ROLES & RESPONSIBILITIES

Vulnerability Management Maturity Model (VMMM v2)

Domain: Prepare
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT

Why this matters:

- Everyone assumes someone else handles VM activities—nobody owns the outcome

What breaks without it:

- Finger-pointing when vulnerabilities unaddressed—each team claims another responsible
- Organizational gaps emerge—scanning, remediation, validation all inconsistent

What "good" looks like:

- Level 3: RACI matrix, role descriptions with VM responsibilities, decision authority boundaries
- Level 4+: Embedded in workflows with role-specific training and systematic optimization

Who should care:

- Security leadership defining accountability frameworks preventing organizational gaps
- Program managers clarifying who performs scanning, remediation, validation, escalation
- Operational teams understanding their specific VM responsibilities and handoff points

URGENCY ASSESSMENT

- ☑ Critical Foundation (eliminates finger-pointing and gaps)
- ☑ Compliance Driver (frameworks require accountability)
- ☑ Operational Efficiency (enables coordinated execution)

FRAMEWORK ALIGNMENT EXAMPLES

NIST 800-53: Documents VM responsibilities in position descriptions

NIST CSF 2.0: Demonstrates organizational context with defined roles

CIS v8: Defines who performs vulnerability management activities

ISO 27001: Shows segregation of duties with documented accountability

MATURITY QUICK CHECK

- ○ Level 1: No documented roles, ad hoc activities, unclear accountability
- ○ Level 2: Informal understanding, tribal knowledge, conflicting views
- ○ Level 3: **RACI matrix, role descriptions, decision authority boundaries**
- ○ Level 4: Embedded in workflows, periodic review, role-specific training
- ○ Level 5: Continuous optimization, measured effectiveness

DEPENDENCIES & BOUNDARIES

Depends on: Program Governance, Policy & Standards, Asset Inventory

Enables: All capabilities (provides accountability framework)

This is NOT: An org chart, specific role assignments for all organizations

Related Resources: Roles & Responsibilities Guide · Framework Mapping · Self-Assessment