VMMM Companion Guide – VMMM Usage and Domain Descriptions

Introduction

This guide provides detailed domain descriptions to support consistent interpretation and use of the Vulnerability Management Maturity Model (VMMM). While the VMMM defines levels of maturity across various capability areas, this companion document focuses on what each domain represents, why it matters, and what is intended to be assessed within each one.

Each entry includes a two-paragraph explanation that outlines:

- The purpose and scope of the domain within a vulnerability management program
- The types of behaviors, processes, decisions, or outcomes that indicate maturity in this area

The goal is to remove ambiguity, especially for organizations conducting internal maturity assessments or coordinating efforts across teams, regions, or business units. Many domain names can be interpreted differently depending on context—this guide ensures that all users of the model are working from a shared understanding of what each domain is intended to measure.

You can use this guide to:

- Align stakeholders during assessment and scoring activities
- Train assessors, auditors, and program leads on what to look for in each area
- Guide documentation, tooling, and governance decisions to strengthen program capabilities
- Support internal communications by clearly describing each area's role in a mature VM program

This guide complements the model's maturity level definitions, practical examples, and use cases. Together, they provide a full-spectrum reference for organizations seeking to benchmark, plan, and improve vulnerability management in a structured and risk-aware way.

Understanding Foundational, Enhanced, and Strategic Domain Classifications

To help organizations prioritize their improvement efforts and avoid becoming overwhelmed, the VMMM assigns each domain to one of three strategic classifications: Foundational, Enhanced, or Strategic. These labels are not maturity levels themselves—they are groupings used to indicate the relative importance and sequencing of capabilities during program development.

What the Classifications Mean

- Foundational Domains

  These are the building blocks of a functioning vulnerability management program. They represent core capabilities that must be in place before more advanced activities can be effective. Foundational domains focus on basic visibility, governance, and essential processes such as asset inventory, vulnerability scanning, and policy enforcement. Organizations should prioritize maturing these areas first, even if only to an intermediate level, before investing heavily elsewhere.

- Enhanced Domains

  Once foundational practices are reasonably established, enhanced domains help expand and scale the program. These domains introduce cross-functional integration, risk-informed prioritization, more formal governance, and more consistent processes. They often rely on foundational inputs and provide the structures needed to support efficiency and effectiveness at scale.

- Strategic Domains

  Strategic domains extend the value of vulnerability management by embedding it into broader business operations, risk management, and continuous improvement. These capabilities often require foundational and enhanced domains to be stable. Strategic domains emphasize optimization, predictive decision-making, cross-enterprise collaboration, and measurable impact on organizational risk posture.

How to Use These Classifications

- Prioritization and Roadmapping:

  Focus first on foundational domains, aiming for moderate maturity (typically Level 3) before investing in enhanced or strategic areas.

- Phased Assessments or Pilots:

  Use the classifications to divide the model into manageable workstreams. Foundational domains can be assessed first to build confidence and establish a baseline.

- Clear Communication:

These groupings help teams explain where to focus, why certain improvements are more urgent, and how to build maturity progressively without overextending.

This classification model supports realistic, risk-aligned program growth, without implying that all domains must reach the highest maturity levels before broader progress can occur. Instead, it offers a pragmatic path to evolve a VM program over time.

PREPARE

Context

The Context domain defines how well an organization understands the internal and external factors influencing its vulnerability management decisions. This includes awareness of business priorities, regulatory pressures, threat landscape, and industry-specific risks. A solid contextual foundation ensures that risk is evaluated relative to the organization's mission, risk appetite, and operational landscape.

This domain measures the extent to which contextual awareness informs vulnerability prioritization, resource allocation, and policy alignment. It ensures that vulnerability management is not operating in a vacuum but rather is responsive to dynamic business and threat conditions.

Crisis Response & Zero-Day Readiness

This domain evaluates the organization's preparedness to respond to unplanned, high-impact vulnerability events, such as zero-day threats or widespread exploitation campaigns. It includes having response playbooks, designated response roles, escalation paths, and cross-functional coordination mechanisms in place.

The intent is to assess whether the organization can rapidly identify, assess, and respond to emerging threats before damage occurs. Higher maturity is marked by routine simulations, measurable response performance, and integration with business continuity and communications processes.

Policy & Standards

The Policy & Standards domain focuses on the formalization and enforcement of expectations related to vulnerability management. This includes patch timelines, remediation responsibilities, exception handling criteria, and minimum coverage levels. Effective policies should be aligned with business objectives and regulatory obligations.

This domain measures whether policies are defined, reviewed, communicated, and integrated into technical and operational workflows. Higher maturity involves automated policy enforcement and policy evolution informed by risk data and program performance.

Program Governance

This domain assesses the presence and effectiveness of governance structures for vulnerability management. It looks at whether governance bodies exist, whether they receive meaningful data, and whether decisions and oversight occur at appropriate levels of the organization.

The goal is to ensure that vulnerability risk is managed strategically, not just tactically. Mature governance involves executive sponsorship, cross-functional participation, formal review cycles, and escalation paths for unresolved or systemic issues.

Risk Appetite & Tolerance Definitions

This domain reflects whether the organization has clearly defined its risk appetite and tolerance specific to vulnerabilities. These definitions guide remediation decisions, exception approvals, and prioritization logic, especially when not all issues can be addressed simultaneously.

It measures whether risk thresholds are documented, communicated, and applied consistently across teams. Mature organizations tie tolerance definitions to asset criticality, business impact, and evolving threat conditions, ensuring decisions align with enterprise risk posture.

Security Ecosystem Integration

This domain assesses how well vulnerability management is integrated with other security and IT systems—such as asset inventories, change management, threat detection, ticketing platforms, and logging systems. Integration supports accurate scoping, faster response, and aligned remediation.

The intent is to measure whether vulnerability management operates as a connected function within the broader security ecosystem or remains siloed. Mature organizations enable bi-directional data flows and contextual enrichment through integration.

VM Roles & Responsibilities

This domain evaluates whether roles and responsibilities for all parts of the vulnerability management lifecycle are clearly defined, documented, assigned, and enforced. This includes responsibility for discovery, triage, remediation, exception handling, and reporting.

The goal is to measure clarity and accountability. Mature programs ensure role ownership is embedded in workflows, monitored via metrics, and reinforced through governance and team performance reviews.

Crisis Communication Readiness

This domain evaluates the organization's ability to communicate effectively during a high-impact or zero-day vulnerability event. It includes predefined messaging templates, communication plans, and stakeholder coordination processes for both internal and external audiences.

The objective is to ensure messaging is timely, consistent, and aligned with organizational policy and reputational considerations. Higher maturity involves cross-functional simulation exercises, real-time notification mechanisms, and feedback loops for continual refinement.

IDENTIFY

Ephemeral & Short-Lived Asset Discovery

This domain assesses the organization's ability to identify transient, short-lived, or dynamically generated assets that may only exist briefly—such as containers, serverless functions, or auto-scaling cloud instances. Traditional asset discovery methods often miss these, leaving blind spots in coverage.

The intent is to evaluate how well ephemeral assets are detected, cataloged, and included in vulnerability assessments. Mature organizations implement automated discovery tied to orchestration platforms, deployment pipelines, and real-time telemetry to maintain visibility across fast-moving environments.

External Vulnerability Intelligence Ingestion

This domain focuses on how effectively an organization gathers and processes vulnerability information from external sources, including threat intelligence feeds, vendor advisories, and national vulnerability databases. Staying ahead of emerging threats depends on timely and relevant intelligence.

The goal is to assess whether external intelligence is integrated into the vulnerability management lifecycle, informing risk decisions and prioritization. Higher maturity involves automated ingestion, enrichment with internal asset context, and actionable workflows driven by intelligence correlations.

Manual Discovery & Analyst Testing

This domain evaluates the organization's use of human expertise to validate, investigate, or discover vulnerabilities that automated tools may miss. While automation is critical for scale, manual testing plays an essential role in uncovering complex misconfigurations, chained vulnerabilities, or business logic flaws.

The goal is to assess whether manual analysis is structured, repeatable, and integrated into the VM process. Mature organizations use analyst input to enhance detection logic, validate scan results, and uncover environment-specific exposures.

Shadow IT & Rogue Asset Detection

This domain focuses on how well an organization can identify assets that have been deployed without proper authorization or outside of approved IT governance. These systems often operate without visibility, exposing the organization to unmanaged risk.

The objective is to ensure unauthorized or rogue assets are regularly identified, investigated, and addressed. Mature organizations use internal telemetry, external attack surface monitoring, and integration with procurement and security platforms to detect and manage these risks.

Third-Party Asset Discovery

This domain evaluates whether the organization can discover and track assets managed or hosted by third parties, such as vendors, contractors, or cloud service providers. These assets may still impact the organization's risk posture despite being externally owned.

The goal is to ensure that third-party systems are properly inventoried, reviewed, and included in vulnerability assessments. At higher maturity, organizations validate third-party coverage through technical means and enforce security expectations through contracts and risk programs.

Asset Inventory & Classification

This domain measures the organization's ability to maintain a complete, accurate, and up-to-date inventory of its assets—including servers, endpoints, applications, databases, and cloud services. Classification refers to grouping assets by criticality, ownership, business function, and sensitivity.

A strong asset inventory forms the foundation for effective vulnerability management. This domain evaluates whether the inventory is actively maintained, enriched with contextual metadata, and used to scope scanning, prioritize remediation, and track accountability.

ANALYZE

Business Impact Modelling

This domain assesses how well the organization evaluates the potential business consequences of vulnerabilities. It considers how vulnerabilities could affect critical services, customer trust, compliance obligations, revenue streams, or operational continuity. Impact modeling moves risk discussions beyond technical severity to include financial and strategic outcomes.

The goal is to measure whether business impact is calculated in a structured, repeatable way, and whether it meaningfully informs remediation prioritization and decision-making. Mature programs use input from business owners, service maps, and critical asset designations to quantify impact and guide vulnerability response.

Exploitability Assessment

This domain evaluates the organization's ability to determine the likelihood that a vulnerability will be exploited in the wild. It incorporates public exploit availability, threat intelligence, proof-of-concept code, scanning activity, and attacker behavior. Simply knowing a vulnerability exists is not enough—understanding exploitability is key to risk-based prioritization.

The goal is to ensure that exploitability is considered alongside severity and asset value when deciding which vulnerabilities to address first. Mature organizations use curated exploit feeds, predictive analytics (e.g., EPSS), and attacker tactics to dynamically influence prioritization and defensive posture.

False Positive & Suppression Validation

This domain focuses on how the organization handles false positives and the suppression of findings in its vulnerability data. It evaluates whether suppressions are validated, tracked, and justified with appropriate evidence, and whether there are controls to avoid misuse or over-suppression.

The objective is to ensure that suppression practices reduce alert fatigue without allowing real risk to be ignored. Mature organizations establish review workflows, require supporting rationale, track suppression trends, and periodically reassess suppressed items to maintain coverage and integrity.

Risk-Based Prioritization

This domain measures how effectively the organization combines multiple data points—such as CVSS, asset importance, exploitability, and business impact—to prioritize remediation efforts. It moves beyond first-in, first-out or severity-only models and toward risk-informed decisions.

The goal is to assess whether prioritization is repeatable, scalable, and aligned with the organization's risk tolerance. At higher maturity, models are weighted, dynamic, and reviewed regularly with input from stakeholders across security, IT, and business functions.

Third-Party Risk Identification

This domain focuses on how well the organization identifies vulnerability risks introduced by third-party software, components, or services. Unlike asset discovery, this covers software supply chain exposure, library dependencies, and partner systems integrated into business processes.

Mature programs map third-party components, monitor advisories, and incorporate software bill of materials (SBOM) data into risk analysis. This ensures that vulnerability management covers risks from externally developed or supported technologies.

Root Cause Analysis

This domain evaluates whether the organization investigates why vulnerabilities occur and whether lessons learned are used to reduce future occurrences. Root cause analysis (RCA) identifies patterns such as weak development practices, poor patch hygiene, or systemic misconfigurations.

The intent is to move from reactive remediation to long-term risk reduction. Mature programs incorporate RCA into governance reviews, track recurring issues, and use insights to improve development lifecycles, configuration baselines, and business processes.

Threat Intelligence Correlation & Exploit Analysis

This domain assesses how well the organization aligns its internal vulnerability findings with external threat intelligence and exploit data. It includes the use of curated feeds, attack campaigns, active exploitation reports, and mappings to adversary tactics and techniques (e.g., MITRE ATT&CK).

The objective is to determine whether threat context is used to prioritize and respond to vulnerabilities that are most likely to be targeted. Mature programs use correlation tools and integrate exploit data into ticketing, dashboards, and governance reporting.

Vulnerability Aging & Exposure Tracking

This domain measures how long vulnerabilities remain unresolved and how long assets remain exposed. Time-to-remediate (TTR), aging buckets, and SLA compliance are key metrics in understanding backlog health and risk accumulation.

The goal is to determine whether unresolved issues are tracked, reviewed, and addressed in a timely manner. Mature organizations use this data to drive accountability, prioritize resources, identify bottlenecks, and report risk trends to leadership.

Vulnerability Clustering & Campaigns

This domain evaluates whether the organization groups similar or related vulnerabilities to enable more efficient remediation. Clustering may be based on vulnerability type, system type, root cause, threat vector, or affected product family. Campaigns refer to organized efforts to resolve a group of related vulnerabilities at once.

The objective is to assess whether remediation is approached tactically or strategically. At higher maturity, organizations launch coordinated campaigns, track campaign metrics, and use outcomes to address systemic risks and improve remediation throughput.

COMMUNICATE

Alerting & Operational Notification

This domain evaluates how effectively operational teams are alerted when vulnerabilities are identified, particularly for high-severity or time-sensitive issues. It includes the mechanisms used to distribute alerts, how they are prioritized, and the ability to track acknowledgment and action.

The goal is to ensure vulnerability alerts are reliable, actionable, and timely, driving appropriate response. Mature organizations integrate alerting into ITSM platforms or communication tools, include business and risk context in the messages, and monitor performance such as time to acknowledgment and mean time to resolution.

Exception & Risk Acceptance Communication

This domain focuses on how well risk acceptances and exceptions are communicated to stakeholders such as business owners, IT, compliance, and security leadership. It ensures that decisions to not remediate are transparent, reviewed, and understood by accountable parties.

Mature programs define structured communication workflows and provide regular reporting on exceptions—including scope, justification, expiration, and residual risk. This ensures risk ownership is maintained and exceptions do not fall through governance gaps.

Governance & Escalation Reporting

This domain measures how effectively unresolved vulnerabilities, SLA breaches, and systemic failures are escalated to the appropriate governance bodies. It includes tracking of escalation criteria, responsible owners, and resolution outcomes.

The objective is to ensure that persistent or high-risk issues are not ignored but raised and addressed through formal governance structures. At higher maturity, escalations are data-driven, trend-informed, and integrated into program reviews, risk dashboards, and executive briefings.

Metrics & Performance Reporting

This domain assesses how clearly and consistently program performance is measured and reported. This includes tracking KPIs such as remediation timelines, coverage rates, exception volumes, and aging of vulnerabilities. Metrics should drive accountability and support decision-making at various levels.

Mature organizations tailor reports to stakeholder roles, provide trends over time, and highlight bottlenecks or improvement opportunities. Dashboards and reports are aligned with business objectives and contribute to prioritization and resourcing discussions.

Stakeholder Engagement & Risk Framing

This domain focuses on how well the organization frames and communicates vulnerability risk to business and technical stakeholders in language that supports action and alignment. It includes

translation of technical risk into business context, and integration into broader enterprise risk communication.

The goal is to foster shared ownership and a risk-informed culture. At higher maturity, risk framing is part of cross-functional reviews, tailored to stakeholder concerns, and designed to enable informed trade-offs and accountability across the organization.

TREAT

Change Management Integration

This domain assesses how well vulnerability remediation is incorporated into the organization's change management processes. Vulnerability-related changes—such as patch deployment or configuration updates—must be scheduled, approved, and tracked according to IT governance and operational policy.

The objective is to ensure remediation aligns with organizational standards for safety, auditability, and traceability. Mature programs integrate risk ratings into change approval workflows, automate low-risk changes where appropriate, and use change metrics to monitor operational and security performance.

Compensating Controls

This domain evaluates how well the organization uses alternative controls to reduce risk when vulnerabilities cannot be remediated directly. Compensating controls may include isolation, firewall rules, application restrictions, access controls, or temporary process changes.

The goal is to ensure that risk is still addressed when remediation is delayed or infeasible. At higher maturity levels, controls are selected based on risk context, reviewed for effectiveness, and tracked alongside the vulnerability record. Their use is transparent, documented, and subject to governance.

Configuration Management

This domain focuses on how the organization defines, applies, and maintains secure configuration baselines across systems. Misconfigurations are a common source of vulnerability, and drift from secure baselines must be monitored and corrected.

The goal is to measure how effectively configurations are enforced, tracked, and aligned with security policy. Mature organizations use automation to detect and remediate drift, integrate configuration checks into CI/CD workflows, and use compliance metrics to guide improvement.

Patch Management

This domain evaluates how consistently and effectively patches are identified, approved, tested, and deployed. It includes coverage, timeliness, exception handling, and integration with vulnerability management systems. Patching remains a critical defense against exploitation.

The goal is to ensure patches are applied promptly and strategically. At higher maturity, patching is risk-informed, integrated with change and asset management, and monitored through dashboards showing backlog, coverage, and SLA performance.

Remediation Orchestration & Automation

This domain assesses how well remediation activities are coordinated and automated across

teams and systems. It includes the use of scripts, playbooks, ITSM integrations, and automated workflows that trigger based on risk ratings or detection events.

The goal is to improve speed, consistency, and scalability of remediation. At higher maturity, remediation is policy-driven, triggered dynamically by risk signals, and tracked through automation metrics such as coverage, success rate, and rollback incidents.

Remediation Validation & Closure

This domain focuses on whether the organization validates that remediation actions—such as patching or configuration changes—have been successfully completed. It includes rescanning, testing, or verification checks, and ensures closure is based on evidence, not assumption.

The objective is to ensure that vulnerabilities are truly resolved and do not remain silently active. Mature programs automate validation where possible, enforce closure criteria, and track remediation accuracy to guide accountability and program improvement.

Risk Acceptance Governance

This domain evaluates how risk acceptances are documented, approved, tracked, and reviewed. Not all vulnerabilities can or should be remediated; governance ensures that accepted risks are visible, justified, and time-bound.

The goal is to ensure risk acceptance aligns with the organization’s risk tolerance and is not used as a loophole. Mature programs include exception reviews, stakeholder signoff, expiration workflows, and metrics to spot trends or overuse.