - ** <i>Including leveraged vendor services.</i>

*

FedRAMP authorization boundary includes all services used to process government Controlled Unclassified Information



Encryption - Cornerstone of FedRAMP

***Not Unique to
FedRAMP***

Crosswalk for commonly used Standards

Control Area	NIST SP 800-53	ISO 27002	SOC 2 (Common Criteria)
Encryption at Rest	SC-28, SC-13	A.8.2.3	CC6.1, CC6.2
Encryption in Transit	SC-8, SC-13, SC-12 (key management)	A.13.1.1, A.13.1.2, A.13.1.3	CC6.1, CC6.2

Encryption - Cornerstone of FedRAMP

FedRAMP additional Guidance to SP800-53

SC-8 Transmission Confidentiality and Integrity (L)(M)(H)

Protect the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

SC-8 Additional FedRAMP Requirements and Guidance:

Guidance: For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8 (1), physical means as specified in SC-8 (5), or in combination.

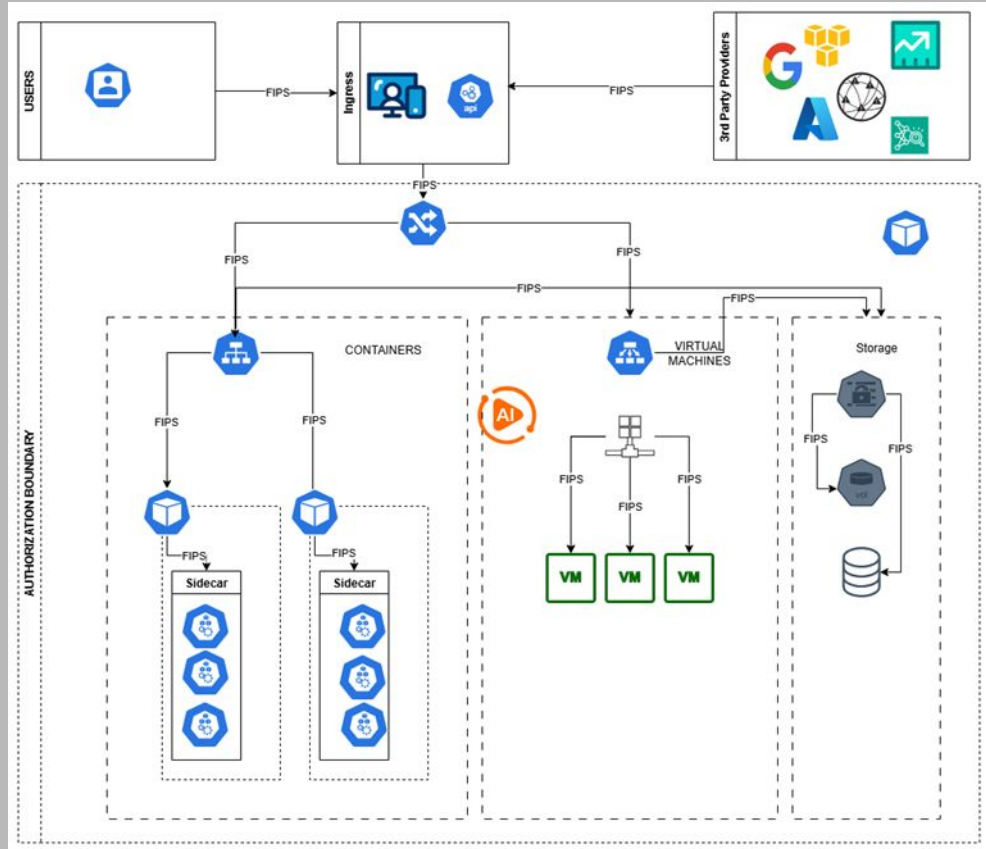
Data In Transit Encrypted includes:

- Crossing the system boundary
- Between compute instances - including containers
- From a compute instance to storage
- Replication between availability zones
- Transmission of backups to storage
- From a load balancer to a compute instance
- Flows from management tools required for their work
 - e.g. log collection, scanning, etc.

Encryption

Data in Transit

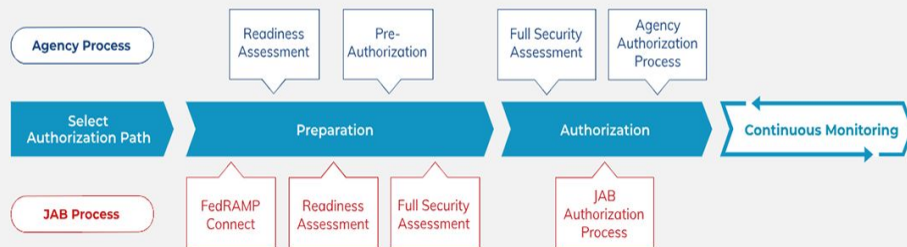
- within Authorization Boundary and
- crossing Authorization Boundary



Continuos Monitoring Good Hygiene

FedRAMP Authorization Process

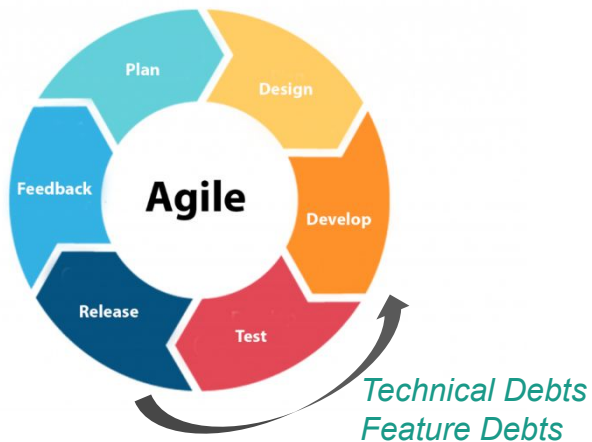
There are two ways to authorize a Cloud Service Offering (CSO) through FedRAMP, through an individual agency or the Joint Authorization Board (JAB).



Note: Readiness Assessment is required for the JAB Process and is optional but highly recommended for the Agency Process.

Agile SDLC

Dev Sec Ops → Agile System Development and Delivery



INTENTION:

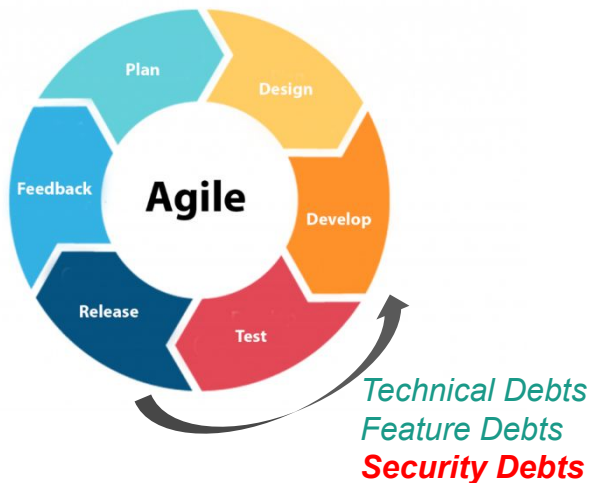
- *Facilitate a Faster Time to Market*
- *Accept Deficiencies as Technical Debts*
- *Remove Technical Debts as Time Permits.*

The PROCESS:

- *Allocate Time for Removing Technical Debts.*

Agile SDLC

DevOps → Agile System Development, Delivery and Security



INTENTION:

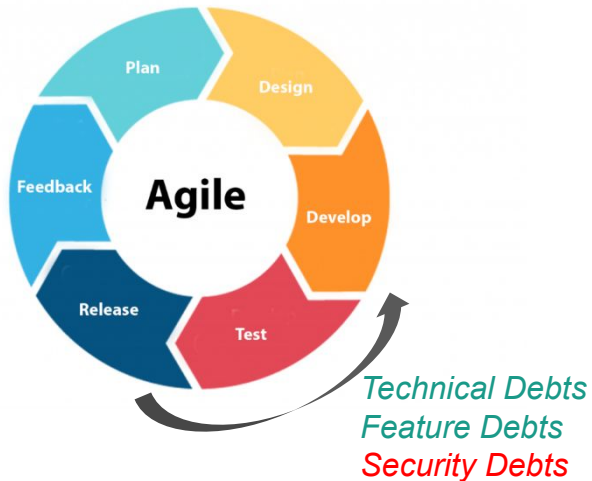
- *Shift Left on Security*
- *Only Allow Low and Medium Security Debts*

The PROCESS:

- *Block Software with High Severity from Deployment*
- *Remediate Medium Severity within SLA.*

Agile SDLC

DevOps → Agile System Development, Delivery and Security



INTENTION:

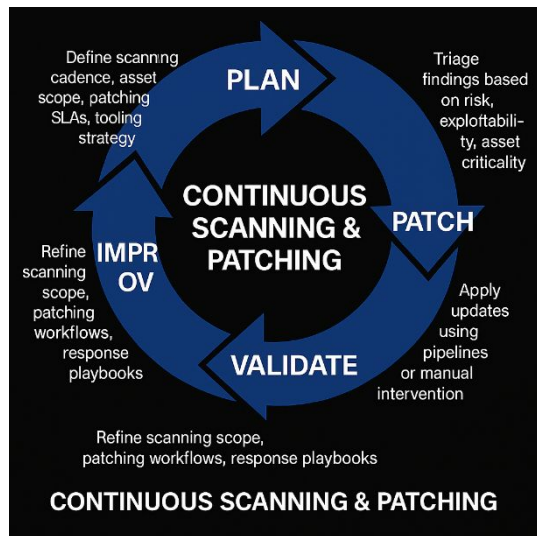
- *Shift Left on Security*
- *Only Allow Low and Medium Security Debts*

The PROCESS:

- *Block Software with High Severity from Deployment*
- *Remediate Medium Severity within SLA.*

Continuous Monitoring - The Long Tail

PLAN → SCAN → PRIORITIZE → PATCH → VALIDATE → IMPROVE → back to PLAN



INTENTION:

To facilitate a disciplined and structured approach to tracking risk-mitigation activities.

The PROCESS:

Plan of Action & Milestone (monthly report, soon moving to continuous API access)

Maintain Continuous Health in Production

A horizontal line with a teal-to-orange gradient, located above the text.

Project objective

Implementation Strategy

Target audience

“If encryption is everyone’s job,
it’s no one’s responsibility.”

– The Mirror



1. The Question

“Who Owns Encryption?”



1. The Real Question

~~“Who Owns Encryption?”~~

It's: *“How do we ensure encryption becomes enforceable, explainable, and consistent—without slowing teams down?”*

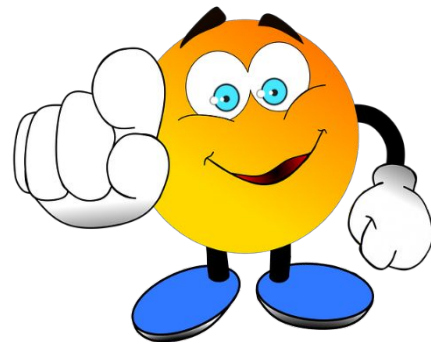
FedRAMP teaches us this: Trust is not a feature. It's a repeatable system.



The Myths That Derail Encryption Programs

- “It’s already handled by AWS KMS / Azure Key Vault / GCP CMEK.”
- “DevSecOps owns it.”
- “It’s on the backlog.”
- “We have secrets in GitHub Actions, we’re good.”

Truth: Encryption tooling $\neq$ encryption governance



Tools Exist. What's Missing Is the “Why”

- Why do we encrypt this data?
- Why these keys?
- Why now and not at runtime?



: Trust is not a feature. It's a repeatable system.

FedRAMP as a Forcing Function

FedRAMP isn't just about encryption compliance—it forces cross-functional alignment:

Principle	Encryption Example
Least Privilege	Envelope encryption with scoped access
Auditability	CMKs with logging in CloudTrail, Sentinel, etc
Consistency	Terraform modules / OPA / policy-as-code



A horizontal line with a teal-to-orange gradient, located above the text.

Project objective

The Real World Problem

The Real-World Problem:

Heterogeneous Dev Patterns

- Acquired teams with no vault strategy
- Legacy apps with no envelope encryption
- Cloud-native microservices vs .NET monoliths
- Data scientists spinning up rogue buckets



The Real-World Problem

You can't govern what you can't standardize and,

You can't standardize what you don't understand.

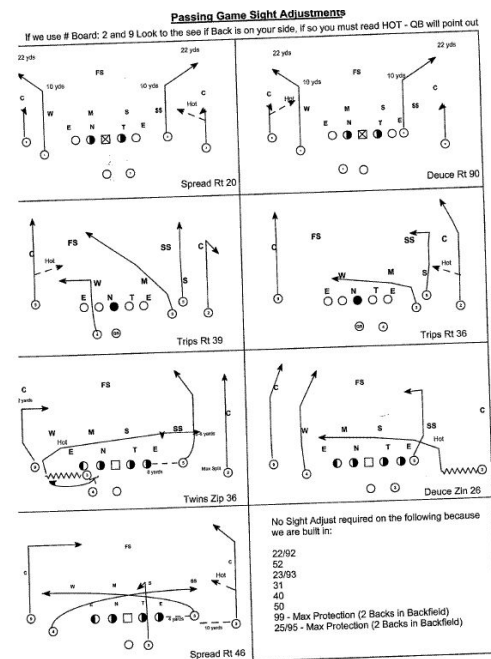
- Acquired teams with no vault strategy
- Legacy apps with no envelope encryption
- Cloud-native microservices vs .NET monoliths
- Data scientists spinning up rogue buckets



The Playbook:

Anchor to FedRAMP, Scale via Automation

- 1. Define intent: What counts as sensitive? What are our trust zones?**
- 2. Codify controls: Use IaC, templates, policy-as-code (e.g., Sentinel, OPA, Rego)**
- 3. Enforce in pipelines: GitHub Actions, Azure DevOps, Terraform Cloud, Backstage**
- 4. Monitor + prove: Audit logs, CI/CD evidence, dashboards for execs**



Your Encryption Program Isn't a Tech Problem, It's a Narrative Problem

"If you can't explain why encryption matters to a CFO, it won't matter how good your KMS strategy is."

Help people understand:

- *Why this matters*
- *Why it's hard*
- *Why now*



In Closing

Encryption at Scale Is Not About Keys—It's About Culture

- *Anchor to FedRAMP to drive alignment*
- *Codify trust into your pipelines*
- *Scale across non-standard clouds and codebases*
- *Make the invisible visible*

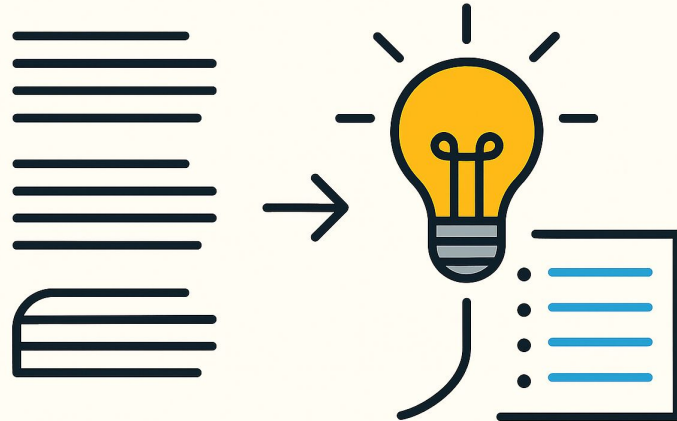
Make it easier to understand



How Can This Community Help?

Make SSL/TLS

Make it easier to understand



Thank you.

Q&A

