BSides Seattle – May 2023:

FedRAMP as an OnRAMP

Elisabeth Knottingham

Information Security Manager – Public Sector

Executive Director @ JPMorgan Chase

Agenda

- Introduction
- FedRAMP, NIST, and Learning to Love the Controls
- What is an Authorization Boundary Anyway?
- Dashboards, Org Priorities, and Getting to the Cash
- Gatekeepers, Roadmaps, and the FedRAMP Acronym Jungle
- What’s Coming Next and Places to Look for Help

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 History

It’s been a busy decade

- 2011- Building on FISMA, Congress creates FedRAMP to give uniform security reviews across all agencies
- 2021 – TxRAMP, StateRAMP, and Local cybersecurity regulations add requirememtns and increase the reach of FedRAMP throughout the US
  - FedRAMP Moderate = TxRAMP = StateRAMP
- 2022 – FedRAMP Authorization Act as part of the NDAA spending bill makes FedRAMP US Gov wide (previously just GSA mandated)
- 2021 – 2022 White House Cybersecurity Directives
- Executive Order 14028, M-22-09 (ZTA), and M M22-18 (SBOM) give clear guidance and oversight in this area to CISA and hold agencies accountable for security as systems migrate to the cloud

FedRAMP, NIST, and Learning to Love the Controls

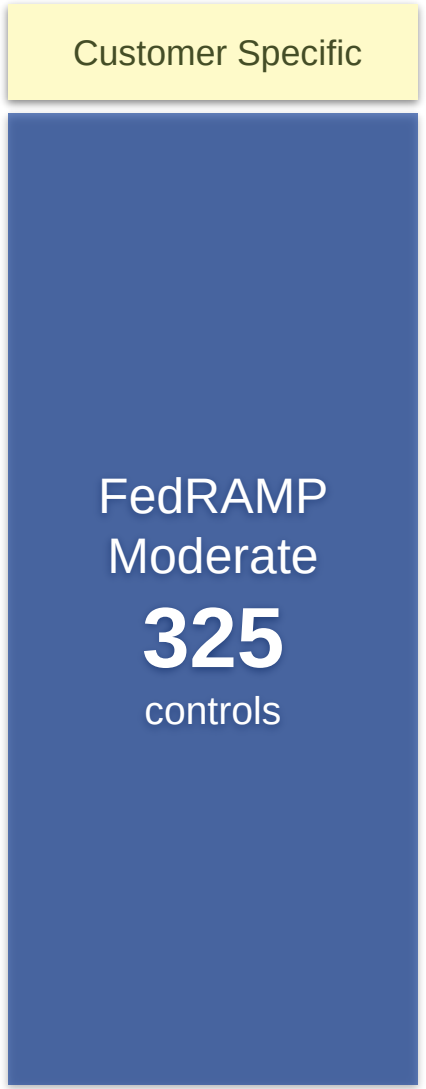
FedRAMP: What is it?

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



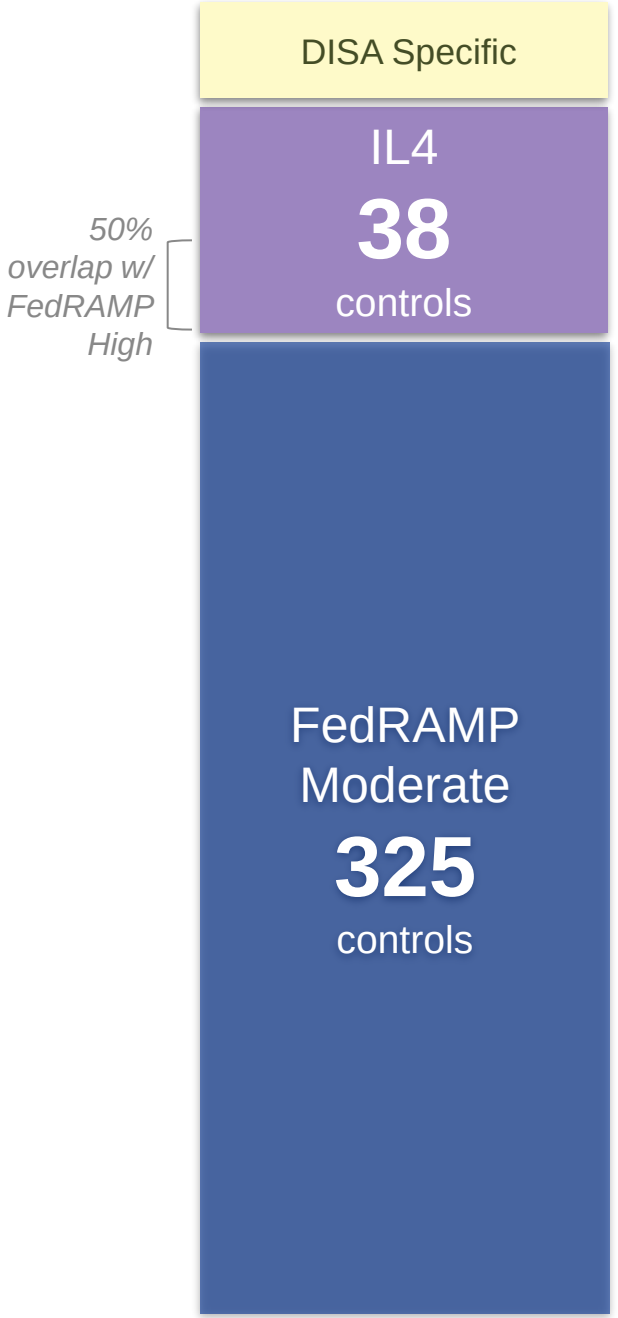
IL4: What is it?

Overview

Impact Level 4 (IL4) is a standardized security model for cloud products and services used by *U.S. DoD mission owners*

- FedRAMP Moderate + 38 additional controls + DFARS
- System must be independent (“air gapped”)
- Must contain only DoD users
- Requires US Citizen on US Soil for operation

Impact levels are audited under, and controlled by, the Department of Defense Cloud Computing Security Requirements Guide (SRG)



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 IL4
- Sets the audit standard for all federal spaces
- Used to prove we meet the other NIST frameworks
- Operational motion of the NIST Cybersecurity Framework

NIST 800-53 is there to set the Authorization Boundary so that the environment can protect and defend high value data

Any type of public sector or other US domestic customers generally can be inside an authorized FedRAMP environment.

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

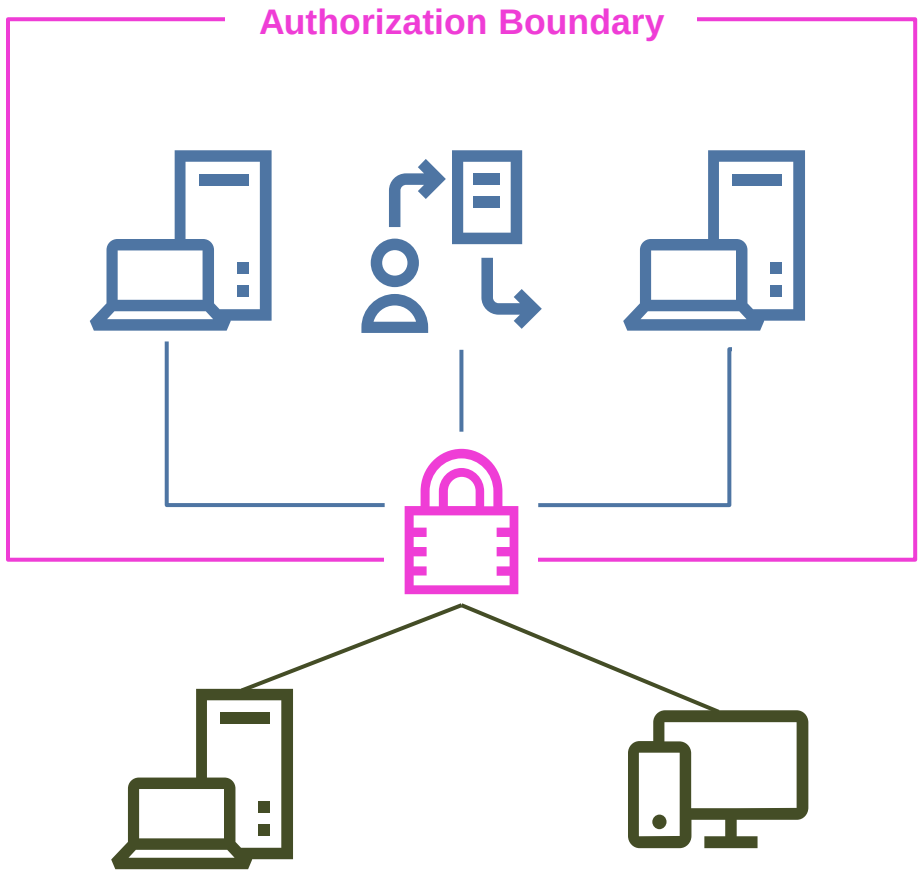
Intrusion protection & detection

Secrets are well managed

What is an Authorization Boundary Anyway?

What is the Authorization Boundary?

The perimeter within which the government authorizes a CSP to process protected federal data



This is the **environment**

Environments are authorized, ***not*** products

Products are authorized functions operating with security controls within an authorization boundary

Functions can be added to an already authorized boundary via the significant change process

Any actions that cross the boundary must be carefully reviewed to meet data and metadata requirements

Protected federal data includes metadata

How to get started defining the boundary

Guidance directly from FedRAMP

Goal: Define and describe all system data flows and interconnections

Consider diagramming the following:

- Customer/User Authentication Logical Data Flow
- Administrative/Privileged User Authentication Logical Data Flow
- System Application Data Flow within the Proposed Cloud Boundary
- System Application Data Flow to All Interconnected Systems

FedRAMP and the Commercial Cloud

AWS, Azure, and GCloud

FedRAMP was developed to make the risks inherent in the public cloud visible, trackable, and fixable

Shared Responsibility with the cloud provider gives effective risk management, but also leveraging them correctly helps because:

- They've worked for decades to build infrastructure adhering to FedRAMP
- Effective control monitoring means less work for InfoSec Teams
- Thousands of successful audits attest to their methods
- Robust body of public knowledge

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 integrations don’t negatively impact your boundary

Artifacts of Discovery

When you've defined the boundary, you'll know what you are protecting

Network Boundary Diagram

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

Data Flows Diagrams

- Hosting Location
- Repository Types

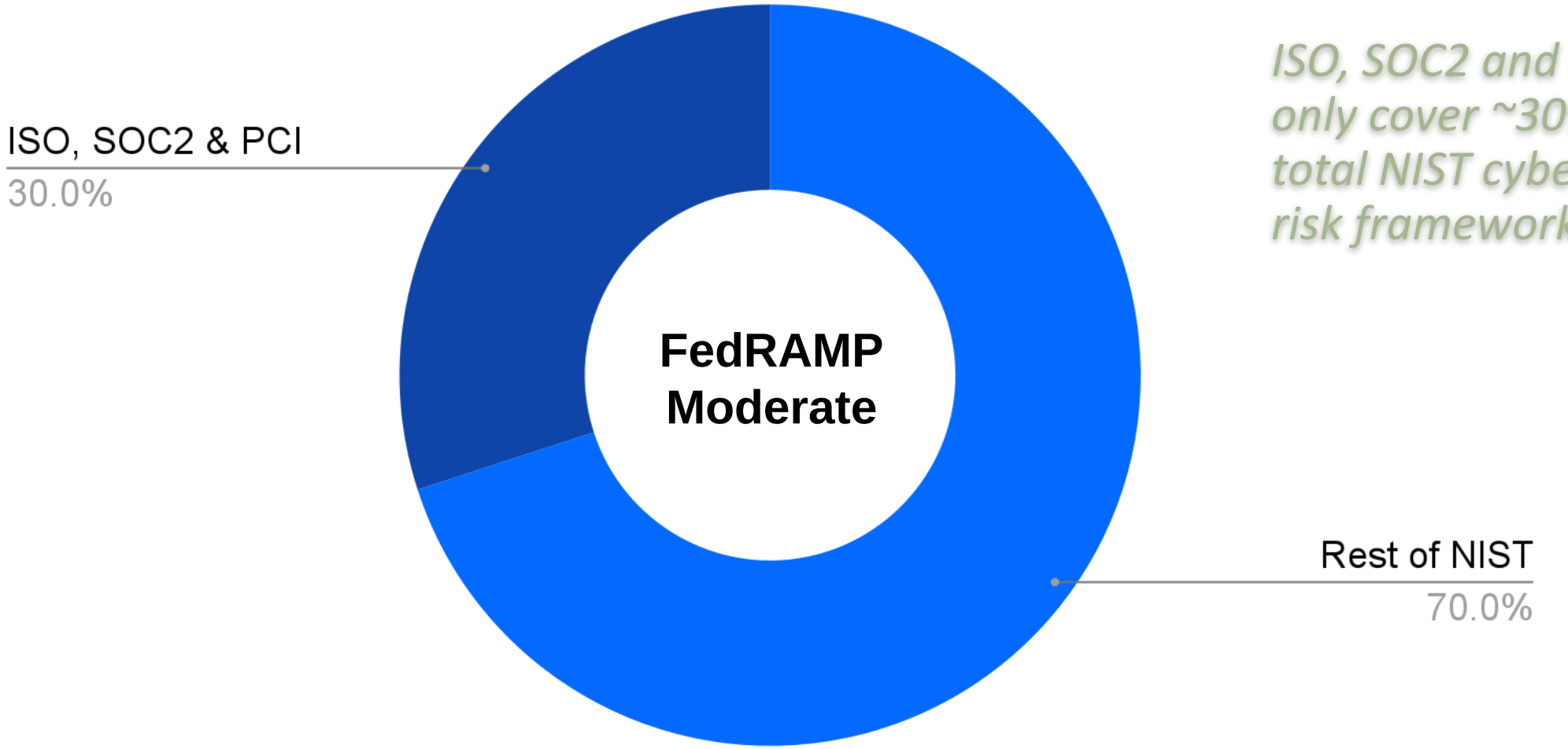
Access Control Lists

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

Dashboards, Org Priorities, and Getting to the Cash

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.

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

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

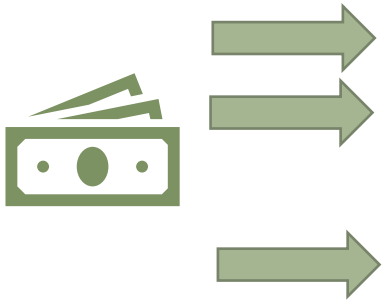
SYSTEM AND INFORMATION INTEGRITY

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



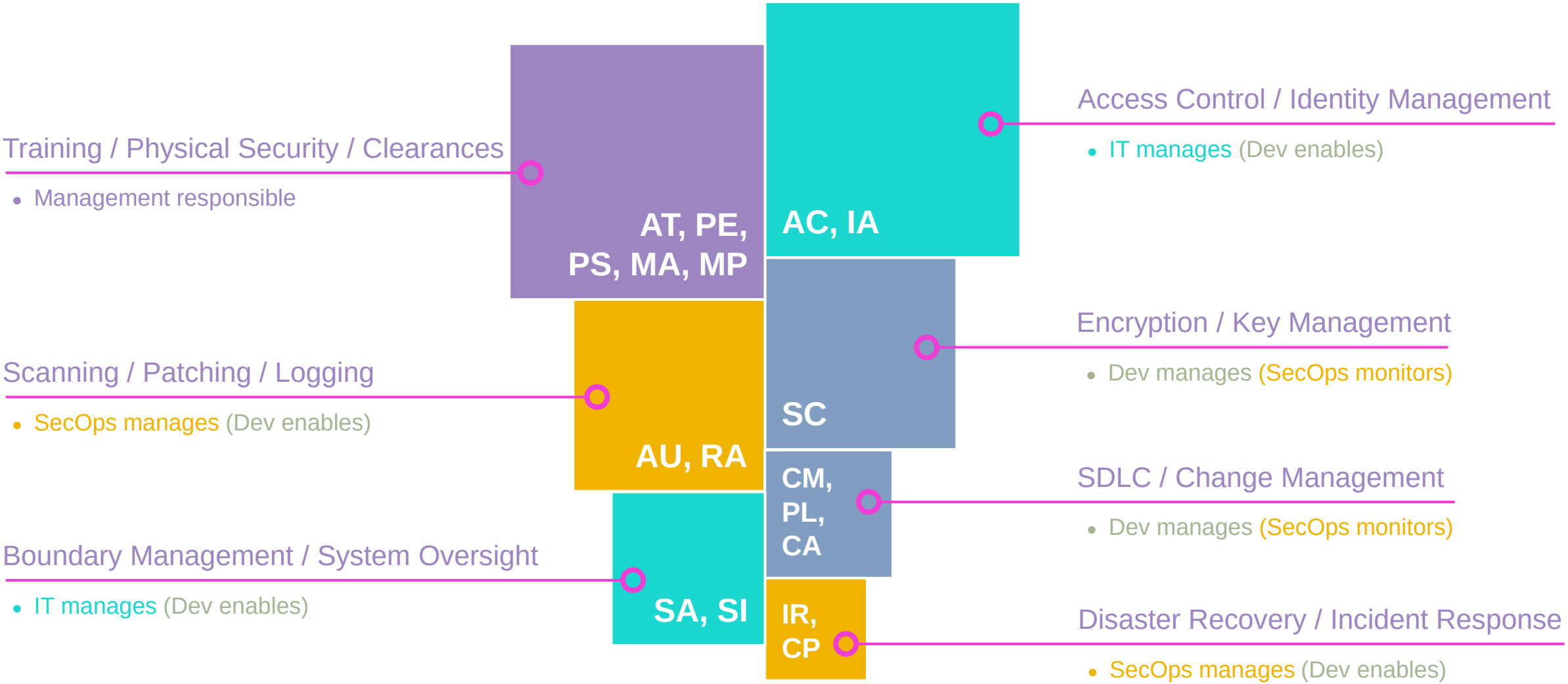
Start	Status	Blockers	
Q1	🔴	Staffing	ACCESS CONTROL
Q1	🟢		AUDIT AND ACCOUNTABILITY
Q1	🔴	Staffing	IDENTIFICATION AND AUTHENTICATION
Q1	🟡	Conflicting Priority	INCIDENT RESPONSE
Q1	🟢		PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY
Q1	🟡	Underestimated	SYSTEM AND COMMUNICATIONS PROTECTION
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

Here now

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

Which controls matter to whom?

Controls by Topic and Control Family with team responsibilities



Gatekeepers, Roadmaps, and the FedRAMP Acronym Jungle

So you wanna go FedRAMP?

Who's Who

Cloud Service Provider (CSP): The company that wishes to offer cloud-based services on the FedRAMP Marketplace

FedRAMP PMO: the arbitrators of what is included in FedRAMP including control overlays and systems of authorization

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

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

JAB: Joint Authorization Board, aka DISA, DHS, and the FedRAMP PMO

Two Paths to FedRAMP

Path 1: Agency Sponsored

1. Pair with a US Federal Agency
2. Undergo a 3rd Party Assessment with an authorized 3PAO
3. Complete the Security Assessment Report
4. Submit to the FedRAMP PMO

Path 2: Joint Authorization Board

1. Complete a FedRAMP Ready Assessment (RaR) with 3PAO
2. Address RaR findings with the FedRAMP PMO
3. Petition for JAB Review after full Security Assessment Report
4. Successfully complete JAB Review

More details on the FedRAMP Website

Collateral Needed to Start Assessment

FedRAMP's Official List

- System Security Plan (SSP) and attachments
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POA&M)
- Signed agency Authorization to Operate (ATO) - For Agency Authorizations
- Signed JAB Provisional-ATO (P-ATO) - For JAB Authorizations

Details needed to complete the assessment, including the recommended team to build, timelines, and many other topics are covered in FedRAMP's CSP Authorization Playbook

Also very helpful, the full set of controls for each assessment type in the FedRAMP Security Controls Baseline

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

What’s Coming Next and Places to Look for Help

What's Next?

NIST 800-53 Rev 5

- FedRAMP still waiting to adopt
- Includes 2 New control families (SR & PI)

ZTA – Zero Trust Architecture

- CISA's ZTA Maturity Model Version 2.0 – Stage 1 MFA
  Still awaiting timelines for the next stage
- Updates expected to NIST SP 800-63 that will change authentication requirements

SBOM – Software Bill of Materials

- National Telecommunications and Information Administration's Early Adoption Process
  With great details, documents, and action plans for SBOM implementation

Great Sources of Help

Best place to stay up to date? The FedRAMP Blog!

It has links to guidance on:

- Boundary creation
- Securing Subnets
- OsCal
- Updates to FedRAMP processes
- NDAA required committees and changes
- CISA required changes

AWS and Azure have great pages for FedRAMP & shared controls

- AWS Compliance pages
- Azure Compliance pages

FedRAMP assistance for hire available from most authorized 3PAOs

Thank you BSides!

Elisabeth Knottingham

elisabethknottingham.com