POLICY & STANDARDS

Vulnerability Management Maturity Model (VMMM v2)

EXECUTIVE SNAPSHOT (30-60 seconds)

Why this matters:

- Policies exist but nobody follows them, becoming shelf-ware rather than governance

What breaks without it:

- Teams operate on unwritten rules while policy documents collect dust
- Auditors find disconnect between documented policy and actual practice

What "good" looks like:

- Level 3: Documented policies enforced through workflows and accountability
- Level 4+: Automated enforcement integrated with tools and continuous updates

Who should care:

- Security leadership establishing VM governance framework
- Policy teams creating enforceable requirements
- GRC teams demonstrating systematic governance

URGENCY ASSESSMENT

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

- ☑ Critical Foundation (enables accountability and governance)
- ☑ Compliance Driver (frameworks require documented policies)
- ☑ Operational Efficiency (clear expectations reduce confusion)

FRAMEWORK ALIGNMENT EXAMPLES

NIST 800-53: Establishes policy framework and program management foundation

NIST CSF 2.0: Demonstrates governance through documented expectations

CIS v8: Defines VM process requirements and ownership

ISO 27001: Shows management commitment through formal policies

MATURITY QUICK CHECK

Where are you today?

- ○ Level 1: No formal policies, ad hoc operations
- ○ Level 2: Informal guidelines, inconsistent enforcement
- ○ Level 3: **Documented, approved, communicated**
- ○ Level 4: Automated compliance checking, regular updates
- ○ Level 5: Continuous evolution, automated enforcement

DEPENDENCIES & BOUNDARIES

Depends on: Context, Program Governance, Stakeholder Engagement

Enables: All capabilities (provides governance framework)

This is NOT: A policy template, compliance guarantee

NEXT STEPS

☐ Read Full Guide: Policy & Standards Guide (10 pages)

☐ Review Mapping: Framework Control Details

☐ Self-Assess: VMMM Assessment Tool