RISK-BASED PRIORITIZATION

Vulnerability Management Maturity Model (VMMM v2)

Domain: Analyze
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT (30-60 seconds)

Why this matters: Remediation effort disconnected from risk reduction

What breaks without it:

- Teams patch thousands of Medium vulnerabilities while Critical exposures wait
- Cannot defend decisions to executives or regulators

What "good" looks like:

- Level 3: Documented, repeatable criteria aligned to business risk
- Level 4+: Automated scoring with continuous refinement

Who should care:

- CISOs and Security Leaders accountable for risk decisions
- VM and Exposure teams prioritizing remediation
- GRC teams validating defensible risk processes

URGENCY ASSESSMENT

(If unchecked at Level 2+, risk decisions are likely indefensible)

☑ Critical Foundation (enables meaningful VM program)
☑ Compliance Driver (required for risk-based frameworks)
☑ Risk Mitigation (stops wasting effort on wrong things)

FRAMEWORK ALIGNMENT EXAMPLES

This capability supports risk-based requirements across multiple commonly adopted security frameworks. These examples illustrate alignment, not exhaustive control coverage.

- NIST 800-53 – Supports risk assessment and remediation decision-making
- NIST CSF 2.0 – Enables vulnerability risk identification and response
- CIS Controls v8 – Aligns remediation effort to risk impact
- SO/IEC 27001 – Supports risk-driven vulnerability management

MATURITY QUICK CHECK

Where are you today?

○ Level 1: Patch by CVSS score alone, no business context
○ Level 2: Informal criteria, inconsistent application
○ Level 3: Documented criteria, defended decisions
○ Level 4: Automated scoring, metrics-driven refinement
○ Level 5: Predictive models, continuous optimization

DEPENDENCIES & BOUNDARIES

Depends on: Asset Inventory, Context, Threat Intelligence

Enables: Metrics & Reporting, SLA Management

This is NOT: A vulnerability scanner, compliance certification

NEXT STEPS

☐ Read Full Guide: Risk-Based Prioritization Guide (10 pages)
☐ Review Mapping: Framework Control Details
☐ Self-Assess: VMMM Assessment Tool