Blade RiskManager - AI Enabling DoW CSRMC

Executive Overview

The Department of War (DoW) Cybersecurity Risk Management Construct (CSRMC) framework advances beyond traditional cybersecurity approaches by emphasizing automation, continuous authorization, and mission-centric cyber readiness. While the NIST Risk Management Framework (RMF) provides foundational guidance for strengthening cybersecurity posture, it remains largely compliance-focused and dependent on manual processes, limiting scalability and the ability to achieve continuous assurance.

Although automated risk management products such as Blade RiskManager have long advocated for automation and 'shift-left' practices— embedding cybersecurity activities earlier in system development to identify and manage intrinsic risk as a key driver for effective security requirements—adoption has historically been limited. Most efforts remained focused on periodic assessments, manually linking vulnerabilities to mission risks, performing ad-hoc attack path modeling, and staging checklist-driven compliance.

While adversaries increasingly leverage Artificial Intelligence (AI) to conduct sophisticated and adaptive cyberattacks, defenders cannot rely on slow, manual, and reactive defenses. Modern cyber warfare demands AI-driven capabilities that allow defenders to continuously, instantaneously, and dynamically assess mission risk in response to evolving threats. They must be able to identify the highest-impact risks to mission success and automatically determine the most effective mitigations and their optimal placement to reduce risk to an acceptable level.

About Blade RiskManager (BRM)

BRM is a standards-based commercial solution already deployed across government and industry, where it has been proven effective in operational environments. It delivers end-to-end, AI-driven cyber risk automation enabling CSRMC framework transformation from reactive RMF compliance to proactive mission assurance. It enables data-driven automation, continuously adaptive, mission-centric cybersecurity intelligence across the DoW Defense Systems and Information Network.

BRM integrates and extends digital engineering frameworks to deliver fully automated model-based cyber risk assessment. Using a Model-Based Systems Engineering (MBSE) approach, BRM gathers detailed information about systems under analysis, enabling risk evaluation early in the design and development lifecycle. When integrated into DevSecOps pipelines, BRM enhances analytical depth, ensures consistent objectivity, and supports continuous assessment of architectural or threat changes while recommending appropriate mitigations.

BRM serves as the analytical backbone for CSRMC, mission, system, and control architectural layers to facilitate proactive defence. It automates attack path and attack tree analysis, prioritized risk assessment, and Test & Evaluation (T&E) reporting. Its AI reasoning engine enhances automation through a standards-based ontology encompassing knowledge modeling, knowledge graphs, rule enforcement, model-based prediction, Bayesian updating, fuzzy logic, and formal verification. Together, these capabilities deliver proactive, explainable, and scalable cyber risk management.

When extended with complementary Blade Solutions—including Blade OneReport and Blade Validate—BRM provides broader integration to achieve full-spectrum cyber resilience and seamless interoperability across the DoW cyber ecosystem.

How BRM together with its AI Engine Advances CSRMC

BRM Alignment with the Five Phases of CSRMC

In addition to supporting CSRMC's strategic tenets, BRM aligns closely with the framework's five operational phases, providing analytical automation and mission assurance throughout the cybersecurity lifecycle.

1. Design – Select Requirements, Form Team

In the Design phase, BRM enables mission-centric architecture modeling, followed by automated threat-based risk assessment and the selection of the most effective risk mitigation. This way, it assists teams in defining cybersecurity requirements early, mapping Mission Essential Functions (MEFs) to system assets and control frameworks (e.g., NIST 800-171/172 or NIST 800-53 or any other), and establishing traceability for later testing and validation. Its ontology and knowledge graphs help ensure consistent meaning and alignment across controls, requirements, and risks from the outset.

2. Build – Implement Requirements, Gather Data

During Build, BRM integrates into engineering and development workflows to implement and validate selected controls. It gathers and structures cyber data through integrations with Blade OneReport, vulnerability scanners, and configuration management tools. This data populates BRM's analytical model, providing the foundation for real-time risk quantification and traceability of control implementation.

3. Test – Assess & Remediate

In the Test phase, BRM automatically generates attack trees, attack paths, and Test & Evaluation (T&E) reports to identify vulnerabilities and quantify their impact. It continuously recalculates residual risk as findings are remediated, providing dynamic, evidence-driven visibility into system posture. This supports agile assessment cycles and eliminates manual data stitching between vulnerabilities, mitigations, and mission risk.

4. Onboard – CSSP Reviews Risk, Validates Controls

For Onboarding, BRM provides traceable, explainable artifacts such as Security Control Traceability Matrices (SCTMs), risk matrices, and audit trails that streamline Cybersecurity Service Provider (CSSP) and Authorizing Official (AO) reviews. Its explainable AI and formal verification capabilities ensure defensible, evidence-based validation, accelerating acceptance and onboarding decisions.

5. Operate – Continuous Monitoring Enabling

In the Operate phase, BRM integrates with Security Information and Event Management (SIEM) systems, Information Security Continuous Monitoring (ISCM) platforms, and Security Orchestration, Automation, and Response (SOAR) tools, as well as CSSP capabilities to maintain continuous monitoring and authorization. It automatically ingests posture data and recalculates risks in real time, ensuring that mission readiness and cyber survivability remain aligned with changing threat and operational conditions.

AI-Driven Cyber Risk Automation

- Ontology & Knowledge Graphs: Establish shared meaning across systems, controls, vulnerabilities, and mitigations; power traceability and impact propagation.
- Rule-Based Reasoning: Encode policy and compliance as executable rules; enforce gates and control conformance.

- Model-Based Reasoning: Use formal system representations to predict risk outcomes and highlight high-value test conditions.
- Probabilistic Methods: Bayesian networks and fuzzy logic quantify uncertainty and update posture as evidence changes.
- Formal/Symbolic Methods: Provide mathematically defensible verification of policy compliance.

Analytical Backbone for CSRMC

Serving as the analytical backbone for CSRMC, BRM automates attack path generation, risk scoring, residual risk recalculation, and continuous reporting. It connects vulnerabilities, controls/mitigations, and mission functions in a unified, model-based environment for transparent decision-making.

Mission-Centric Risk Intelligence

By linking vulnerabilities and controls/mitigations directly to MEFs, BRM ensures operational resilience under adversarial conditions. Its mission-centric analytics provide leadership with insights that directly translate to mission assurance.

Continuous Authorization and Real-Time Visibility

Through dynamic data ingestion and automated recalculation, BRM maintains real-time situational awareness and continuous authorization (ATO) posture. It provides exportable reports and dashboard feeds that give stakeholders live visibility into evolving risk conditions.

Accelerating DevSecOps

BRM extension known as Blade OneReport integrates with Continuous Integration/Deployment/Delivery (CI/CD) environments to automate DevSecOps gates.

It prioritizes test conditions, validates design choices pre-release, and enforces policy-as-code through API-level integration for continuous security assurance throughout development pipelines.

Model-Based, Explainable, and Scalable

BRM's model-based reasoning and explainable AI deliver transparent, mathematically defensible insight into cyber risk. The system scales across complex enterprise portfolios while maintaining auditability and trust in every automated assessment.

Building Workforce Confidence

BRM empowers cybersecurity professionals through structured e-learning, intuitive modeling tools, and explainable analytics. It bridges technical complexity and operational clarity, enabling personnel to confidently manage cyber risk with precision.

Enterprise Efficiency and Reciprocity

BRM minimizes redundant effort by managing reusable control catalogs, baselines, and knowledgebases. Its support for reciprocity and inheritance enables cross-program evidence reuse, accelerating authorization and audit readiness.

Future-Ready and Interoperable

Built for the future, BRM's open API framework ensures ongoing adaptability. As no single product can fully automate CSRMC, BRM complements and extends existing tools to deliver end-to-end CSRMC automation and alignment across mission, system, and control architectural layers.

Seamless Integration Across the Ecosystem

BRM is architected for interoperability, providing robust APIs for integration with complementary COTS products. Key opportunities include:

- Integration with SIEM/ISCM tools to enhance continuous ATO through automated evidence ingestion and posture updates.
- Integration with SOAR/CSSP systems to operationalize incident workflows, closing the loop between detection, decision, and corrective action.

Table 1: Summary Alignment Table

CSRMC Strategic Tenet	Definition / Intent	BRM Baseline
Automation – Driving Efficiency and Scale	Automate evidence collection, risk scoring, and reporting to scale across systems.	Automates attack path generation (Identifying direct and multi-stage attacks), risk scoring, residual risk recalculation, and reporting Automatically identifies vulnerability (test) conditions per threat source and maps software conditions to vulnerability patterns for bottom-up analysis. Ingests vulnerability findings via Blade OneReport to recompute residual risk. Prioritizes portfolio-wide risks and produces T&E spreadsheets, system architecture specifications, SCTMs, and risk matrices; supports variants and calibration of likelihood and impact.
Critical Controls – Identifying and Tracking What Matters Most	Identify, track, and assess the most critical cybersecurity controls.	Auto-suggests and prioritizes controls and mitigations based on architecture, with likelihood and impact which are automatically calculated from threat means/opportunity and asset severity/criticality. Extracts MEFs from system models, propagates system-level risk to mission-level risk, and automatically recommends MEF controls to mitigate identified mission risks. Auto-generates SCTMs.
Continuous Monitoring and ATO – Real-Time Posture	Maintain real-time ATO posture via continuous situational awareness.	Validates models and automatically perform risk recalculation when change in model or threat environment is introduced or new vulnerability discovered Automatically ingests data related to identified vulnerabilities that triggers auto-recalculation of risk. Supports Cyber Security Framework (CSF)

		Maintains evolving risk registers reflecting posture changes with auto-prioritized conditions and attack scenarios.
DevSecOps – Secure, Agile Development and Deployment	Integrate cybersecurity automation into CI/CD pipelines.	Exports risk and T&E data for automated test workflows. Provides prioritized test conditions for validation. Supports variants to assess design choices before release. Integrates with CI/CD via Blade OneReport to ingest vulnerability findings and recompute residual risk. Provides API to BRM risk model through which data can be extracted to serve as DevSecOps enforcement. API is in the multiple forms: JSON, CSV
Cyber Survivability – Operating in Contested Environments	Ensure mission continuity under cyber attack or degradation.	Generates multi-stage and cascading attack paths, and variant simulations to identify survivability gaps. Supports Cyber Survivability KPPs Prioritizes mitigations for the most critical attack paths.
Training – Upskilling Personnel	Educate personnel to apply automated cyber risk management effectively.	Provides structured e-learning (Quick Start → Expert) on modeling, attack paths, mitigation, and reporting. Builds analytical skills in risk modeling and mitigation.
Enterprise Services & Inheritance – Reduce Duplication	Promote reuse of evidence and control data across systems and organizations.	Manages baselines, control catalogs, and reusable knowledgebases; Enables cloning and model reuse across projects.
Operationalization – Near Real-Time Visibility	Ensure stakeholders have near real-time visibility into risk posture.	Produces prioritized risk lists, T&E spreadsheets, SCTMs, and reports that can feed dashboards. Provides exportable reports and data feeds.

		Through provide API can easily be integrated into preferable enterprise dashboards
Reciprocity – Reuse Assessments Across Systems	Enable reuse of validated assessments to reduce redundancy.	Supports reuse within projects (baselines, catalogs, knowledgebases, variants) and export of reports for external consumption and integration.
Cybersecurity Assessments – Threat-Informed Validation	Integrate threat-informed testing to validate control effectiveness.	Auto-generates attack paths and ranks attack paths Auto-generates prioritized T&E reports identifying critical risks and mapping risks to test conditions Guides vulnerability analysis tools with risk-prioritized vulnerability types