CONTEXT

Vulnerability Management Maturity Model (VMMM v2)

Domain: Prepare
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT

Why this matters:

- Organizations operate VM without meaningful context linking security to business priorities

What breaks without it:

- Marketing server patched before financial system. Dev environment same urgency as production. No business impact consideration
- Compliance audit approaches. Team realizes unclear which systems in PCI scope. Emergency discovery days before deadline

What "good" looks like:

- Level 3: Business functions, asset classification, compliance scope, context-aware prioritization
- Level 4+: Business impact ratings, threat intelligence integration, context-aware dashboards

Who should care:

- Security leadership establishing VM strategy requiring shared understanding of mission and critical assets
- Risk management teams integrating business context into security decisions and remediation priorities
- Program managers developing prioritization frameworks based on business impact and regulatory scope

URGENCY ASSESSMENT

☑ Critical Foundation (enables risk-informed prioritization)

☑ Compliance Driver (maps systems to regulatory requirements)

☑ Risk Mitigation (focuses resources on critical systems)

☐ Operational Efficiency

☑ Strategic Enhancement (aligns security with business objectives)

(If unchecked at Level 2+, organization remediates mechanically without business impact consideration)

FRAMEWORK ALIGNMENT EXAMPLES

This capability supports accountability requirements in commonly adopted security frameworks. These examples illustrate alignment, not exhaustive control coverage.

NIST 800-53: Demonstrates security categorization and risk assessment with organizational context

NIST CSF 2.0: Shows risk management informed by organizational environment and priorities

CIS v8: Provides organizational context for penetration testing scope and priorities

ISO 27001: Demonstrates threat intelligence and vulnerability management with context

MATURITY QUICK CHECK

○ Level 1: No organizational context, mechanical remediation, no business linkage

○ Level 2: Informal context, inconsistent application, individual initiative not process

○ Level 3: **Business functions, asset classification, compliance scope, context-aware decisions**

○ Level 4: Business impact ratings, threat intelligence, contextual enrichment, shared dashboards

○ Level 5: Real-time dynamic context, KPI integration, executive business-aligned dashboards

DEPENDENCIES & BOUNDARIES

Depends on: Asset Inventory, Risk-Based Prioritization, Risk Appetite Definitions

Enables: Risk-informed decisions, business-aligned security, compliance-driven remediation

This is NOT: Business impact analysis (BIA), comprehensive threat intelligence program

Related Resources: Context Guide · Framework Mapping · Self-Assessment