

Graphion™ | Map Every Threat. Secure Every Connection.

FedRAMP 20x: Persistent Validation and Assessment (PVA) Standard

As part of the FedRAMP 20x initiative, RFC-0017 proposes requirements for a Persistent Validation and Assessment Standard – streamlining FedRAMP 20x authorizations by ¹ “requiring providers to directly and deeply integrate the security and compliance process within their engineering activities”. Consequently, “automation should be used to ² align engineering teams with security goals ³ and empower them to rapidly develop and deploy changes and capabilities ⁴ in an environment where secure outcomes are encouraged or enforced....⁵ including native integration into processes and tools wherever possible.”

Graphion Features	Description	RFC Intentions				
		1	2	3	4	5
Holistic View (SBOM + IBOM)	Overlays each application’s software on dynamic cloud infrastructure, showing exactly what runs on each component in the connected operational cloud ecosystem and thus helps ascertain policy (compliance) mapping; continuously builds this view from (a) an application’s Software Bill of Materials (SBOM) produced by CI/CD pipelines and (b) the Infrastructure Bill of Materials (IBOM) generated by Cloud Security Posture Management (CSPM) as modifications occur within the monitored runtime environment.	✓	✓	✓	✓	✓
Context-Based Scoring	Quantifies risks by combining asset criticality, configuration state, and relevant vulnerability analyses – supporting prioritization based on each application’s holistic view and unique characteristics, shifting focus from "finding everything" to fixing what matters most.	✓	✓	✓	✓	
Compliance Standards	Encodes security controls for all major compliance standards (e.g., NIST SP 800-53 and FedRAMP Moderate), including the mapping of each control to one or more policies and any associated auto-remediation steps. Also implements each policy for all major Cloud Service Providers (AWS, Azure, Google Cloud Platform, Oracle Cloud Infrastructure, etc.).	✓			✓	✓
Compliance Posture	Reports and maintains the detailed and summarized results of each relevant Compliance Standard’s run against the various cloud accounts – including failed controls and any auto-remediation steps taken.	✓	✓	✓	✓	
Policy Creation & Compliance	Permits users to create customized policies, including auto-remediation steps, triggers for policy execution (and evaluation of compliance), and the configuration of notifications to be sent upon policy failure.	✓	✓		✓	✓

Holistic View (SBOM + IBOM)

Compliance Posture

Summary by Control Family

Control Family	Successes	Violations	Errors
ACCESS CONTROL	6	15	1
AUDIT AND ACCOUNTABILITY	4	15	1
SYSTEM AND COMMUNICATIONS PROTECTION	5	11	1
SYSTEM AND INFORMATION INTEGRITY	2	8	1
SECURITY ASSESSMENT AND AUTHORIZATION	2	3	1
INCIDENT RESPONSE	2	0	0
RISK ASSESSMENT	2	0	0

Policy Creation & Compliance

Summary by Control Family

▼ AUDIT AND ACCOUNTABILITY

% Resources Compliant: 85.22%

Control Violations: 11

Control Name	Policy Name	Resource Type	Status	Action
AU-2 Event Logging	AWS Audit Cloudtrail...	Account	Violations	VIEW
AU-2 Event Logging	AWS Audit VPC Flow...	VPC	Success	VIEW
AU-2 Event Logging	Azure Audit Network ...	Virtual_Networks	Success	VIEW
AU-3 Content of Audit Records	AWS Audit S3 Bucket...	S3	Success	VIEW
AU-3 Content of Audit Records	Azure Audit Diagnosti...	Azure_Discover...	Violations	VIEW

Graphion's core features cover the categorized FedRAMP Requirements (FRR) presented in RFC-0017

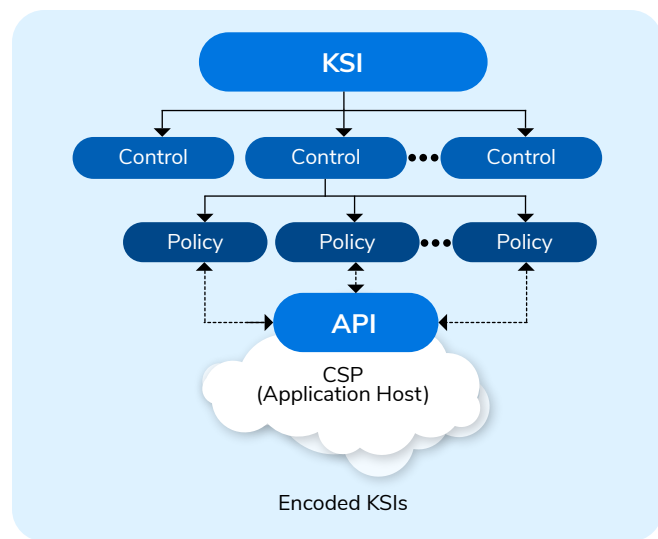
Graphion Features

ID	Requirement Summary	How Graphion Helps	HV	CBS	CS	CP	PC
PVA Blanket requirements for the Persistent Validation and Assessment (PVA) standard			HV = Holistic View; CBS = Context-Based Scoring; CS = Compliance Standards; CP = Compliance Posture; PC = Policy Creation				
01	Maintain simple high-level summaries of various attributes for each Key Security Indicator (KSI) .	<ul style="list-style-type: none"> Captures & maintains configuration data for automatable KSIs. Maintains configurable mapping of KSIs to policies, plus policies to standards. 			✓		✓
02	Persistently run validation processes for each KSI , in accordance with (IAW) the application's FedRAMP baseline's timeframes for persistent validation.	<ul style="list-style-type: none"> Performs validation for each build (SBOM-based). Performs validation for each CSPM-generated IBOM. Uses context-based scoring to assess validation results. 	✓	✓			✓
03	Treat failures detected during persistent validation as vulnerabilities and remediate them accordingly.	<ul style="list-style-type: none"> Leverages context-based scores to translate validation results into risk-prioritized vulnerabilities. 	✓	✓			✓
04	Include persistent validation activity in the requisite reports on vulnerability detection and response activity .	<ul style="list-style-type: none"> Tracks detailed validation analytics for each build (SBOM) and infrastructure mod (IBOM). 	✓	✓			✓
05	Track significant changes that impact KSIs.	<ul style="list-style-type: none"> Tracks each build (SBOM) and CSPM run (IBOM). Permits comparison between different versions. 	✓				
TF-LO Requirements for timeframes for FedRAMP Low authorizations							
02	Complete the validation processes for KSIs of machine-based information resources at least once every 7 days.	<ul style="list-style-type: none"> Performs validation for each build (SBOM). Performs validation for each CSPM run, with configurable frequency. 	✓	✓			✓
03	Complete a Persistent FedRAMP Assessment at least once every 12 months.	<ul style="list-style-type: none"> Performs validation for each build (SBOM). Performs validation for each CSPM run, with configurable frequency. Permits comparison between different versions to identify significant changes. 	✓	✓			✓
TF-MO Requirements for timeframes for FedRAMP Moderate authorizations							
02	Complete the validation processes for KSIs of machine-based information resources at least once every 3 days.	<ul style="list-style-type: none"> Performs validation for each build (SBOM). Performs validation for each CSPM run, with configurable frequency. 	✓	✓			✓
03	Complete a Persistent FedRAMP Assessment at least once every 9 months.	<ul style="list-style-type: none"> Performs validation for each build (SBOM). Performs validation for each CSPM run, with configurable frequency. Permits comparison between different versions to identify significant changes. 	✓	✓			✓
PA Requirements pertaining to providers of a cloud service offering							
01	Have the implementation of goals and validation processes assessed by a 3PAO or FedRAMP, then report the results.	<ul style="list-style-type: none"> Integrates with CI/CD pipelines for builds (on demand). Agentless integration with CSPs for CSPM, with configurable frequency of execution. 	✓	✓	✓	✓	✓
02	Allow a complete assessment of validation procedures by all necessary assessors.	<ul style="list-style-type: none"> Maintains configurations for all KSIs. Maintains audit trail for executions of all SBOM (builds) and IBOM (CSPM) runs. 	✓	✓	✓	✓	✓
03	Provide technical explanations, demonstrations, and proof to all necessary assessors regarding assertions of technical capabilities to meet KSIs and provide validations.	<ul style="list-style-type: none"> Enables and tracks configurations for all KSIs, including mapping to security standards. Tracks the execution and results of all validation runs. 	✓	✓	✓	✓	✓
07	Maintain sufficient information about significant changes	<ul style="list-style-type: none"> Permits comparison between different SBOM (software) and IBOM (infrastructure) versions – and the combination/overlay thereof – to identify significant changes. 	✓				

ID	Requirement Summary	How Graphion Helps	HV	CBS	CS	CP	PC
AA	Requirements pertaining to assessors of a cloud service offering						
01	Evaluate the underlying processes that providers use to validate KSIs.	<ul style="list-style-type: none"> Easily integrates with CI/CD pipelines (SBOM) through SBOM submission via APIs. Supports agentless CSPM integration with CSPs (IBOM). 	✓	✓	✓	✓	✓
02	Evaluate the accuracy of KSI goals against actual implementation of the process.	<ul style="list-style-type: none"> Reports configurations for all KSIs. Reports analytics for all executions of SBOM (builds) and IBOM (CSPM) runs. Supports customized policies (in addition to standard policies). 	✓	✓	✓	✓	✓
03	Evaluate if the underlying processes are consistently creating the desired security outcome documented by the provider.	<ul style="list-style-type: none"> Reports configurations. Reports diffs between executions of SBOM (builds) and IBOM (CSPM) runs. 	✓	✓	✓	✓	✓
04	Perform evaluation using a combination of quantitative and expert qualitative assessment.	<ul style="list-style-type: none"> Provides quantitative data for all KSI validations. Facilitates qualitative analysis. 	✓	✓		✓	
06	Minimize reliance on screenshots, configuration dumps, or other point-in-time output as evidence.	<ul style="list-style-type: none"> Provides evidence via tracked KSI configurations and validation results. 	✓	✓	✓	✓	✓
09	Deliver a high-level summary of the assessment process and resulting findings for each relevant KSI.	<ul style="list-style-type: none"> Tracks and reports KSI configurations and validation results. 	✓	✓		✓	
11	Limit persistent assessments to significant changes made by the cloud service offering.	<ul style="list-style-type: none"> Permits comparison between different SBOM (software) and IBOM (infrastructure) versions – and the combination/overlay thereof – to identify significant changes. 	✓				

CoreStack maps each KSI

- to the relevant automatable NIST 800-53 security controls
- implemented as policies
- integrated with each major CSP



Sample Set of KSIs

ID	KSI Summary	NIST Security Controls Mapping	HV	CBS	CS	CP	PC
CMT	Change Management		HV = Holistic View; CBS = Context-Based Scoring; CS = Compliance Standards; CP = Compliance Posture; PC = Policy Creation				
01	Log and monitor system modifications.	<ul style="list-style-type: none"> au-2 Event Logging cm-3 Configuration Change Control cm-4.2 Verification of Controls cm-6 Configuration Settings ma-2 Controlled Maintenance 	✓		✓	✓	
02	Execute changes through redeployment of version controlled immutable resources rather than direct modification wherever possible.	<ul style="list-style-type: none"> cm-2 Baseline Configuration cm-3 Configuration Change Control cm-5 Access Restrictions for Change cm-6 Configuration Settings cm-7 Least Functionality cm-8.1 Updates During Installation and Removal si-3 Malicious Code Protection 	✓		✓	✓	

CNA Cloud Native Architecture

01	Configure ALL information resources to limit inbound and outbound traffic.	<ul style="list-style-type: none"> ac-17.3 Managed Access Control Points ca-9 Internal System Connections 			✓	✓	✓
03	Use logical networking and related capabilities to enforce traffic flow controls.	<ul style="list-style-type: none"> ac-17.3 Managed Access Control Points ca-9 Internal System Connections sc-7 Boundary Protection 			✓	✓	
04	Use immutable infrastructure with strictly defined functionality and privileges by default.	<ul style="list-style-type: none"> cm-2 Baseline Configuration si-3 Malicious Code Protection 	✓	✓			
05	Have denial of service protection .	<ul style="list-style-type: none"> sc-5 Denial-of-service Protection 			✓	✓	

IAM Identity and Access Management

01	Enforce multi-factor authentication (MFA) using methods that are difficult to intercept or impersonate (phishing-resistant MFA) for all user authentication.	<ul style="list-style-type: none"> ac-2 Account Management ia-2 Identification and Authentication (Organizational Users) ia-2.1 Multi-factor Authentication to Privileged Accounts ia-2.2 Multi-factor Authentication to Non-privileged Accounts ia-2.8 Access to Accounts — Replay Resistant ia-8 Identification and Authentication (Non-organizational Users) 			✓	✓	
02	Use secure passwordless methods for user authentication and authorization when feasible, otherwise enforce strong passwords with MFA.	<ul style="list-style-type: none"> ac-2 Account Management ac-3 Access Enforcement ia-2.1 Multi-factor Authentication to Privileged Accounts ia-2.2 Multi-factor Authentication to Non-privileged Accounts ia-2.8 Access to Accounts Replay Resistant ia-5.1 Password-based Authentication ia-5.2 Public Key-based Authentication ia-5.6 Protection of Authenticators ia-6 Authentication Feedback 			✓	✓	
03	Enforce appropriately secure authentication methods for non-user accounts and services.	<ul style="list-style-type: none"> ac-2 Account Management ac-4 Information Flow Enforcement ia-3 Device Identification and Authentication ia-5.2 Public Key-based Authentication 			✓	✓	
06	Automatically disable or otherwise secure accounts with privileged access in response to suspicious activity.	<ul style="list-style-type: none"> ac-2 Account Management ac-2.1 Automated System Account Management ac-2.3 Disable Accounts ac-2.13 Disable Accounts for High-risk Individuals ac-7 Unsuccessful Logon Attempts ps-4 Personnel Termination ps-8 Personnel Sanctions 			✓	✓	

INR Incident Reporting

01	Report incidents according to FedRAMP requirements and cloud service provider policies.	<ul style="list-style-type: none"> ir-4 Incident Handling ir-4.1 Automated Incident Handling Processes ir-6 Incident Reporting ir-6.1 Automated Reporting ir-7 Incident Response Assistance ir-7.1 Automation Support for Availability of Information and Support ir-8 Incident Response Plan 			✓	✓	
03	Maintain a log of incidents and periodically review past incidents for patterns or vulnerabilities.	<ul style="list-style-type: none"> ir-3 Incident Response Testing ir-4 Incident Handling ir-4.1 Automated Incident Handling Processes ir-8 Incident Response Plan 			✓	✓	

MLA Monitoring, Logging, and Auditing

03	Rapidly detect and remediate or mitigate vulnerabilities .	<ul style="list-style-type: none"> • au-5 Response to Audit Logging Process Failures • ca-7 Continuous Monitoring • ra-5 Vulnerability Monitoring and Scanning • ra-5.2 Update Vulnerabilities to Be Scanned • sa-22 Unsupported System Components • si-2 Flaw Remediation • si-5 Security Alerts, Advisories, and Directives 	✓	✓	✓	✓	✓
05	Perform Infrastructure as Code and configuration evaluation and testing.	<ul style="list-style-type: none"> • ca-7 Continuous Monitoring • cm-2 Baseline Configuration • cm-6 Configuration Settings 	✓	✓			

SVC Service Configuration

03	Encrypt all federal and sensitive information at rest.	<ul style="list-style-type: none"> • ac-20.2 Portable Storage Devices — Restricted Use • cm-12 Information Location • cp-9.8 Cryptographic Protection • sc-13 Cryptographic Protection 			✓	✓	
06	Use automated key management systems to manage, protect, and regularly rotate digital keys and certificates.	<ul style="list-style-type: none"> • ac-17.2 Protection of Confidentiality and Integrity Using Encryption • ia-5.2 Public Key-based Authentication • ia-5.6 Protection of Authenticators • sc-12 Cryptographic Key Establishment and Management 			✓	✓	

TPR Third-Party Information Resources

02	Regularly confirm that services handling federal customer data or are likely to impact the confidentiality, integrity, or availability of federal customer data are FedRAMP authorized and securely configured .	<ul style="list-style-type: none"> • ac-21 Information Sharing • ca-3 Information Exchange • cm-12 Information Location • ps-7 External Personnel Security • sa-2 Allocation of Resources • sa-4 Acquisition Process • sa-9 External System Services 	✓	✓	✓	✓	
----	---	---	---	---	---	---	--



CoreStack is an AI-powered NextGen Cloud Governance & Security Platform that enables enterprises to embrace cloud with confidence, rapidly achieving continuous and autonomous cloud governance at scale. CoreStack helps 750+ global enterprises govern more than \$2B in annual cloud consumption. The company is a Microsoft Azure (Legacy) Gold Partner, Amazon AWS Technology Partner with Cloud Operations Competency, Oracle Cloud Build Partner, and Google Cloud Build Partner.