PROGRAM GOVERNANCE

Vulnerability Management Maturity Model (VMMM v2)

Domain: Prepare
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT (30-60 seconds)

Why this matters:

- VM operates without authority, escalation paths, or systematic resource allocation

What breaks without it:

- Critical vulnerabilities remain unpatched with no path to executive action
- Resource requests disappear without prioritization, conflicts go unresolved

What "good" looks like:

- Level 3: Charter, steering committee, defined escalation, executive reporting
- Level 4+: Strategic governance with risk-informed resource allocation

Who should care:

- CISOs and security leadership establishing oversight structures
- Executive and board members providing program visibility and resources
- Program managers navigating organizational decision-making

URGENCY ASSESSMENT

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

☑ Critical Foundation (enables organizational legitimacy)
☑ Compliance Driver (frameworks require oversight)
☑ Operational Efficiency (enables systematic decision-making)

FRAMEWORK ALIGNMENT EXAMPLES

NIST 800-53: Establishes program management and oversight structure

NIST CSF 2.0: Demonstrates organizational context and oversight mechanisms

CIS v8: Provides organizational infrastructure for systematic VM

ISO 27001: Shows management commitment through formal accountability

MATURITY QUICK CHECK

Where are you today?

○ Level 1: No formal structure, VM operates independently
○ Level 2: Basic oversight, periodic meetings, informal escalation
○ Level 3: **Charter, steering committee, defined escalation**
○ Level 4: Strategic governance, risk-informed decisions
○ Level 5: Continuous improvement, measured effectiveness

DEPENDENCIES & BOUNDARIES

Depends on: Policy & Standards, Roles & Responsibilities, Metrics & Reporting

Enables: All capabilities (provides authority and resources)

This is NOT: An org chart, committee attendance requirement

NEXT STEPS

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