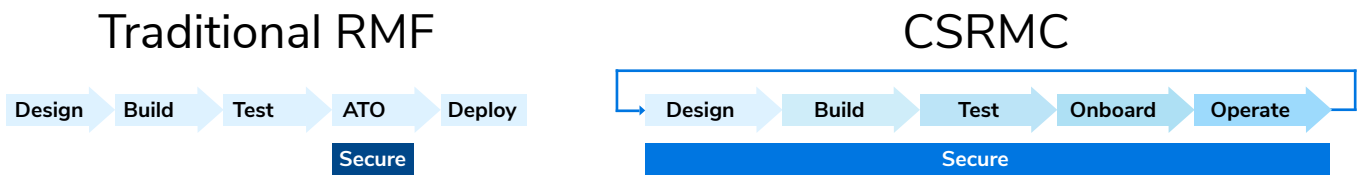
Graphion™ | Map Every Threat. Secure Every Connection.

Cybersecurity Risk Management Construct (CSRMC)

The Department of War (DoW) recently introduced the CSRMC as "a transformative framework to deliver real-time cyber defense at operational speed". At first glance, the CSRMC may appear to be a repackaged version of NIST's Risk Management Framework (RMF) – especially since each RMF step is explicitly mapped to one of CSRMC's phases. However, on further examination, it becomes apparent that CSRMC ***extends*** the RMF in one subtle but crucial way: **it involves the Security Team at the start of solution development and thus embeds security throughout the entire lifecycle.** Hence, the implementation of security-related requirements becomes as critical to a project's success as functional requirements.



RMF Challenge		CSRMC Approach	Tenets Met [1]									
Title	**Description**	**Remedy**	A	CC	CC&A	DSO	CS	T	E&I	O	R	CA
Late Security	ATO is **bolted-on** towards the end of the cycle, which typically results in re-work and delays.	Security is **built-in** from the start, treated as part of the application and developed along with all other features… then **continuously assessed and tuned** post-deployment.	✓	✓	✓	✓	✓	✓	✓	✓		✓
Tunnel-Visioned Teams	Teams are **siloed**, operating within their respective phases of the assembly line.	Teams are **integrated**, collaborating throughout the entire cycle.				✓		✓		✓		✓
Disjointed Metrics	Data is **manually collected** and **heavily abstracted** (e.g., checklists).	**Organized and standardized** data is **automatically collected**.	✓	✓	✓	✓			✓	✓	✓	✓
"Point in Time" Assessments	**Every 3 years**, a **single release** is assessed, **iteratively stabilized**, then **deployed and forgotten**.	Assessments are **automatically performed** with **every build**; deployed applications are **continuously monitored**.	✓		✓	✓					✓	✓
Costly	Manual efforts (including re-work due to issues identified late in the cycle) require significant time and effort, leading to **schedule and budget overruns.**	**Continuous and contextualized assessments** help teams focus efforts on the right spots, allowing teams to **get the most from their resources and budgets**.	✓	✓	✓	✓		✓	✓	✓	✓	✓

[1] A=Automation CC=Critical Controls CC&A=CONMON, Control, and ATO DSO=DevSecOps CS=Cyber Survivability T=Training E&I=Enterprise & Inheritance O=Operationalization R=Reciprocity CA=Cybersecurity Assessments (for details on all tenets, reference DoW's Strategic Tenets)

Remedies Implemented Integrate, Calibrate, Evaluate

CoreStack's Cloud Native Application Protection Platform (CNAPP) - with Graphion as its foundation - **implements CSRMC's remedies** via a solution that makes it easy for Security Teams to:

1. **INTEGRATE** into the lifecycle from the start
2. **CALIBRATE** applications as pertinent information emerges across the lifecycle
3. **EVALUATE** applications after deployment to ensure compliance

Phase 1: Design → Phase 2: Build (IOC) → Phase 3: Test (FOC) → Phase 4: Onboard → Phase 5: Operations

CSRMC Remedy	INTEGRATE — SecOps: Map & Encode Policies / Select Standards/ Controls / Customize Policies & Remediation	CALIBRATE — AppSecOps: Overlay SBOM & IBOM / Context-ualize Vulnerabilities / Assess Vulnerability Prevalence	EVALUATE — CloudOps: Assess Policy Compliance / Calculate Compliance Posture / Assess Cross-Cloud Posture
Built-In Security	• Leverage "out of the box" policies coded for major Cloud Service Providers (CSPs) • Capitalize on pre-mapped policies to security controls under major standards (e.g., FedRAMP) • Create customized policies & remediation logic to address unique needs	• See full scope of what runs on each component in the cloud ecosystem • Acquire clear, powerful, and holistic insights into an application to fix what matters most • Assess the prevalence of each vulnerability throughout your organization to determine priority and ownership	• Ensure continuous compliance as your applications evolve • Support self-attestations to improve adoption of your applications • Maintain detailed posture snapshots for each build & deployment
Integrated Teams	• Developers understand security requirements in their terms (Policy as Code) • Security selects the appropriate compliance standards – and thus the corresponding controls and underlying policies • Operations views/tunes/creates remediation steps for each policy	• Developers clearly understand what specifically needs to be fixed and why (the needles in the haystack of vulnerabilities) • Security has visibility into posture improvements across builds • Operations knows what specifically is changing in upcoming releases and can adequately prepare to support them	• Developers acquire intel about issues that surface and need to be fixed post-deployment • Security gains rapid insights into holistic runtime security, including the prevalence of Known Exploited Vulnerabilities (KEV) • Operations can assess policy violations and determine the relevant course of action
Useful Metrics	Understand and effectively utilize the data generated by each: • Control • Policy violation • Remediation script	• Process security assessment results per build • Consider auto-generated contextualized scores as well as industry insights (e.g., Common Vulnerability Scoring System (CVSS)) • Access industry references from a single pane of glass (e.g., vulnerability bulletins)	• Inspect the posture of multi-cloud accounts from a single pane of glass • Analyze detailed messages that triggered any policy violation • View multi-cloud inventory, including groupings by service category
Continuous Assessments	• Configure assessment frequency per application, environment, and CSP • Assess proper handling of runtime violations • Review and tune selected standards, controls, policies, and/or remediation scripts on an as-needed basis	• Initiate build-related assessments on an as-needed basis or integrate them into CI/CD pipelines for automated assessments • Examine time series (build-over-build) to determine posture improvements • Identify shifted priorities based on industry knowledge and dynamic application characteristics	• Automatically perform assessments in accordance with configured schedules • Create an ongoing evidence pipeline to support audit-ready reporting for various industry standards and security requirements • Leverage CSP-native services agentlessly
High Value	• Select relevant standards; no need to bother with tedious controls and policies (per CSP) • Utilize the holistic view (SBOM + IBOM) to set up proper controls per asset (e.g., for internet-reachable resources) • Use templated scripts to remediate policy violations automatically or on-demand	• Detect issues early; avoid significant rework • Pinpoint the right team to make changes (based on expertise and ownership); fix once, use for many • With security embedded throughout the lifecycle, streamline final sign-off for deployments	• Quickly identify security issues, which could "save face" in addition to time, money, and effort • Create a multi-cloud hub of runtime data unique to your organization, streamlining operations • Capitalize on the data hub via Agentic AI to further improve your cloud ecosystem

Tenets Followed

	Phase 1: Design	Phase 2: Build (IOC)	Phase 3: Test (FOC)	Phase 4: Onboard	Phase 5: Operations
	INTEGRATE		CALIBRATE		EVALUATE
	SecOps		AppSecOps		CloudOps
	Map & Encode Policies	Select Standards/ Controls	Customize Policies & Remediation	Overlay SBOM & IBOM	Context-ualize Vulnerabilities	Assess Vulnerability Prevalence	Assess Policy Compliance	Calculate Compliance Posture	Assess Cross-Cloud Posture
Automation	✓		✓	✓	✓	✓	✓	✓	✓
Critical Controls	✓	✓	✓	✓			✓	✓	✓
Continuous Monitoring (COMMON), control, and ATO	✓	✓	✓		✓	✓	✓	✓	✓
DevSecOps		✓	✓		✓	✓	✓	✓	✓
Cyber Survivability			✓	✓					✓
Training					✓	✓			
Enterprise Services & Inheritance	✓	✓	✓				✓	✓	✓
Operationalization				✓		✓	✓	✓	✓
Reciprocity	✓						✓	✓	✓
Cybersecurity Assessments		✓	✓		✓	✓		✓	✓

CoreStack improves the secure operations of all applications (software and infrastructure)... which includes streamlining and securing the build process

Solutions Integrated

Phase 1: Design

Phase 2: Build (IOC)

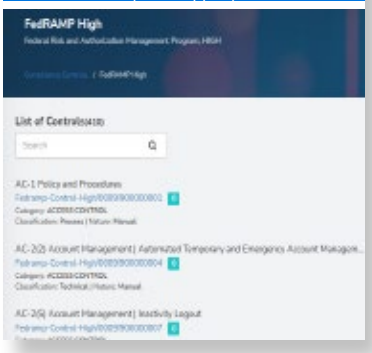
Phase 3: Test (FOC)

Phase 4: Onboard

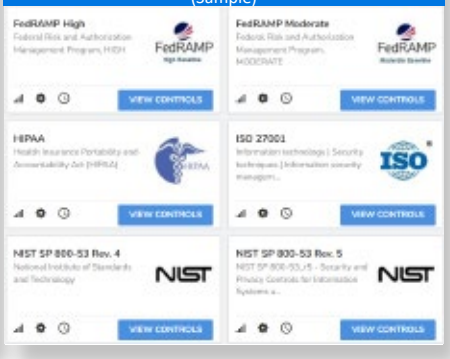
Phase 5: Operations

INTEGRATE

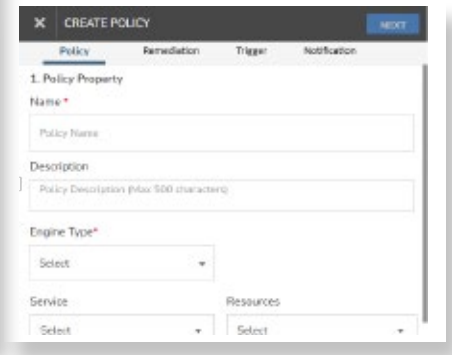
Controls & Policies
(Pre-Mapped)



Compliance Standards
(Sample)

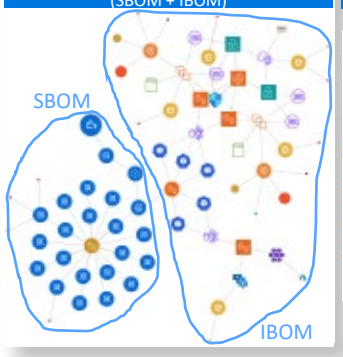


Policy Customization

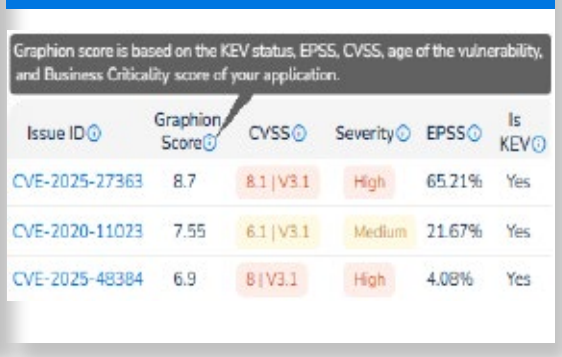


CALIBRATE

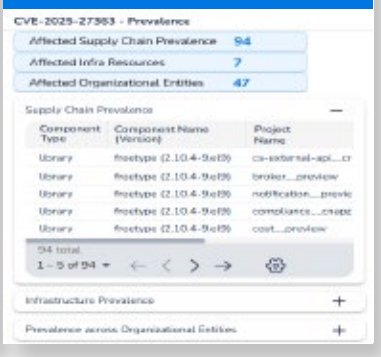
Holistic View
(SBOM + IBOM)



Context-Based Scoring

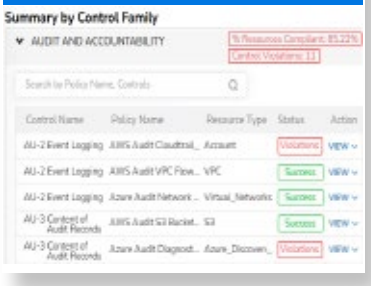


Vulnerability Prevalence

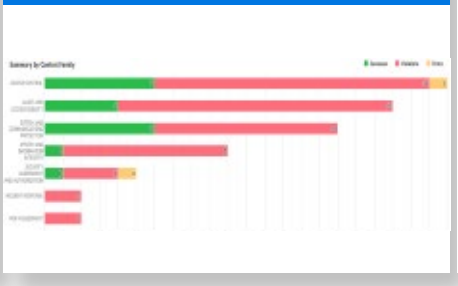


EVALUATE

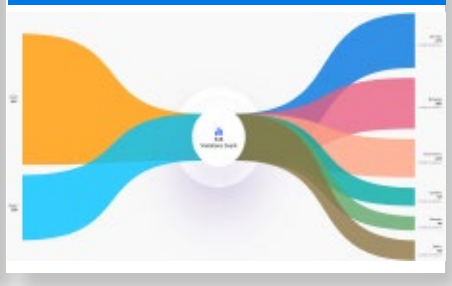
Policy Compliance



Compliance Posture



Multi-Cloud Posture



CORESTACK®

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.