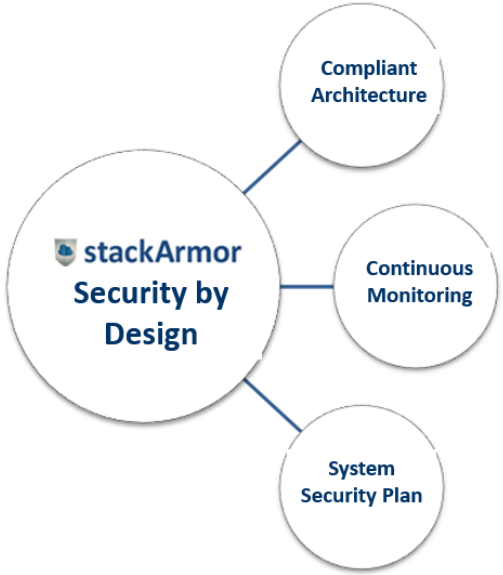
stackArmor

amazon web services | Partner Network

ADVANCED CONSULTING PARTNER

Security by Design



Ensuring the confidentiality, integrity and availability of digital assets in the cloud
Session 3

STACKARMOR MICRO-SUMMIT OCT 2017

Salim Ajmeri, CISSP

stackArmor

- 14+ years of experience in Sarbanes-Oxley, FISMA, FedRAMP, ISCM, CDM, On-going Authorization
- **Government**: DoD Army, IRS, USDA, Mint, FMC
- **Commercial**: AT&T, Deloitte, Orbitz, Avis Budget Group, Centennial Communications, Verizon Wireless

FISMA

stackArmor

- FISMA
  - FIPS
  - SP
- NIST Risk Management Framework (RMF) –SP 800-37r1
  - Previously known as Certification and Accreditation (C&A)
  - Categorize, Select, Implement, Assess, Authorize, Monitor
- Security Assessment and Authorization (SA&A)
  - Security Categorization Worksheet
  - Scope Memo
  - System Security Plan
  - Information System Contingency Plan
  - Assessment Plan
  - Security Assessment Report
  - Authorization to Operate Memo

ISCM

- Information Security Continuous Monitoring
- NIST SP 800-137
- On-going Authorization
- Manual and Automated assessments
- Continuous Diagnostics and Monitoring (CDM)

FedRAMP Program

stackArmor

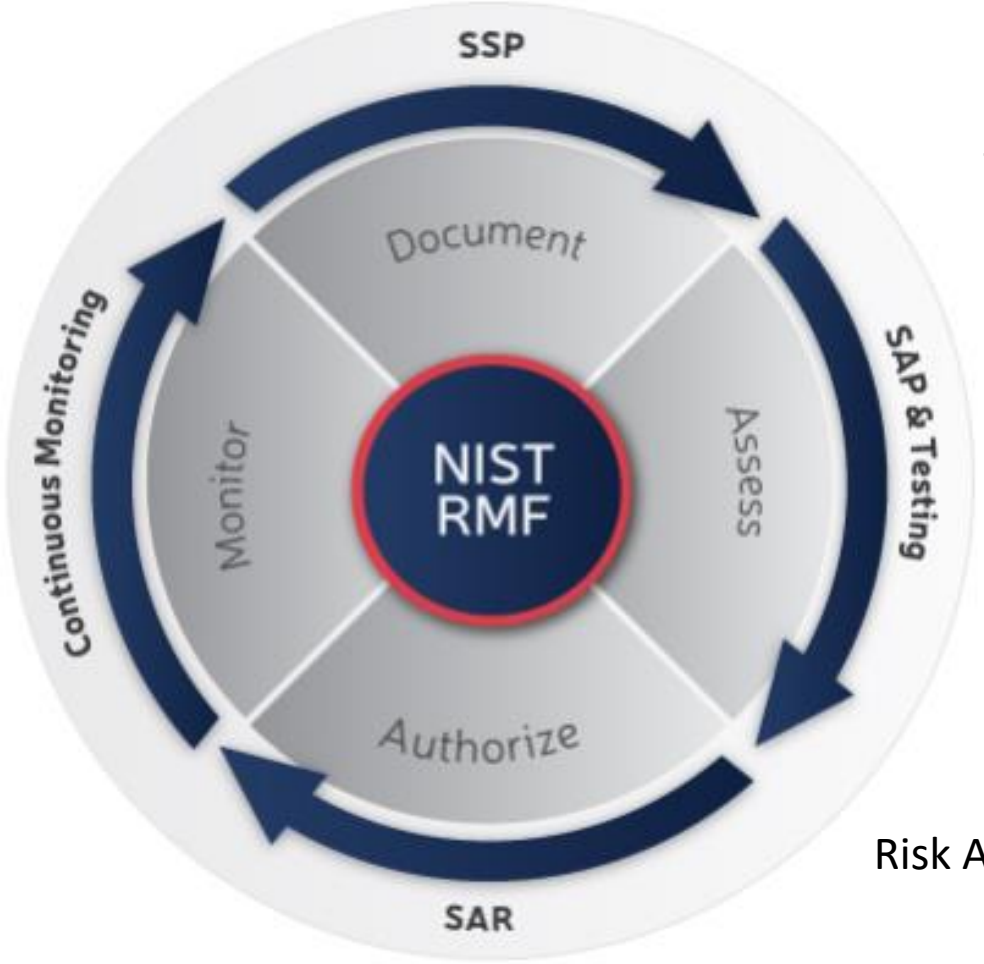
- Program created to support US Government in using secure cloud solutions to meet mission/business needs efficiently
- Complies with FISMA
- Governed by the Joint Authorization Board (JAB) consisting of representatives from DHS, GSA, and DoD
- Solution can be IaaS, PaaS, or SaaS

FedRAMP Required Documents

- Package Checklist
- SSP plus attachments
  - Policies and Procedures
  - User Guide
  - E-Authentication
  - PIA
  - RoB
  - ISCP
  - CMP
  - IRP
  - CIS
  - FIPS 199
  - Separation of Duties Checklist
  - Laws and Regs
  - Inventory
- SAP
  - PenTest Plan and Methodology
  - 3PAO Supplied PenTest material
- SAR
- POAM
- Continuous Monitoring Plan
- ATO Letter (Agency Packages)

FedRAMP Process

Categorize, Select, Implement, Document



3PAO, Assessment, Evidence Collection

Operational Visibility, Change Control, Incident Response

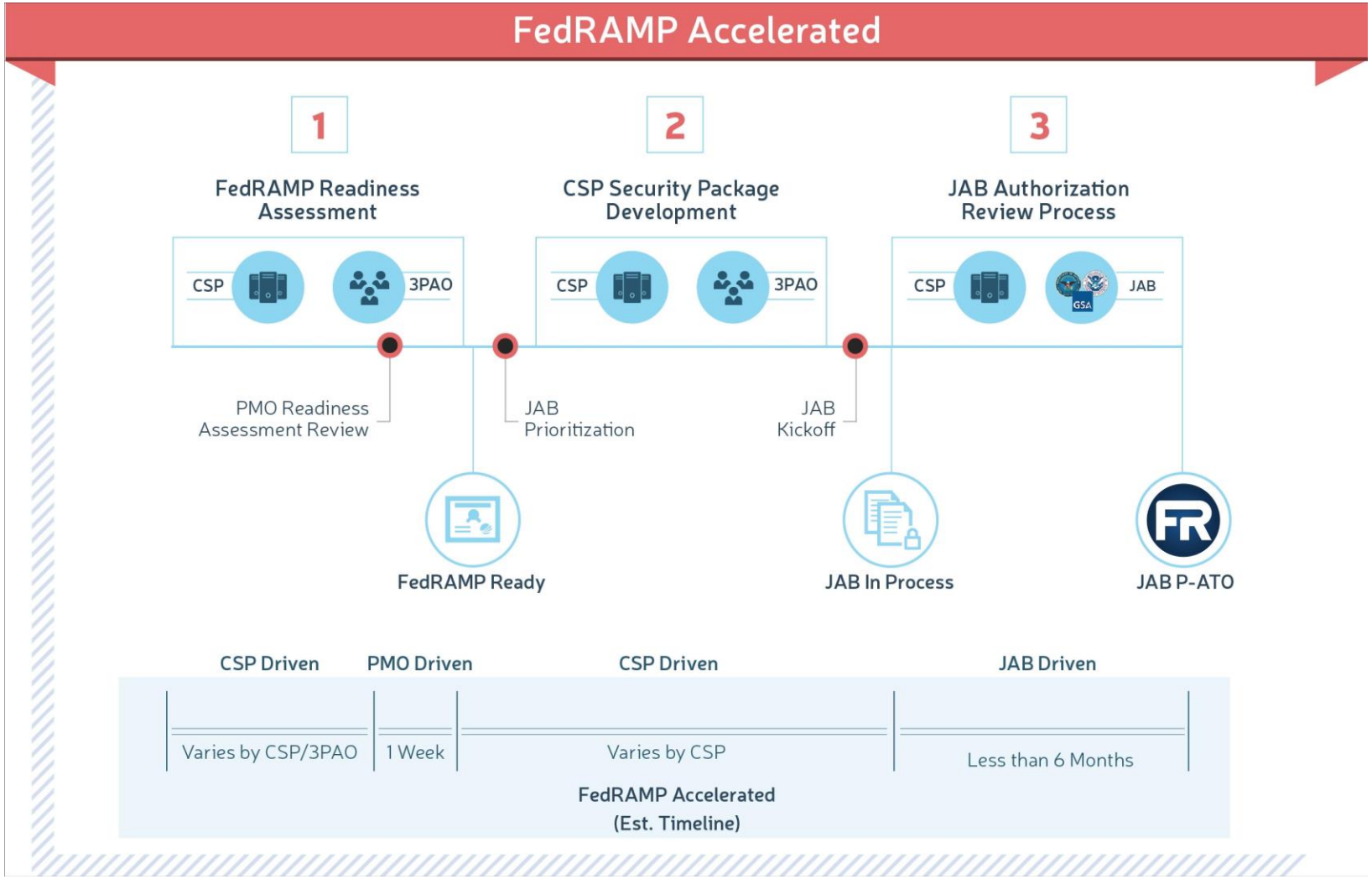
Risk Analysis, POA&Ms, Authorization

FedRAMP Timeline

stackArmor

- Old FedRAMP process was lengthy and largely unpredictable
- FedRAMP accelerated process shifts focus to initial assessment of operational security capabilities instead of the documentation intensive process
- 3PAO Readiness assessment will be reviewed within 1 week and provide agencies, CSPs, and FedRAMP PMO with early feedback on likelihood of CSPs success
- If positive, CSP is noted as ‘FedRAMP ready’ and begins documentation development process

FedRAMP Accelerated Process

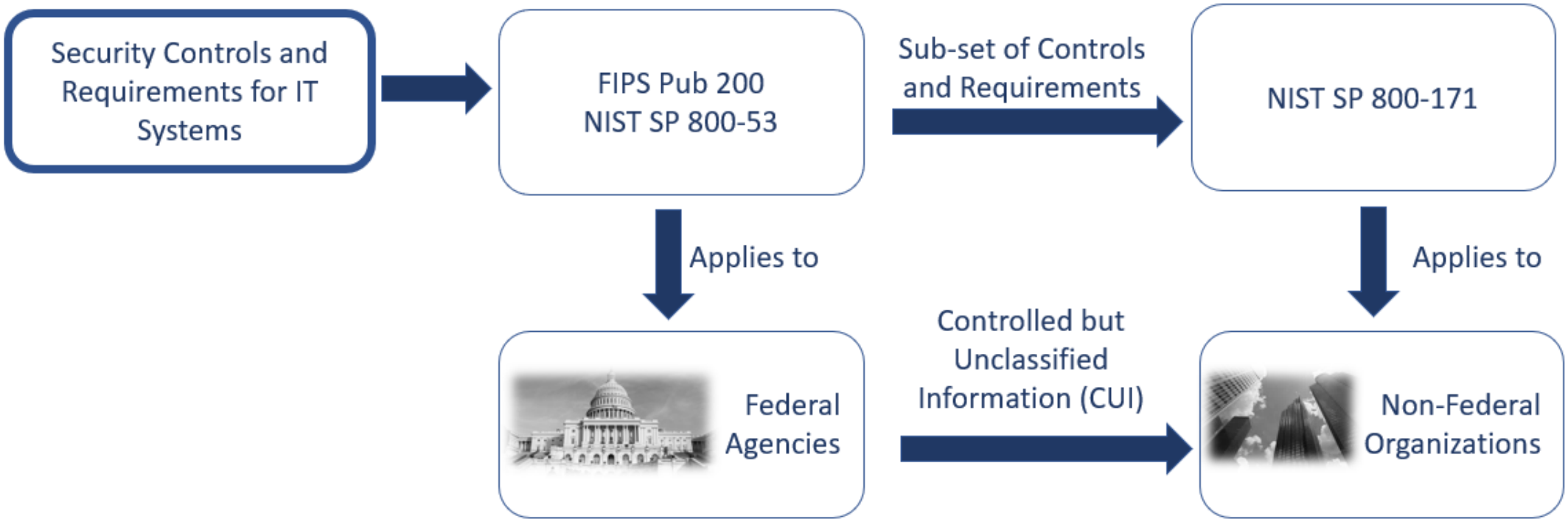


FedRAMP vs DFARS

- Federal Risk and Authorization Management Program (FedRAMP)
  - For Cloud Service Providers
  - Uses NIST SP 800-53 Rev 4 and requires additional non-baselined controls
  - Requires use of a FedRAMP Certified Third Party Assessment Organization (3PAO)
  - System must be authorized by Joint Authorization Board (JAB) or through Federal Agency ATO process
  - Must use FedRAMP provided templates to complete deliverables
- Defense Federal Acquisition Regulation Supplement (DFARS)
  - Defense contractors who process, store, or transmit Controlled Unclassified Information (CUI) within their IT environment
  - Uses NIST SP 800-171 (based off of SP 800-53 and FIPS 200)
  - Requires a self-certification of implementation of security controls
  - No authorization requirements
  - Can choose any format to document control implementation and remediation plans

FedRAMP and NIST SP 800-171

stackArmor



FedRAMP vs DFARS

stackArmor

	FedRAMP	DFARS
Applies to	Cloud Service Providers wanting to host Federal Agency data	Non-Federal Organizations processing, storing, or transmitting CUI
Controls	FedRAMP Controls based on SP 800-53 Rev 4	SP 800-171 based on SP 800-53 and FIPS 200
Assessment	Requires FedRAMP Certified – Third Party Assessment Organization (3PAO)	Self-Certification
Authorization	Must be authorized by FedRAMP PMO or Federal Agency	None
Templates	Must use FedRAMP provided templates	Any format organization chooses

NIST SP 800-53 vs SP 800-171

stackArmor

Control Family	800-53	800-171	Control Family	800-53	800-171
Access Control	35	22	Personnel Security	8	2
Awareness and Training	5	3	Physical Protection	18	6
Audit and Accountability	18	9	Planning	6	0
Configuration Management	21	9	Risk Assessment	7	3
Contingency Planning	22	0	Security Assessment	10	4
Identification and Authentication	22	11	System and Communications Protection	24	16
Incident Response	12	3	System and Information Integrity	21	7
Maintenance	9	6	System and Services Acquisition	14	0
Media Protection	9	9			

SP 800-53	SP 800-171
261	110

DFARS - Implementation

stackArmor

- Organizations must be compliant by December 31, 2017
- Primary focus is the protection of confidentiality of CUI at the moderate risk impact level
- Separate environment using CUI to minimize burden on entire IT infrastructure through use of subnetworks and firewalls
- Leverage security specialists with in-depth knowledge of SP 800-53 to assist in documentation and POA&M creation

FedRAMP Plus (FedRAMP+)

stackArmor

- Leveraging the work done as part of the FedRAMP assessment
- Adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements
- Results used as basis for DoD Provisional Authorization and admittance into DoD Cloud Service Catalog

DoD IL Levels

- DoD Security Requirements Guide v1, r2 – 3/18/16
- Information Impact Levels
  - Sensitivity / Confidentiality level of information (e.g. Public, Private, Classified, etc.) to be stored and process in the cloud
  - Potential impact of an event that results in loss of confidentiality, integrity, or availability
- 6 Levels (pre-2015) are now only 4
  - Level 1 integrated with Level 2; Level 3 integrated with Level 4
  - Based on Moderate Impact Level
  - Adds 30-40 additional controls plus privacy control catalog

DoD IL Levels (Reference Chart)

stackArmor

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

NIST SP 800-53r5

stackArmor

- Final Draft – October 2017
- Final Version – December 29, 2017
- Key Changes made for public draft (August 2017)
  - Making controls outcome-based
  - Integrating the privacy controls into the security control catalog
  - Separating the control selection process from the actual controls
  - Promoting integration with different risk management and cybersecurity approaches and lexicons
  - Incorporating new, state-of-the-practice controls based on threat intelligence and empirical attack data

Thank you

www.stackArmor.com
solutions@stackArmor.com

Security By Design
https://www.stackArmor.com/SecurityByDesign