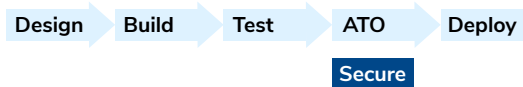


Graphion™ | Map Every Threat. Secure Every Connection.

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.

Traditional RMF



CSRMC



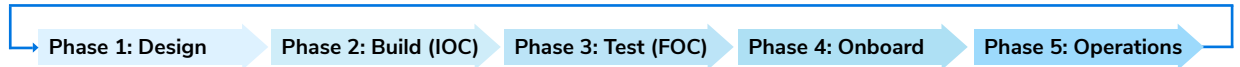
RMF Challenge		CSRMC Approach	Tenets Met ¹									
Title	Description	Remedy	A	CC	CC&A	DSO	CS	T	E&I	O	R	CA
Late Security	ATO is bolted-on towards the end of the cycle, which typically results in re-work and delays.	Security is built-in from the start, treated as part of the application and developed 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=COMMON, 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













CSRMC Remedy

	INTEGRATE SecOps	CALIBRATE AppSecOps	EVALUATE 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

Built-In Security	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<p>Understand and effectively utilize the data generated by each:</p> <ul style="list-style-type: none"> Control Policy violation Remediation script 	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 SecOps			CALIBRATE AppSecOps		EVALUATE 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

INTEGRATE

Phase 1: Design

Controls & Policies (Pre-Mapped)

FedRAMP High
Federal Risk and Authorization Management Program, HIGH

List of Controls (10)

AC-1 Policy and Procedures
FedRAMP Control High(020300000000)
Category: ACCESS/CONTROL
Classification: Process (Native Manual)

AC-2(2) Account Management (1) Administrative Temporary and Emergency Account Management
FedRAMP Control High(020300000004)
Category: ACCESS/CONTROL
Classification: Technical (Native Manual)

AC-2(9) Account Management (1) Inactivity Logout
FedRAMP Control High(020300000007)
Category: ACCESS/CONTROL

Compliance Standards (Sample)

FedRAMP High
Federal Risk and Authorization Management Program, HIGH

FedRAMP Moderate
Federal Risk and Authorization Management Program, MODERATE

HEPAA
Health Insurance Portability and Accountability Act (HIPAA)

ISO 27001
Information technology Security techniques Information security management...

NIST SP 800-53 Rev. 4
National Institute of Standards and Technology

NIST SP 800-53 Rev. 5
NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems...

Policy Customization

CREATE POLICY

1. Policy Property

Name*

Policy Name

Description

Policy Description (max 500 characters)

Engine Type*

Select

Service

Resources

Phase 2: Build (IOC)

CALIBRATE

Holistic View (SBOM + IBOM)

SBOM

IBOM

Context-Based Scoring

Graphion score is based on the KEV status, EPSS, CVSS, age of the vulnerability, and Business Criticality score of your application.

Issue ID	Graphion Score	CVSS	Severity	EPSS	Is KEV
CVE-2025-27363	8.7	8.1 V3.1	High	65.21%	Yes
CVE-2020-11023	7.55	6.1 V3.1	Medium	21.67%	Yes
CVE-2025-48384	6.9	8 V3.1	High	4.08%	Yes

Vulnerability Prevalence

CVE-2025-27363 - Prevalence

Affected Supply Chain Prevalence: 5/4

Affected Infra Resources: 7

Affected Organizational Entities: 4/7

Supply Chain Prevalence

Component Type	Component Name (Version)	Project Name
Library	freetype (2.10.4-9e10)	cs-external-api...
Library	freetype (2.10.4-9e10)	broker_preview
Library	freetype (2.10.4-9e10)	notification_provi
Library	freetype (2.10.4-9e10)	compliance_crypt
Library	freetype (2.10.4-9e10)	cost_preview

5/4 total

Infrastructure Prevalence

Prevalence across Organizational Entities

Phase 3: Test (FOC)

Phase 4: Onboard

EVALUATE

Policy Compliance

Summary by Control Family

AUDIT AND ACCOUNTABILITY

81 Passions Controls (81/22%)
Custom Violations: 11

Control Name	Policy Name	Resource Type	Status	Action
AU-2 Event Logging	AIRIS Audit Cloudtrail...	Account	Violations	VIEW
AU-2 Event Logging	AIRIS Audit VPC Flow...	VPC	Success	VIEW
AU-2 Event Logging	Azure Audit Network...	Virtual Networks	Success	VIEW
AU-3 Control of Audit Records	AIRIS Audit S3 Bucket...	S3	Success	VIEW
AU-3 Control of Audit Records	Azure Audit Diagon...	Azure Diagon...	Violations	VIEW

Compliance Posture

Bar chart showing compliance posture across various categories.

Multi-Cloud Posture

Sankey diagram showing the flow of compliance posture across different cloud providers and services.

Phase 5: Operations



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.