THIRD-PARTY VM READINESS

Vulnerability Management Maturity Model (VMMM v2)

Domain: Prepare
Maturity Tier: Enhanced

EXECUTIVE SNAPSHOT

Why this matters:

- Organizations operate VM without extending expectations to vendors, suppliers, and service providers

What breaks without it:

- Zero-day announced. No vendor security contact. Days wasted finding who handles security. No contractual SLA
- Vendor runs outdated software with Critical vulnerabilities. No leverage. Organization dependent with no recourse

What "good" looks like:

- Level 3: Documented requirements, contract security language, vendor assessment, performance tracking
- Level 4+: Systematic vendor scoring, continuous monitoring, response metrics, regular security reviews

Who should care:

- Procurement teams establishing vendor security requirements before contract signature
- Vendor risk management teams assessing supplier VM maturity and ongoing performance
- Security teams managing third-party risk requiring vendor vulnerability notifications and remediation evidence

URGENCY ASSESSMENT

☐ Critical Foundation

☑ Compliance Driver (supply chain security requirements)

☑ Risk Mitigation (prevents vendor security failures)

☐ Operational Efficiency

☑ Strategic Enhancement (enables confident vendor selection)

(Enhanced tier—improves supply chain security but not foundational requirement)

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 supply chain controls with vendor VM requirements

NIST CSF 2.0: Shows supply chain cybersecurity risk management

CIS v8: Provides service provider management with vendor security expectations

ISO 27001: Demonstrates information security in supplier relationships

MATURITY QUICK CHECK

○ Level 1: No vendor VM requirements, reactive vendor security incidents

○ Level 2: Informal vendor expectations, ad hoc security questions, inconsistent assessment

○ Level 3: **Documented requirements, contract language, vendor assessment, performance tracking**

○ Level 4: Systematic vendor scoring, continuous monitoring, response metrics, security reviews

○ Level 5: Automated risk scoring, systematic offboarding, ecosystem analysis, predictive detection

DEPENDENCIES & BOUNDARIES

Depends on: Program Governance, Policy & Standards, Risk-Based Prioritization

Enables: Supply chain security, confident vendor selection, contractual leverage

This is NOT: Vendor audit service, guarantee of vendor compliance

Related Resources: Third-Party VM Readiness Guide · Framework Mapping · Self-Assessment