Roles & Responsibilities

Capability Alignment Guide

Model: VMMM v2.0.0
Domain: Prepare
Maturity Tier: Foundational

Purpose:

Roles & Responsibilities establishes clear accountability and ownership for vulnerability management activities across the organization, documenting who performs scanning, remediation, validation, and escalation with defined decision authority boundaries preventing organizational gaps and finger-pointing.

This document is interpretive guidance. Normative definitions of the Roles & Responsibilities capability and maturity levels are defined in the VMMM v2 Canon.

Executive Summary

Organizations operate vulnerability management without clear accountability. Everyone assumes someone else handles VM activities. Development teams believe infrastructure handles patching. Infrastructure teams assume applications patch themselves. Security team scans and reports but lacks authority to enforce remediation. When critical vulnerabilities remain unpatched for months, finger-pointing begins—each team claims another team responsible. Nobody owns the outcome.

Roles & Responsibilities capability documents who does what across VM lifecycle. RACI matrix or equivalent defines who scans systems, who approves scan schedules, who receives scan results, who is notified of critical findings. Role descriptions include VM-specific responsibilities: system owners remediate vulnerabilities within SLA timeframes, security team validates remediation effectiveness, CISO approves risk acceptance decisions exceeding tolerance thresholds. Decision authority boundaries documented: security team cannot approve exceptions without system owner input, system owners cannot delay Critical patches beyond 30 days without CISO approval, third parties must coordinate patching with internal teams.

Mature roles operate strategically. Post-incident reviews identify responsibility gaps and drive role updates. Organizational changes trigger systematic reassessment. Role effectiveness measured through accountability metrics: percentage of vulnerabilities remediated by designated owners within SLA, escalation timeliness, validation completion rates. When accountability is clear and enforced, VM transforms from blame game into coordinated program.

This guide explains why role clarity matters, what accountability maturity looks like, and how to use the detailed mapping document for compliance and organizational effectiveness.

This document is interpretive guidance. Normative definitions of the Roles & Responsibilities capability and maturity levels are defined in the VMMM v2 Canon.

Why This Capability Exists

Security team scans systems and generates vulnerability reports. Reports distributed to IT teams. Months pass. Critical vulnerabilities remain unpatched. Security asks infrastructure why not remediated. Infrastructure says applications team responsible. Applications team says those are infrastructure vulnerabilities. Development says not their systems. Nobody owns the outcome. This is organizational accountability failure, not technical failure.

Without documented roles, systematic gaps emerge. Scanning performed inconsistently because unclear who manages scanners for which systems. Remediation delayed because system owners don't recognize patching as their responsibility—they believe security team handles it. Validation skipped because nobody designated to confirm fixes effective. When validation does occur, unclear who has authority to reject inadequate fixes. Escalation paths broken because unclear who has decision-making authority to elevate unresolved vulnerabilities or approve exceptions.

New employees join and nobody explains their VM responsibilities. Contractors work on systems without understanding their vulnerability management obligations. Third-party vendors assume internal teams handle all security activities. Cloud service providers believe customers responsible for patching. Each party points to others creating accountability vacuum where critical vulnerabilities persist indefinitely.

Roles & Responsibilities capability establishes organizational accountability framework. RACI matrix or equivalent documents: who scans which systems (Responsible), who approves scan schedules and configurations (Accountable), who provides input on scan timing or scope (Consulted), who receives scan results and notifications (Informed). Role descriptions updated to include VM-specific responsibilities aligned to documented matrix. Decision authority boundaries explicitly defined preventing ambiguity about who can approve exceptions, escalate issues, or accept residual risk.

Segregation of duties implemented preventing conflicts of interest: individuals performing remediation cannot validate their own work, risk acceptance requires approval from authority independent of remediation team, scanning teams separated from system administration preventing scope gaming. At highest maturity, roles evolve through continuous feedback: post-incident reviews identify gaps, organizational transformations trigger reassessment, effectiveness metrics demonstrate accountability framework working.

Before and After Comparison

WITHOUT MATURE ROLES & RESPONSIBILITIES:

- Critical vulnerability identified in production system. Security sends report to multiple teams. Nobody remediates. Each team claims another responsible. Vulnerability remains unpatched
- Contractor rotates off project. New contractor joins. Nobody explains VM responsibilities. Contractor makes changes without patching. Systems become more vulnerable
- Remediation claimed complete. Security rescans. Vulnerability still present. Unclear who validates fixes. No authority to reject inadequate remediation
- Business unit requests exception to delay patching. Unclear who has authority to approve. Exception sits unanswered for weeks. Risk unmanaged

WITH MATURE ROLES & RESPONSIBILITIES:

- Critical vulnerability detected. RACI matrix consulted. System owner identified: Database Team. Automated workflow assigns remediation ticket to Database Team lead. Owner accountability clear. Remediation completed within SLA

- New contractor onboards. HR provides role-specific VM training materials. Contractor understands: must coordinate patching through change control, required to maintain systems at approved patch levels, escalation path if blocked. Responsibilities clear from day one
- Remediation claimed complete. Validation Team (separate from remediation) performs independent verification. Vulnerability persists. Validation Team has documented authority to reject remediation and reassign ticket. Clear accountability for quality
- Exception request submitted. Decision authority matrix shows: exceptions exceeding 30-day Critical tolerance require CISO approval. Request routed automatically. CISO reviews with documented criteria. Decision made within 48 hours. Authority clear

Maturity is about replacing organizational ambiguity with documented accountability. Defining who performs each activity, establishing decision authority boundaries, implementing segregation of duties, continuously improving through feedback.

Maturity Progression

The maturity ladder shows how accountability capability evolves from undefined ownership to continuously optimized role framework with measurable effectiveness.

LEVEL 5 STRATEGIC	**Continuous role optimization, measured effectiveness, incident-driven improvements, systematic learning** Investment for organizations requiring demonstrable accountability framework optimization
LEVEL 4 ENHANCED	**Embedded in workflows, periodic review, role-specific training, systematic overlap resolution**
LEVEL 3 DOCUMENTED	**RACI matrix, role descriptions with VM responsibilities, decision authority boundaries, segregation of duties** ← *Baseline for organizational accountability* *Eliminates finger-pointing and gaps*
LEVEL 2 REACTIVE	**Informal understanding, tribal knowledge, conflicting interpretations, no documentation**
LEVEL 1 AD HOC	**No documented roles, activities performed ad hoc by whoever notices, unclear accountability**

What Changes at Each Level

Level 1 to 2: Organization begins informal conversations about who handles what (security team does VM) but no documentation or consistent understanding.

Level 2 to 3: Organization documents responsibility matrix (RACI), updates role descriptions with VM responsibilities, defines decision authority boundaries, implements segregation of duties.

Level 3 to 4: Roles embedded in operational workflows with automated task routing, periodic review process established, onboarding includes role-specific VM training, overlaps systematically resolved.

Level 4 to 5: Continuous optimization through post-incident reviews identifying gaps, organizational transformation triggering reassessment, role effectiveness measured with accountability metrics, systematic learning.

Framework Alignment at a Glance

Roles & Responsibilities capability provides the accountability framework required by frameworks for organizational security activities and segregation of duties.

NIST 800-53 (Personnel Security)

Core capability for PS-2 (Position Risk Designation) documenting VM responsibilities in position descriptions, CP-2 (Contingency Plan) showing contingency roles, AT-2 (Literacy Training) enabling role-based training.

Evidence: Position descriptions with VM sections, contingency role documentation, role-based training materials

NIST CSF 2.0 (Govern)

Demonstrates GV.OC (Organizational Context) with established cybersecurity risk management responsibilities and GV.RR (Roles, Responsibilities, Authorities) for supply chain including third-party VM obligations.

Evidence: Organizational context documentation, responsibility assignments, supply chain role definitions

CIS Controls v8 (Control 7)

Supports Control 7.1 (Establish VM Process) by defining who performs vulnerability management activities enabling systematic process execution with clear ownership.

Evidence: VM process documentation including role assignments for scanning, remediation, validation

ISO 27001:2022 (Organizational Controls)

Core demonstration of A.5.3 (Segregation of Duties) showing conflicting duties separated and A.6.8 (Information Security Event Management) documenting event handling roles including vulnerability-related events.

Evidence: Segregation documentation, event management role assignments, responsibility matrix

This document is interpretive guidance. Normative definitions of the Roles & Responsibilities capability and maturity levels are defined in the VMMM v2 Canon.

How to Use the Mapping Document

This guide explains why role clarity matters and what accountability maturity looks like. The detailed mapping document contains framework control mappings and implementation guidance.

Reader Navigation

Security Leadership: Read entire guide to understand accountability framework design, then use mapping for documentation requirements.

Program Managers: Focus on Why This Exists and Before/After to understand eliminating organizational gaps through clear ownership.

Operational Teams: Read Maturity Progression to understand specific responsibilities and handoff points to other functions.

GRC Teams: Read Framework Alignment overview, then use mapping to demonstrate organizational accountability to auditors.

Use Case Scenarios

Scenario 1: Accountability Framework Design

- Read: Why This Exists + Maturity Snapshot
- Use: Create RACI matrix defining who performs each VM activity
- Then: Use mapping document for decision authority examples

Scenario 2: Gap Identification

- Read: Full guide for accountability patterns
- Use: Analyze current responsibilities identifying unclear ownership
- Then: Use mapping for segregation of duties requirements

Scenario 3: Third-Party Management

- Read: Boundaries section for vendor responsibilities
- Use: Define vendor and contractor VM obligations explicitly
- Then: Use mapping for contractual requirement examples

Scenario 4: Audit Preparation

- Read: Framework Alignment + Boundaries
- Use: Demonstrate organizational accountability to auditors
- Then: Use mapping to compile accountability evidence package

Common Misconceptions

MISCONCEPTION: "Having job titles means we have defined responsibilities"

REALITY: A team called Vulnerability Management Team does not automatically clarify who scans which systems, who validates remediation, or who approves exceptions. Mature capability requires explicit documentation of activities each role performs, decision authority boundaries, and handoff points between roles. Job titles create organizational structure but not accountability.

MISCONCEPTION: "RACI matrix alone satisfies this capability"

REALITY: RACI matrix is foundation but insufficient alone. Mature capability requires: role descriptions updated with VM responsibilities, decision authority boundaries documented, segregation of duties implemented, onboarding materials incorporating role-specific training. RACI shows relationships but not implementation. Documentation must be comprehensive and actionable.

MISCONCEPTION: "Roles should be identical across all organizations"

REALITY: Role definitions must reflect actual organizational structure. Documenting responsibilities for Security Operations Center when organization lacks SOC creates confusion not clarity. Small organizations may combine roles that larger enterprises separate. Role framework must match organizational capacity, structure, and maturity. Template adoption without customization fails.

Boundaries and Non-Claims

What This Guide Is NOT:

- An organizational chart showing reporting relationships (roles focus on activities not hierarchy)
- A determination of specific role assignments appropriate for any organization (must reflect structure)
- A guarantee that documented roles eliminate all VM gaps (execution still required)
- A replacement for Program Governance capability (roles define who does what while governance provides authority)

What This Guide Provides:

- Guidance on accountability maturity characteristics and role framework development
- Framework alignment for organizational accountability requirements
- Examples of evidence demonstrating clear ownership and segregation
- Pathway to detailed mapping document for implementation

Critical Dependencies:

Roles & Responsibilities depends on Program Governance (provides oversight authority enforcing accountability), Policy & Standards (defines requirements roles must fulfill), and Asset Inventory & Classification (determines which assets each role manages). Without these, roles lack authority to enforce responsibilities, unclear what activities roles should perform, and ambiguous which systems fall under each role's accountability.

Third-party and vendor responsibilities must be explicitly documented. Assuming contractors understand VM obligations without documentation creates gaps when external personnel rotate. Small organizations may need documented compensating controls when single individual must perform conflicting activities due to limited capacity.

This document is interpretive guidance. Normative definitions of the Roles & Responsibilities capability and maturity levels are defined in the VMMM v2 Canon.

Next Steps

Assess Your Current State

- Identify whether organization has documented responsibility matrix for VM activities
- Evaluate whether role descriptions include VM-specific responsibilities or rely on tribal knowledge

Identify Your Target State

- Level 3 provides baseline accountability framework eliminating finger-pointing and gaps
- Consider Level 4 if you need embedded workflows and systematic role optimization

Plan Your Journey

- Document responsibility matrix (RACI or equivalent) defining who performs each VM activity
- Update role descriptions to include VM-specific responsibilities aligned to matrix
- Define decision authority boundaries and implement segregation of duties

Resources Available

- VMMM self-assessment tool for capability evaluation
- Detailed mapping documents for all 40 capabilities
- RACI matrix templates and role description examples

Questions or Feedback?
Contact ZenzizenSec for additional information or clarification.