EZRMF · WHITEPAPER · COMPLIANCE

CSRMC 5-Phase Alignment Reference

Phase-by-phase mapping of ezRMF capabilities to the DoD Cyber Survivability Risk Management Construct, from Design through Operate.

SHE BASH LLC · **EZRMF** 2026 · V4.2 DISTRIBUTION: UNCLASSIFIED

About the CSRMC

> The Cyber Survivability Risk Management Construct is the DoD's five-phase framework for risk-managed authorization of cyber-physical systems. Each phase has explicit entry and exit criteria, and each transition produces artifacts that downstream phases depend on. ezRMF is organized around those same five phases.

#	PHASE	GOAL
01	Design	Establish categorization, baselines, and tailored controls.
02	Build	Implement controls, capture evidence, link to CCIs.
03	Test	Assess controls, run STIG checks, record test results.
04	Onboard	Integrate dashboards, DevSecOps pipelines, telemetry.
05	Operate	Continuous monitoring, cATO, real-time posture.

Phase 01 — Design

GOAL: ESTABLISH CATEGORIZATION AND TAILORED BASELINE

ezRMF capabilities

- **FIPS-199 categorization wizard.** Drives Confidentiality / Integrity / Availability impact from system information types (NIST SP 800-60). Produces a categorization rationale automatically.
- **Baseline selection.** NIST SP 800-53 Rev 5 catalog with Low / Moderate / High / Privacy profiles, plus DoD overlays.
- **Tailoring workspace.** Per-control selection status (Selected, N/A, Tailored Out) with rationale fields and ODP (Organization-Defined Parameter) resolution.
- **System information types library.** Searchable NIST SP 800-60 v2r1 information-type catalog with recommended impacts.

Exit criteria

A signed-off baseline with a categorization rationale, an applicable control set, and resolved ODPs for every parameterized control. ezRMF produces this in a single SSP-shaped data structure that the Build phase reads from directly — no copy-paste between phases.

Phase 02 — Build

GOAL: IMPLEMENT, EVIDENCE, AND LINK

ezRMF capabilities

- **Body of Evidence (BoE) pipeline.** Upload PDFs, DOCX, XLSX, CKLs. Files are chunked, embedded, and indexed in pgvector for semantic recall.
- **Implementation narrative drafting.** Per-control description, responsible role, technology components, and inheritance designations.
- **Suggestion queue.** Agents propose CCI ↔ evidence links from semantic similarity; analysts approve, reject, or amend in bulk.
- **Inheritance chain.** Mark controls as inherited from a parent system; export-time resolution preserves provenance.

> ezRMF treats evidence as first-class: every artifact carries its file, anchor (page / heading / bookmark), and the CCI it satisfies. Evidence linkage is queryable both ways — control → evidence, and evidence → controls.

Phase 03 — Test

GOAL: ASSESS, RECORD, AND REMEDIATE

ezRMF capabilities

- **Combined Assess workbench.** Side-by-side internal and external assessment with status (Compliant / Non-Compliant / N/A / Not Reviewed) per AP and per CCI.
- **Assessment Procedure (AP) coaching.** Agent reads collected evidence and the AP text; recommends the specific tests still required to satisfy outstanding CCIs.
- **STIG ingest.** CKL files are parsed into the project; STIG check IDs are correlated against CCIs.
- **POA&M auto-generation.** Findings (manual or imported) become POA&M line items with NIST control mapping, milestones, and resource estimates.

Exit artifacts

An eMASS-ready Test Result Import Template (.xlsx) with row-per-AP status, test results text, and tester provenance. Generated, not authored.

Phase 04 — Onboard

GOAL: INTEGRATE WITH THE OPERATING ENVIRONMENT

ezRMF capabilities

- **MCP tool surface.** Read-only and read-write endpoints for use by CI/CD pipelines and external dashboards.
- **Audit log export.** Every change to evidence, narratives, and statuses is exposed via API for SIEM ingestion.
- **Data Requests.** Externally-shareable, time-boxed evidence requests with anonymous submission portals — enables onboarding teams to gather evidence from systems they do not yet own credentials for.

Phase 05 — Operate

GOAL: CONTINUOUS MONITORING AND CATO

ezRMF capabilities

- **Scheduled cloud discovery.** AWS inventory refreshes on cron; deltas surface in the project with a diff view.
- **Security Hub bridge.** Findings auto-create POA&M items with control mapping and severity-derived target dates.
- **Continuous telemetry.** Project posture is queryable as a live view — control coverage, evidence freshness, outstanding APs — never as a "last refreshed by the analyst" snapshot.
- **cATO readiness.** Standing reports demonstrate that posture is continuously assessed; the documentation gate is removed without removing the rigor.

Coverage matrix

CSRMC ACTIVITY	TOOLING DEPTH
System categorization (FIPS-199)	First-class wizard
Control selection / tailoring	First-class workspace
Implementation narrative authoring	First-class editor with AI drafting
Evidence capture + indexing	First-class BoE pipeline (vector search)
CCI ↔ evidence linking	First-class suggestion queue
Assessment (internal / external)	First-class workbench
STIG ingest / authoring	CKL parser, in-progress authoring view
POA&M lifecycle	First-class with Security Hub auto-create
eMASS import package	First-class one-click export (.xlsx, 3 templates)
Continuous monitoring	First-class scheduled discovery
cATO reporting	Aggregated dashboards (in scope for v5.x)

For a phase-specific deep dive or a tailored ezRMF demonstration, contact **info@shebash.io**.