Hacks & Hops – October 2025

FedRAMP as an OnRAMP

Elisabeth Knottingham

Information Security Manager – Public Sector

Executive Director @ JPMorgan Chase

Disclaimer

All opinions, attitudes, understandings and information distillations expressed by Elisabeth during this session are hers alone and do not represent the opinions, attitudes, and understandings of her employer, JPMorgan Chase.

FedRAMP, NIST, and Learning to Love the Controls

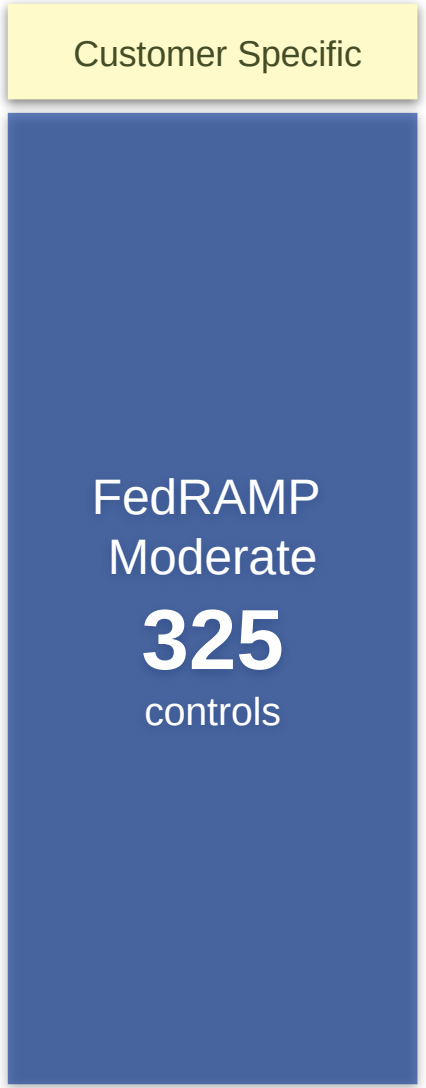
FedRAMP: What is it?

Overview

Standardized security assessment and authorization for cloud products and services used to ensure that federal data is consistently protected at a high level

- Run by the FedRAMP Program Management Office (PMO) operated by the General Services Administration (GSA)
- Requires adhering to 325 NIST 800-53 controls, 14 applicable laws and regulations, and 19 standards and guidance documents
- Requires ongoing monthly and annual reassessments
- 3 levels: Low, Moderate, & High. Moderate is most common.

Successful audit completion allows a company to offer services on the FedRAMP Marketplace



NIST: What is it?

National Institute of Standards and Technology

NIST SP 800-53: *Security and Privacy Controls for Information Systems and Organizations*

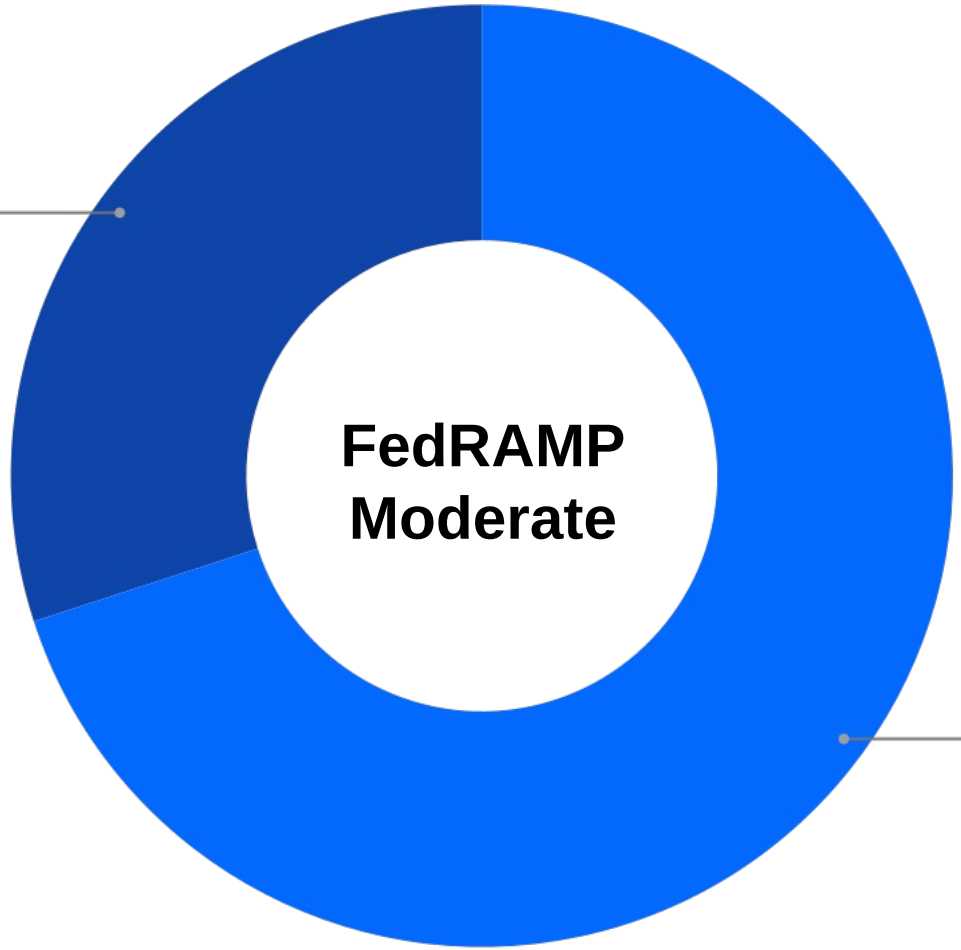
- The “Mother Control Set” for FedRAMP and DoD IL & CMMC audits
- The audit standard library for all federal spaces
- Used to prove compliance with the NIST 800 frameworks
- Operational motion of the NIST Cybersecurity Framework

NIST 800-53 is the library of controls for an environment that must protect high value data and is organized into low, moderate, and high overlays based on the value of the data being protected.

A good overview of the NIST 800-53 controls, with the control overlays, is available at CSF Tools

ISO, SOC2, PCI, and NIST

Help the org understand they need more than ISO, SOC, and PCI to see the whole picture



ISO, SOC2 and PCI controls only cover ~30% of the total NIST cybersecurity risk framework.

What is important in FedRAMP?

What regulators want is the same thing that helps any security team

Who has access to data?

Human – how do we know who they really are?
Digital – how are connections authorized?
Levels of Access – privileged vs non-privileged

What assets have which data?

Assigned tasks & expected data types
Age of asset & current vuln status
Location (geofencing)

Where is data flowing?

External & internal inputs and outputs
Hard coded connections are properly mapped and monitored
Ephemeral connections only with proper security and authentication

How are you managing general security?

Vulnerability status & meeting SLAs
Intrusion protection & detection
Secrets are well managed

Artifacts of Discovery

What you'll need to show what you are protecting and how that's going

Network Boundary Diagram

- Outside vendors & external service providers
- Customer input and outflow connections
- Corporate services

Data Flows Diagrams

- Hosting Location
- Repository Types

Access Control Lists

- Privileged and non-privileged access
- Access control by region / duty / asset type

Third Parties – Thinking Beyond the Cloud

Where regulators are always looking the hardest

You always inherit the compliance posture of your third party tools

Make sure these integrations don’t negatively impact your system

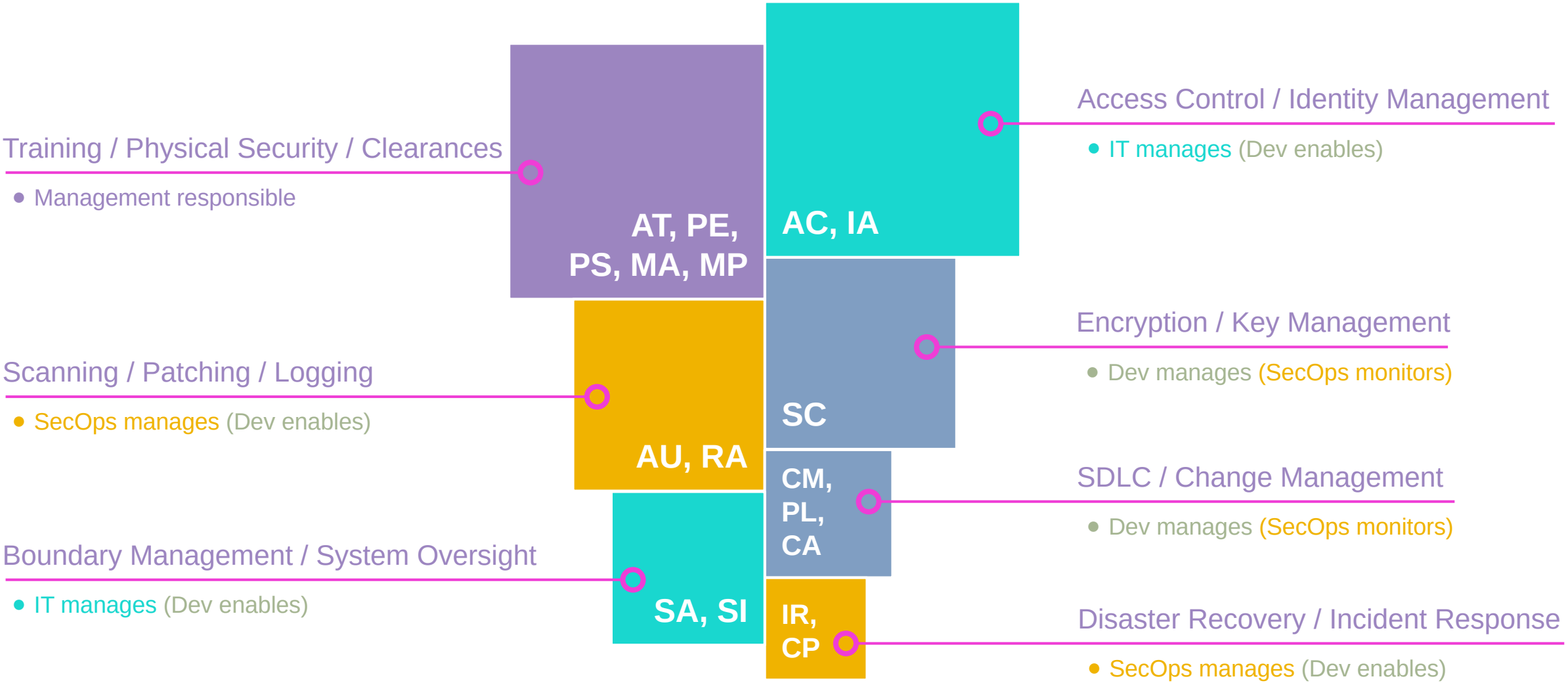
Dashboards, Org Priorities, and Getting to the Cash

FedRAMP Control Families

Acronym	Name	Important Topics
AC	ACCESS CONTROL	System Access
AT	AWARENESS AND TRAINING	Training
AU	AUDIT AND ACCOUNTABILITY	Logging
CA	ASSESSMENT, AUTHORIZATION, AND MONITORING	Audit & Oversight
CM	CONFIGURATION MANAGEMENT	SDLC
CP	CONTINGENCY PLANNING	Backup & Recovery
IA	IDENTIFICATION AND AUTHENTICATION	Validating Users
IR	INCIDENT RESPONSE	Incident Handling
MA	MAINTENANCE	Upgrades & updates
MP	MEDIA PROTECTION	Disposal of Material
PE	PHYSICAL AND ENVIRONMENTAL PROTECTION	Physical Security
PL	PLANNING	Security Planning
PM	PROGRAM MANAGEMENT	Budget
PS	PERSONNEL SECURITY	Human Security
PI	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	Privacy & PII
RA	RISK ASSESSMENT	Vulnerability management
SA	SYSTEM AND SERVICES ACQUISITION	Third Party Risk
SC	SYSTEM AND COMMUNICATIONS PROTECTION	System Protection
SI	SYSTEM AND INFORMATION INTEGRITY	Data Integrity
SR	SUPPLY CHAIN RISK MANAGEMENT	Supplier Risk

Which controls matter to whom?

Controls by Topic and Control Family with team responsibilities



Example Control Evaluation (Moderate)

Acronym	Name	Grade	Effort to Grade A
AC -01	Policy and Procedures	B -	$
AC -02	Account Management	C -	$$$
AC -03	Access Enforcement	A	
AC -04	Information Flow Enforcement	B+	$$$
AC -05	Separation of Duties	F	$
AC -06	Least Privilege	D	$$
AC -07	Unsuccessful Logon Attempts	A	
AC -08	System Use Notification	N/A	
AC -11	Device Lock	A	
AC -12	Session Termination	B	$
AC -14	Permitted Actions Without Authentication	C -	$$$
AC -17	Remote Access Controls	B+	$
AC -18	Wireless Access	A	
AC -19	Access Control for Corp Mobile Devices	N/A	
AC -20	Use of External Systems	F	$$$
AC -21	Information Sharing	B-	$
AC -22	Publicly Accessible Content	A	
Score	**Overall Score for Access Control Family**	**B- (81%)**	**$$**

Example: Control Families by Org Priorities

ACCESS CONTROL

AWARENESS AND TRAINING

AUDIT AND ACCOUNTABILITY

ASSESSMENT, AUTHORIZATION, AND MONITORING

CONFIGURATION MANAGEMENT

CONTINGENCY PLANNING

IDENTIFICATION AND AUTHENTICATION

INCIDENT RESPONSE

MAINTENANCE

MEDIA PROTECTION

PHYSICAL AND ENVIRONMENTAL PROTECTION

PLANNING

PROGRAM MANAGEMENT

PERSONNEL SECURITY

PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

RISK ASSESSMENT

SYSTEM AND SERVICES ACQUISITION

SYSTEM AND COMMUNICATIONS PROTECTION

SYSTEM AND INFORMATION INTEGRITY

SUPPLY CHAIN RISK MANAGEMENT

Example: Control Families Effort by Quarter

Q1	Q2	Q3	Q4
ACCESS CONTROL			
			AWARENESS AND TRAINING
AUDIT AND ACCOUNTABILITY			
		ASSESSMENT, AUTHORIZATION, AND MONITORING	
		CONFIGURATION MANAGEMENT	
	CONTINGENCY PLANNING		
IDENTIFICATION AND AUTHENTICATION			
INCIDENT RESPONSE			
	MAINTENANCE		
			MEDIA PROTECTION
		PHYSICAL AND ENVIRONMENTAL PROTECTION	
	PLANNING		
			PROGRAM MANAGEMENT
	PERSONNEL SECURITY		
PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY			
		RISK ASSESSMENT	
	SYSTEM AND SERVICES ACQUISITION		
SYSTEM AND COMMUNICATIONS PROTECTION			
SYSTEM AND INFORMATION INTEGRITY			
	SUPPLY CHAIN RISK MANAGEMENT		

Example: Dashboard by Control Family

Start	Status	Blockers		Add'nl Cost
Q1	🔴	Staffing	ACCESS CONTROL	$$
Q1	🟢		AUDIT AND ACCOUNTABILITY	
Q1	🔴	Staffing	IDENTIFICATION AND AUTHENTICATION	$$
Q1	🟡	Conflicting Priority	INCIDENT RESPONSE	$
Q1	🟢		PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	
Q1	🟡	Underestimated	SYSTEM AND COMMUNICATIONS PROTECTION	$$
Q1	🔴	Tool Budget	SYSTEM AND INFORMATION INTEGRITY	$$$
Q2	🟢		CONTINGENCY PLANNING	
Q2	🟢		MAINTENANCE	
Q2	🟡	Staffing	PLANNING	$
Q2	🟢		PERSONNEL SECURITY	
Q2	🟡	Staffing	SYSTEM AND SERVICES ACQUISITION	$$$
Q2	○		SUPPLY CHAIN RISK MANAGEMENT	
Q3	○		ASSESSMENT, AUTHORIZATION, AND MONITORING	
Q3	○		CONFIGURATION MANAGEMENT	
Q3	○		PHYSICAL AND ENVIRONMENTAL PROTECTION	
Q3	○		RISK ASSESSMENT	
Q4	○		AWARENESS AND TRAINING	
Q4	○		MEDIA PROTECTION	
Q4	○		PROGRAM MANAGEMENT	

We are here now

Ontime/budget 🟢 At Risk 🟡 Failing 🔴 Just started ○ Not started ⚫

So you wanna go FedRAMP?

Who's Who

Cloud Service Provider (CSP): any company providing digital services to the US, state, local, or regional governmental body

FedRAMP PMO: the federal arbitrators of what is included in FedRAMP

General Services Administration (GSA): agency that owns the FedRAMP PMO

Agency: the US Federal Agency that pairs with an outside CSP to achieve FedRAMP

GOVRAMP: the non-profit member funded PMO for state, local, and regional authorization

Last Thoughts and Helpful Links

Never Waste a Good Emergency

- Always have a plan for the stuff you were denied $$ for
- Keep the plans hot and ready for when the news catches up

Protect Yourself – Do the Paperwork!

FedRAMP isn't required….. But it sure is nice to have

Currently, the best NIST 800-53 controls listing is at CSF Tools (watch the overlays!)

Official NIST 800-53 Rev. 5 and NIST CSF 2.0 websites

FedRAMP official website, and it's very useful to follow their blog as well

Acronyms

AG: Attorney General

AO: Authorizing Official

AO/ATO: Authority To Operate

CAP: Cloud Access Point

ConMon: Continuous Monitoring

CSM: Cloud Security Model

CSO: Cloud Service Offering

CSP: Cloud Service Provider

CUI: Controlled Unclassified Information

DFARS: Defense Federal Acquisition Regulation Supplement

DISA: Defense Information Systems Agency

DOD: Department of Defense

FCI: Federal Contract Information

FedRAMP: Federal Risk and Authorization Management Program

FISMA: Federal Information Security Modernization Act

FIPS: Federal Information Processing Standards

GSA: General Services Administration

IL: Impact Level (IL-2, IL-4, etc.)

ISO: International Organization for Standardization

JAB: Joint Authorization Board

NARA: National Archives and Records Administration

NIST: National Institute of Standards and Technology

OMB: Office of Management and Budget

OSCAL: Open Security Controls Assessment Language

PATO: Provisional Authority to Operate

PCI: Payment Card Industry

PMO: Program Management Office

POA&M: Plan of Action and Milestone

RAR: Readiness Assessment Report

SAP: Security Assessment Plan

SAR: Security Assessment Report

SCR: Significant Change Request

SNAP: System/Network Approval Process

SOC: System and Organization Control

SSP: System Security Plan

TIC: Trusted Internet Connection

3PAO: Third Party Assessment Organization

Thank you FRSecure!

Elisabeth Knottingham

elisabethknottingham.com