CRJ Security

COMBAT. REINFORCE. JUSTIFY.

Security Governance Methodology

“Security maturity informs governance. Governance enables security.”

Security Governance Methodology

CRJ Security
COMBAT. REINFORCE. JUSTIFY.

Overview

CRJ Security applies a **governance-first cybersecurity methodology** designed to help organizations understand their current security posture, establish defensible governance, and maintain executive oversight over time.

Rather than focusing on technical remediation or security tooling, this methodology emphasizes **clarity, accountability, and documentation**—the foundational elements required for effective cybersecurity programs, audit readiness, and informed leadership decision-making.

Methodological Approach

The CRJ Security Governance Methodology follows a structured, risk-aligned lifecycle:

Assess → Govern → Authorize → Oversee

This approach ensures cybersecurity efforts are grounded in organizational reality and supported by formal governance.

Phase 1: Security Maturity Assessment

Objective:

Establish a clear, evidence-based understanding of the organization's current cybersecurity posture.

Summary:

CRJ Security evaluates maturity across key security domains, measuring the consistency, formalization, and oversight of security practices. The assessment provides domain-level scoring and an executive summary of strengths, weaknesses, and systemic gaps.

Key Outcome:

A defensible baseline that answers:

"Where are we today?"

Phase 2: Policy Coverage & Governance Analysis

Objective:

Determine whether the organization has appropriate governance and documentation in place given its risk profile.

Summary:

Building on the maturity assessment, CRJ Security analyzes existing security policies and governance artifacts to identify coverage gaps, outdated documentation, and governance

maturity. The analysis focuses on policy existence, ownership, approval, and review discipline, with alignment to recognized frameworks such as NIST CSF and CIS Controls.

Key Outcome:

A policy coverage and governance view that answers:

"Do we have the governance we should have, given our risk?"

Phase 3: Governance Establishment & Authorization

Objective:

Formalize security expectations through approved governance artifacts.

Summary:

Organizations may establish or enhance security policies, charters, and role definitions to clearly document authority, accountability, and expectations. This phase emphasizes leadership authorization and consistency, not technical implementation.

Key Outcome:

Formally approved and documented cybersecurity governance.

Phase 4: Oversight, Review, and Re-Assessment

Objective:

Maintain effective governance over time.

Summary:

CRJ Security supports periodic policy review and re-assessment to ensure governance remains current as organizational risk evolves. Comparative reporting provides leadership with ongoing visibility into governance health.

Key Outcome:

Sustained oversight and audit-ready governance documentation.

Scope Statement

CRJ Security focuses on **cybersecurity governance, documentation, and executive-level reporting**. This methodology complements—but does not replace—technical security operations or managed services.

Guiding Principle

Security maturity informs governance. Governance enables security.