

# Policy & Standards

## Capability Alignment Guide

**Model:** VMMM v2.0.0

**Domain:** Prepare

**Maturity Tier:** Foundational

**Purpose:**

*Policy & Standards capability ensures vulnerability management policies drive actual behavior rather than becoming shelf-ware, establishing clear expectations for remediation timelines, responsibilities, and risk management.*

© 2026 ZenzizenSec Inc.

## Executive Summary

Many organizations have vulnerability management policies that no one follows. Documents sit in policy repositories collecting dust while teams operate according to unwritten rules and individual judgment. When auditors request policies, teams scramble to find outdated documents that bear no resemblance to actual practice.

Policy & Standards capability transforms this by establishing enforceable policies that define who owns what, when remediation must occur, what risk thresholds are acceptable, and how exceptions get approved. These policies integrate with actual workflows through automation, enforcement mechanisms, and regular updates that keep pace with organizational change.

Mature Policy & Standards provides the governance foundation for vulnerability management programs. Teams understand their responsibilities, stakeholders know what to expect, auditors can verify compliance with documented requirements, and the organization can demonstrate that security activities align with risk tolerance and regulatory obligations.

This guide explains why formal policies matter, what maturity looks like at different levels, and how to use the detailed mapping document for framework alignment and audit preparation.

## Why This Capability Exists

Policies fail when they describe an ideal state that nobody implements. A document stating "all Critical vulnerabilities will be remediated within 7 days" means nothing when the organization routinely misses that SLA with no consequences. Teams learn to ignore policies when enforcement is nonexistent and updates never happen.

Without formal policies, vulnerability management operates on tribal knowledge. New team members struggle to understand expectations. Decisions depend on who you ask rather than documented standards. Business stakeholders have no visibility into remediation commitments. Auditors find no evidence of systematic governance.

The challenge is making policies enforceable. This requires integration with actual systems, automated checks that flag violations, clear accountability when standards are not met, and regular updates that reflect organizational reality. Policies must evolve as threats change, regulations update, and business priorities shift.

### Before and After Comparison

#### **WITHOUT MATURE POLICY & STANDARDS:**

- Policy document exists but nobody knows where to find it
- Teams ask: "What's our SLA for Critical vulnerabilities?" Answer: "Depends who you ask"
- Auditors request policy evidence. Team spends days updating outdated document to match current practice

#### **WITH MATURE POLICY & STANDARDS:**

- Policy is accessible, current, and referenced in daily workflows
- Teams know: "Critical = 15 days, High = 30 days, documented exceptions process if needed"
- Auditors request policy evidence. Team provides current, enforced document with compliance metrics

Maturity is about policies that drive behavior. Enforceable standards embedded in processes, automated compliance checking, regular updates reflecting reality, and governance ensuring accountability.

## Maturity Progression

The maturity ladder shows how policy capability evolves from nonexistent to continuously improving governance framework.

<b>LEVEL 5</b> STRATEGIC	<b>Continuous evolution through feedback loops, automated enforcement</b> ROI diminishing returns beyond well-governed programs
<b>LEVEL 4</b> ENHANCED	<b>Automated compliance checking, embedded in CI/CD, regular policy updates</b>
<b>LEVEL 3</b> DOCUMENTED	<b>Formal policies approved and communicated, standards with SLAs</b> ← <i>Baseline for governance and audit requirements</i> <i>Foundation for compliance frameworks</i>
<b>LEVEL 2</b> REACTIVE	<b>Informal guidelines exist but not enforced, inconsistent application</b>
<b>LEVEL 1</b> AD HOC	<b>No formal policies, teams operate independently</b>

### What Changes at Each Level

**Level 1 to 2:** Teams develop informal guidelines and best practices, but these remain undocumented and inconsistently applied.

**Level 2 to 3:** Organization formalizes policies with approval, documentation, and communication. This establishes baseline governance and audit defensibility.

**Level 3 to 4:** Automation enforces policies through CI/CD integration, compliance checking, and exception tracking. Policies update regularly to stay current.

**Level 4 to 5:** Continuous feedback loops adapt policies based on metrics, incidents, and threat evolution. Investment returns diminish unless operating complex enterprise environments.

## Framework Alignment at a Glance

Policy & Standards capability provides the governance foundation required by security frameworks, demonstrating systematic approach to vulnerability management through documented requirements and accountability.

### NIST 800-53 (Planning, Program Management)

Implements PL-1 (Policy and Procedures) and PM-1 (Information Security Program) through documented VM policies. Supports PM-9 (Risk Management Strategy) by defining risk tolerance and remediation requirements.

**Evidence:** Approved policy documents, standards with SLAs, exception tracking, enforcement metrics

### NIST CSF 2.0 (Govern)

Supports GV.PO (Policy Establishment) and GV.RR (Roles, Responsibilities, and Authorities) by documenting VM expectations and accountability. Demonstrates systematic governance approach.

**Evidence:** Policy approval records, stakeholder acknowledgment, compliance reporting

### CIS Controls v8 (Control 7)

Establishes VM process foundation for Control 7.1 (Establish and Maintain VM Process). Policies define remediation timelines, responsibilities, and risk-based prioritization criteria.

**Evidence:** VM policy document, remediation SLAs, process documentation

### ISO 27001:2022 (Leadership, Planning)

Demonstrates management commitment (A.5.1) and information security policies (A.5.2) through documented VM governance. Supports A.5.10 (Acceptable Use) by defining risk tolerance.

**Evidence:** Policy approval by leadership, documented roles and responsibilities, policy update logs

# How to Use the Mapping Document

This guide provides the overview. The detailed mapping document (MD file) contains framework control mappings and evidence requirements.

## Reader Navigation

**Executives:** Read Executive Summary and Maturity Snapshot to understand governance requirements. Skip detailed mappings unless specific framework questions arise.

**Policy Teams:** Read entire guide, then use mapping document's Evidence Progression to identify required policy elements and approval processes.

**GRC Teams:** Read Framework Alignment overview here, then reference mapping document for detailed control mappings and audit evidence requirements.

**Security Engineering:** Review Maturity Progression to understand automation opportunities at Levels 4-5, then use mapping document for implementation guidance.

## Use Case Scenarios

### Scenario 1: Policy Creation

- Read: Why This Exists + Maturity Snapshot
- Use: Understand policy requirements and stakeholder expectations
- Then: Use mapping document for framework-aligned policy template

### Scenario 2: Compliance Assessment

- Read: Framework Alignment + Boundaries
- Use: Map existing policies to framework requirements
- Then: Use mapping document to identify evidence gaps

### Scenario 3: Process Automation

- Read: Maturity Progression focusing on Levels 3-4 transition
- Use: Identify automation opportunities (CI/CD integration, compliance checking)
- Then: Use mapping document for implementation patterns

### Scenario 4: Audit Preparation

- Read: Full guide for context
- Use: Understand what auditors expect to see
- Then: Use mapping document to compile evidence package

## Common Misconceptions

**MISCONCEPTION:** "Having a policy document means we have mature Policy & Standards capability"

**REALITY:** Maturity requires policies that people follow. Document existence doesn't equal enforcement, automation, or regular updates.

**MISCONCEPTION:** "Policies can't change once approved"

**REALITY:** Mature policies evolve based on threat changes, business needs, and operational feedback. Static policies become outdated shelf-ware.

**MISCONCEPTION:** "This mapping means our policies satisfy all framework requirements"

**REALITY:** Mapping shows how capability supports frameworks. Assessors determine whether your specific implementation satisfies requirements.

## Boundaries and Non-Claims

### What This Guide Is NOT:

- A complete VM policy template ready for adoption
- A guarantee of compliance with any regulation or framework
- A substitute for legal review or executive approval of policies
- A claim that documented policies equal organizational compliance

### What This Guide Provides:

- Guidance on policy maturity characteristics
- Framework alignment reference for governance requirements
- Examples of evidence demonstrating policy effectiveness
- Pathway to detailed mapping document for implementation

### Important Context:

Policy & Standards establishes governance foundation but depends on other capabilities. Context defines what policies should address. Risk-Based Prioritization provides criteria for remediation timelines. Asset Inventory determines scope. Program Governance ensures policy updates and enforcement.

Policies must reflect organizational reality. Generic templates fail when they ignore your environment, risk tolerance, regulatory requirements, and operational constraints. Use this guide to understand characteristics of effective policies, then adapt to your context.



## Next Steps

### Assess Your Current State

- Review existing VM policies (if any) against maturity progression
- Identify gaps: documentation, enforcement, automation, currency

### Identify Your Target State

- Most organizations should target Level 3 for baseline governance
- Consider Level 4 if you need automation or operate at scale

### Plan Your Journey

- Use mapping document to identify required policy elements
- Draft or update policies with stakeholder input
- Establish approval process and communication plan

### Resources Available

- VMMM self-assessment tool for capability evaluation
- Detailed mapping documents for all 40 capabilities
- Policy templates and implementation guidance

### Questions or Feedback?

Contact ZenzizenSec for additional information or clarification.