Vulnerability Management Maturity Model (VMMM)

Version: v2.0.0
Release Date: 2026-01-29

	Capability	Tier	Level 1	Level 2	Level 3	Level 4	Level 5
Prepare	Context	1 - Foundational	Vulnerability management operates without meaningful context. Teams focus only on scanning and patching, with no linkage to business priorities, asset value, or regulatory drivers.	Some teams consider external pressures such as audits, compliance deadlines, or customer demands, but these are applied inconsistently. Business and risk context depends on individual initiative rather than a structured process.	Policies and prioritization reference business functions, asset classifications, and regulatory requirements. Contextual factors such as compliance scope, departmental risk tolerance, and service criticality influence remediation decisions.	Business impact ratings, asset ownership, and customer-facing importance are integrated into prioritization workflows. Threat intelligence and contextual data (e.g., cloud tags, CMDB metadata, attack surface maps) enrich decision-making. Dashboards reflect both business and threat context for shared situational awareness.	Real-time business and threat context dynamically adjusts prioritization and resource allocation. Contextual inputs include KPIs, telemetry, and active threat campaigns. Dashboards link exposure directly to business objectives, enabling executives and security leaders to make joint, risk-aligned decisions at speed.
	Zero-Day Readiness	1 - Foundational	There is no formal process to assess or respond to high-impact or zero-day vulnerabilities. Teams react inconsistently, with limited coordination or documentation.	Some ad hoc procedures exist for responding to critical or zero-day vulnerabilities, but response depends on individual effort and is not repeatable. Ownership is unclear during high-pressure events.	A defined response process is in place for handling zero-days and critical vulnerabilities, including communication channels, designated leads, and documented response steps. Roles and responsibilities are assigned.	Zero-day readiness is supported by playbooks, pre-established workflows, and regular crisis simulations involving IT, security, and business units. Response timelines and coordination are measured and improved over time.	The organization operates a cross-functional crisis response framework with real-time data inputs, automated workflows, and defined escalation paths. Lessons learned are captured and integrated into future preparedness planning. Response performance is tracked and used to inform strategic risk posture.
	Policy & Standards	1 - Foundational	No formal vulnerability management policies or standards exist. Teams operate independently without defined requirements or alignment to business or regulatory needs.	Basic vulnerability expectations (such as patch SLAs or platform standards) exist but are inconsistently applied. Documentation is fragmented, and enforcement depends on team initiative or external audits.	Organization-wide policies are formally documented, approved, and communicated. Standards define ownership, remediation timelines, acceptable risk thresholds, and exception handling. They are aligned with business priorities and compliance requirements.	Policies and standards are embedded into technical workflows and automated controls (e.g., CI/CD pipelines, IaC templates, compliance checks). Exceptions are centrally documented and reviewed. Updates occur proactively based on regulatory changes, new threats, or changes in risk appetite.	Policies and standards evolve continuously through feedback loops driven by exposure metrics, incident trends, and audit findings. Enforcement is automated across hybrid and cloud environments. Effectiveness is measured, and policies are refined based on performance data and emerging risks.
	Program Governance	1 - Foundational	No formal governance structure exists for vulnerability management. Activities are informal and lack oversight, coordination, or reporting to leadership.	Governance is limited to periodic check-ins or informal reviews. Some reporting occurs, but accountability, oversight, and alignment with business risk are inconsistent.	A defined governance structure is in place, with regular meetings, assigned executive sponsors, and standardized reporting on program performance and risk status. Risk tolerance and prioritization approaches are reviewed annually.	Governance includes cross-functional participation from IT, Security, and Business units. Metrics, exceptions, and strategic blockers are reviewed monthly, and governance inputs directly influence remediation priorities and resourcing.	Governance is tightly integrated with enterprise risk management and strategic planning processes. Performance data, stakeholder feedback, and threat intelligence are used to guide program evolution. Decisions are transparent, repeatable, and directly linked to business outcomes.
	VM Roles & Responsibilities	1 - Foundational	No formal roles or responsibilities are assigned for vulnerability management. Activities are handled reactively and inconsistently by whoever is available.	Some teams have informal or self-assigned responsibilities for parts of the VM process, but ownership is fragmented and accountability is unclear.	Roles and responsibilities for vulnerability discovery, triage, remediation, and oversight are clearly defined, documented, and communicated across technical and business units. Accountability is tracked through assigned owners.	Role-based expectations are embedded in workflows, with responsibilities enforced through automated assignments, escalation paths, and role-specific dashboards. Cross-team coordination is routine and structured.	Role ownership is reinforced through governance, performance metrics, and continuous training. Responsibility models are scalable, embedded across the enterprise, and aligned with organizational structure and accountability frameworks.
	Risk Appetite & Tolerance Definitions	2 - Enhanced	The organization has no defined risk appetite or tolerance for vulnerabilities. Risk decisions are inconsistent and based on individual judgment or urgency.	Some risk thresholds or criteria are referenced informally, but they are not documented, consistently applied, or aligned with business objectives.	Risk appetite and tolerance for vulnerabilities are formally documented and approved. These definitions guide prioritization, remediation timelines, and risk acceptance decisions across the organization.	Risk tolerance is linked to asset criticality, data sensitivity, and business impact. Risk thresholds are embedded in decision-making workflows and reviewed regularly in collaboration with business and risk leaders	Risk appetite is dynamically informed by threat intelligence, operational metrics, and evolving business priorities. Risk tolerance thresholds are tailored to context and continuously refined. Decisions are auditable, consistent, and used to balance security and business agility.
	Security Ecosystem Integration	2 - Enhanced	Vulnerability management operates in a silo with little to no coordination with other security, IT, or business functions. There is no integration with related systems or processes.	Basic data sharing occurs with select tools (e.g., CMDB or SIEM), but integrations are manual, incomplete, or point-in-time. Coordination with other teams is limited.	Vulnerability management is integrated with key systems such as asset inventory, ticketing, and threat intelligence platforms. Data flows are automated, and stakeholders across IT and security reference shared sources of truth.	Vulnerability intelligence is actively consumed by security operations and threat detection teams. Remediation actions are triggered by integrated workflows across detection, response, and change management systems.	Vulnerability data is fully embedded within a unified security architecture. Insights drive threat hunting, control tuning, and risk modeling across the enterprise. Ecosystem integrations are bi-directional, contextualized, and continuously monitored.
	Crisis Communication Readiness	2 - Enhanced	There is no defined process for communicating during a vulnerability-related crisis. Messaging is reactive, inconsistent, and often delayed.	Communication during high-impact vulnerability events occurs informally. Some stakeholders may be informed, but messages are uncoordinated and lack predefined guidance.	A formal crisis communication plan exists, including predefined contact lists, message templates, and internal notification procedures for vulnerability-related events. Roles are assigned for message approval and delivery.	Communication workflows are tested through simulations, and updates are coordinated across security, legal, communications, and executive teams. Internal and external messaging is aligned with organizational policies and regulatory obligations.	Crisis communication processes are proactive and adaptive, supported by scenario-based templates and real-time escalation mechanisms. Stakeholder-specific messages are pre-approved and ready for rapid deployment. Communication effectiveness is measured and continuously improved.

	Data Quality & Source of Truth	1 - Foundational	Vulnerability and asset data is fragmented across tools (scanner, CMDB, cloud, ITSM). Duplicate, stale, or missing records are common. No single source of truth exists, and teams work from conflicting datasets.	Basic reconciliations are performed manually (e.g., periodic CMDB ↔ scanner exports). Asset naming and tagging standards exist but are inconsistently applied. Data accuracy issues are often discovered only during incidents or audits.	An enterprise asset inventory is designated as the source of truth and regularly reconciled against scanners, cloud, and IT systems. Ownership of data quality is assigned. Metrics on coverage gaps and stale records are tracked.	Bi-directional integrations enforce consistent asset identifiers across scanners, CMDB, cloud providers, and ITSM. Automated reconciliation detects and corrects duplicates, stale entries, or gaps. Data quality KPIs (e.g., % orphan assets, % reconciled records) are reviewed in governance cycles.	Data quality is continuously monitored and adaptive. Self-healing processes correct inconsistencies automatically. Source-of-truth decisions are governed by business and risk context. Asset and vulnerability data is enriched with metadata (e.g., ownership, criticality, cloud tags) to ensure reliable, risk-informed decisions.
	Third-Party VM Readiness	3 - Strategic	No vulnerability management expectations are set for vendors, suppliers, or third parties. Contracts lack language on patch timelines, disclosure, or vulnerability reporting.	Some procurement or vendor agreements reference security requirements, but they are generic (e.g., "maintain secure systems") and unenforced. No process exists to validate compliance.	Vendor contracts include basic vulnerability management obligations such as patch timelines for critical issues, breach notification clauses, or evidence of secure development practices. Procurement staff are trained to include these requirements in new agreements.	Third-party VM expectations are standardized across all contracts and tied to risk tiers. Requirements include SBOM availability, coordinated disclosure timelines, and patch SLAs. Compliance evidence (e.g., attestations, third-party audit results) is reviewed periodically.	Third-party VM readiness is proactive and intelligence-driven. Suppliers are required to provide SBOMs, patch SLAs, and vulnerability disclosure reports. Performance is monitored via automated feeds, portals, or continuous assurance mechanisms. Vendor compliance data is integrated into organizational risk dashboards and influences procurement decisions.
Identify	Ephemeral & Short-Lived Asset Discovery	1 - Foundational	The organization has no visibility into ephemeral or short-lived assets. These systems are not included in vulnerability scans and inventory.	Some discovery occurs for dynamic assets, but it is manual, point-in-time, or limited to specific environments. Visibility is incomplete and not actionable.	Defined processes and tools are in place to discover and catalog ephemeral assets in key environments. Data is collected frequently enough to support basic vulnerability identification.	Short-lived assets are discovered automatically using integrations with orchestration platforms, cloud APIs, and deployment pipelines. Data is retained and correlated with vulnerability findings.	Discovery of ephemeral assets is continuous and context-aware, integrated with CI/CD workflows and runtime telemetry. Insights inform risk decisions, coverage metrics, and remediation planning across all environments.
	External Vulnerability Intelligence Ingestion	1 - Foundational	The organization does not monitor or ingest external vulnerability intelligence. Awareness is limited to vulnerabilities detected internally or mentioned informally.	External sources such as vendor bulletins or mailing lists are reviewed manually and sporadically. There is no defined process for validation, prioritization, or dissemination.	A defined process exists to monitor, evaluate, and ingest vulnerability data from trusted sources. Intelligence is triaged by the security team and incorporated into internal analysis and ticketing systems.	External intelligence is automatically ingested from multiple sources—including threat intel feeds, coordination centers, and vulnerability databases—and enriched with asset context and threat likelihood. Distribution to relevant stakeholders is standardized and timely.	Ingestion is real-time, curated, and prioritized based on business relevance and exploitability. Intelligence feeds dynamically influence detection rules, prioritization algorithms, and proactive controls. Feedback loops refine source value and inform vendor engagement.
	Shadow IT & Rogue Asset Detection	1 - Foundational	The organization has no capability to detect or track unauthorized, rogue, or unmanaged assets. Shadow IT remains invisible and unaddressed.	Some shadow IT or rogue assets are discovered reactively, often during incident investigations or audits. There is no systematic approach to detection or tracking.	A defined process exists to identify and review unmanaged or unauthorized assets, using periodic network scans, DNS queries, or third-party data sources. Findings are manually reviewed and addressed.	Detection of shadow IT and rogue assets is automated and integrated with asset management and vulnerability tooling. Discovery leverages telemetry, external attack surface monitoring, and cloud-native APIs.	Rogue asset detection is continuous, risk-prioritized, and integrated with governance processes. Shadow IT findings trigger investigation, remediation, and policy updates. Metrics track asset coverage gaps and inform enterprise IT strategy.
	Asset Inventory & Classification	1 - Foundational	No reliable asset inventory exists. Systems are added, removed, or changed without formal tracking, and there is no consistent asset classification.	Some asset data is collected, but inventories are incomplete, outdated, or limited to specific environments. Classification is informal or missing for most assets.	An organization-wide asset inventory is maintained and updated regularly. Assets are classified based on type, owner, and environment, with risk-critical systems identified. Inventory is used to scope vulnerability assessments.	Asset inventories are continuously updated through automated discovery tools and integrated with configuration management and vulnerability scanning platforms. Assets are tagged by business function, sensitivity, and operational impact.	Asset classification is dynamic and contextual, incorporating real-time telemetry, usage patterns, and business priorities. Inventories support risk-based decision-making, proactive security controls, and audit-ready reporting across all environments.
	Manual Discovery & Analyst Testing	2 - Enhanced	No manual validation or analyst testing occurs. The organization relies solely on automated tools, regardless of asset type, environment, or complexity.	Ad hoc manual checks are performed when scan coverage is questioned or when critical systems are under review. Results are undocumented and inconsistent across teams.	Analysts perform structured manual reviews on high-value or high-risk systems. Testing supplements automation by validating scan accuracy, uncovering misconfigurations, and identifying logic flaws. Results are documented and fed back to remediation teams.	Manual testing is a defined, repeatable process for priority systems (e.g., crown jewels, external-facing apps). Results are tracked, correlated with automated findings, and used to tune scanning tools. Threat-informed validation (e.g., red/purple team insights, bug bounty reports) is incorporated into the workflow.	Manual testing is continuous, risk-informed, and fully integrated into development and operational processes (e.g., SDLC, CI/CD security gates). Findings are categorized, validated, and used to improve detection logic, secure coding practices, and analyst training. Manual analysis is leveraged for adversary emulation and systemic resilience testing, not just gap-filling.
	Third-Party Asset Discovery	2 - Enhanced	The organization has no visibility into systems or services managed by third parties. Dependencies are undocumented and excluded from vulnerability management.	Some third-party systems are known through procurement or onboarding processes, but asset discovery is incomplete and not maintained. Risk is assumed rather than validated.	Third-party assets are tracked using a defined process, including contractual documentation and asset registration. Security expectations are communicated and reviewed periodically.	Third-party asset inventories are validated against technical discovery methods (e.g., traffic logs, cloud integrations). Identified assets are included in scan coverage or require evidence of patching and risk treatment.	Discovery of third-party assets is proactive, continuous, and risk-informed. Integration with third-party risk management enables dynamic tracking, performance monitoring, and enforcement of vulnerability handling requirements across the vendor ecosystem.
	Automated Vulnerability & Exposure Scanning	1 - Foundational	Scanning is irregular, manual, and siloed by team or technology. Only a subset of assets are scanned, often without authentication. Coverage is unknown, and results are not linked to remediation processes.	Routine scans are performed on critical systems or environments, typically scheduled monthly or quarterly. Some authenticated scanning occurs, but coverage is incomplete and cloud/container workloads are often excluded. Reporting is ad hoc.	Enterprise-wide scanning standards exist. Authenticated scans are applied to most critical platforms, and coverage metrics are tracked. Vulnerability scanning is tied to asset inventory and exceptions are documented. Remediation teams receive regular reports with defined timelines.	Scanning is continuous, risk-informed, and covers hybrid environments (on-prem, cloud, containers). Pipelines and orchestration tools integrate scanning directly into builds, deployments, and change workflows. Coverage, latency, and exception metrics are monitored and reviewed.	Scanning is adaptive, dynamic, and intelligence-driven. Threat intel (e.g., KEV, EPSS, active exploit campaigns) adjusts scanning focus automatically. Continuous monitoring extends to external attack surface (ASM/EASM) and SaaS environments. Results feed directly into risk dashboards, governance reviews, and remediation orchestration.

	Application & Service Discovery	2 - Enhanced	Applications and services are not systematically tracked. Web apps, APIs, and SaaS platforms are deployed without visibility into security coverage. Dependencies (open-source libraries, third-party services) are unmanaged.	Critical applications are inventoried manually, often during compliance or audit cycles. Some API discovery occurs, but coverage is incomplete. SaaS usage and software dependencies are poorly tracked and inconsistently included in vulnerability assessments.	An application inventory exists, covering major web apps, APIs, and SaaS platforms. Open-source and third-party software components are identified through basic SBOMs or vendor documentation. Discovery processes are repeatable, and results feed into vulnerability scanning or security reviews.	Application and service discovery is automated and continuous. API gateways, service maps, and SaaS management tools feed data into asset inventories. SBOMs are generated for critical applications and incorporated into vulnerability analysis. Findings are correlated with business context and integrated into risk-based prioritization.	Discovery is comprehensive, dynamic, and risk-driven. Applications, APIs, SaaS, and software components are continuously mapped and enriched with business criticality, threat intelligence, and exploit data. Dependency tracking and SBOMs are automated, validated, and linked to patching and remediation workflows. Exposure from applications and services is proactively monitored, with trends reported to governance for strategic investment decisions.
Analyze	Exploitability Assessment	1 - Foundational	Exploitability is not evaluated. All vulnerabilities are treated equally, based solely on default scanner scores or severity labels.	Teams manually review exploitability information for some high-profile vulnerabilities, but there is no standardized or timely process to assess exploit likelihood.	A defined process exists for assessing exploitability using public sources such as exploit databases, vendor advisories, or threat intelligence feeds. Exploitability is factored into prioritization decisions.	Exploitability ratings are enriched with real-time data, including known exploit code, proof-of-concept availability, active scanning activity, and threat actor targeting. Ratings are integrated into scoring systems and remediation workflows.	Exploitability assessments are predictive and dynamic, incorporating external intelligence, telemetry, and machine learning signals. Inputs feed into automated risk models that adjust prioritization and defense posture based on observed attacker behavior and emerging threats.
	Risk-Based Prioritization	1 - Foundational	All vulnerabilities are treated equally, or prioritized solely by severity (e.g., CVSS score). There is no consideration of exploitability, business impact, or exposure context.	Teams manually adjust priorities when major threats emerge (e.g., headlines, vendor alerts), but decisions are inconsistent, undocumented, and vary by analyst or team.	Prioritization models incorporate multiple data points including asset criticality, business function, and vulnerability severity. Risk scoring is applied consistently across teams, with defined SLAs and ticketing integration.	Risk-based prioritization integrates exploitability intelligence (e.g., EPSS, KEV, threat feeds), asset value, and exposure metrics (aging, external vs. internal). Prioritization outputs are automatically reflected in remediation workflows and governance reporting.	Prioritization is predictive, automated, and continuously updated with contextual business data, exploit trends, and risk tolerance thresholds. Models are governed, transparent, and tailored to organizational priorities. Real-time scoring routes vulnerabilities directly to the right owners, ensuring the highest-risk issues are addressed first.
	Vulnerability Aging & Exposure Tracking	1 - Foundational	The organization does not track how long vulnerabilities remain open or how long systems remain exposed. There is no visibility into backlog or remediation timelines.	Some aging information is reviewed manually or during audits, but data is incomplete, inconsistent, or not used for decision-making or accountability.	Vulnerability aging is tracked across all environments using defined time windows. Metrics such as average time-to-remediate (TTR) and overdue issues are monitored and reviewed by responsible teams.	Aging data is integrated into dashboards, SLA enforcement, and performance reporting. Exposure timelines are aligned to asset criticality and risk ratings. Trends are used to identify blockers and improve remediation workflows.	Exposure and aging metrics are dynamic, predictive, and tailored by vulnerability type, asset context, and business impact. Insights are used to optimize remediation pipelines, influence staffing or tooling decisions, and drive measurable risk reduction outcomes.
	Business Impact Modeling	2 - Enhanced	Vulnerability analysis considers only technical severity. No structured method exists to evaluate how unresolved vulnerabilities affect the business, customers, or operations.	Some high-profile assets or services are informally flagged as more critical. Business input is anecdotal and rarely documented. Remediation decisions are still driven primarily by severity scores.	A defined methodology exists for assessing business impact. Factors include asset criticality, compliance scope, customer exposure, and operational dependencies. Basic consideration is given to remediation feasibility (e.g., downtime windows, staffing requirements).	Business impact modeling incorporates quantitative and qualitative data, including potential financial loss, reputational damage, and regulatory penalties. Models explicitly evaluate remediation effort, cost, and resource capacity alongside risk. Results are integrated into prioritization workflows and governance discussions.	Impact modeling is dynamic, predictive, and continuously updated with real-world telemetry (e.g., service availability, customer SLAs, revenue streams). Business and IT jointly assess both potential loss if unremediated and remediation feasibility/cost to optimize decisions. Impact models feed directly into enterprise risk dashboards and investment strategies.
	False Positive & Suppression Validation	2 - Enhanced	Suppressions and false positive handling are ad hoc or nonexistent. Findings may be ignored without documentation or validation, increasing both risk and noise.	Some findings are suppressed manually by individuals, but there is no consistent validation process or audit trail. Suppressions may be overused or incorrectly applied.	A documented process exists to suppress or mark findings as false positives, including defined criteria, validation steps, and periodic reviews. Suppressions are tracked and subject to oversight.	Suppression workflows are integrated into vulnerability tooling and tied to role-based permissions. Suppression requests require supporting evidence and are subject to peer or risk team review. Revalidation occurs on a scheduled basis.	Suppression and false positive decisions are data-driven and risk-aware, leveraging automation, system telemetry, and historical accuracy metrics. Governance ensures consistent, justified application, and impact on overall risk posture is measured.
	Root Cause Analysis (RCA)	2 - Enhanced	No formal root cause reviews are performed. Repeated vulnerabilities or failed fixes recur without structured analysis or lessons learned.	Teams occasionally perform informal reviews after repeated issues or SLA breaches, but findings are inconsistent, undocumented, and rarely acted on.	Root cause analysis is triggered by SLA violations, recurring findings, or significant incidents. Reviews are documented, with corrective actions assigned and tracked. Categories may include process gaps, patch quality issues, or configuration drift.	RCA is embedded into post-incident reviews and governance cycles. Findings are categorized using frameworks (e.g., MITRE ATT&CK, CIS Controls) to identify systemic weaknesses. Trends are tracked across teams, and insights drive updates to policies, coding standards, and operational workflows.	Root cause analysis is continuous, data-driven, and predictive. Automated analytics detect recurring patterns across business units, environments, and technologies. RCA insights feed directly into KPIs, risk dashboards, and continuous improvement cycles — proactively reducing future exposure through improved design, secure defaults, and organizational learning.
	Threat Intelligence Correlation & Exploit Analysis	2 - Enhanced	Threat intelligence is not used to correlate or assess vulnerability risk. Exploit availability and active threat actor targeting are not considered in remediation efforts.	Teams occasionally review public threat intelligence or exploit news, but correlation with internal vulnerabilities is manual, limited, and reactive.	A formal process exists to correlate vulnerability data with external threat intelligence sources, including exploit databases, threat feeds, and actor campaigns. Exploitability informs prioritization.	Correlation is automated and continuously updated, with data from multiple curated feeds, exploit frameworks, and real-time monitoring. Internal vulnerability findings are enriched with threat context to guide prioritization and mitigation.	Threat intelligence correlation drives adaptive risk scoring and active defense decisions. Findings are used to forecast threat trends, simulate attack paths, and inform governance and strategic planning. Feedback loops refine detection rules and mitigation strategies.

	Vulnerability Clustering & Campaigns	2 - Enhanced	Vulnerabilities are treated individually, without grouping or thematic analysis. Remediation is one-off and reactive.	Occasional grouping occurs (e.g., same product family or patch bundle). Campaigns are ad hoc, driven by vendor releases or urgent threats, not structured planning.	Defined processes exist to cluster vulnerabilities by type, system, or vendor. Coordinated remediation campaigns are planned for related issues. Attackers' known exploitation trends are considered in campaign design.	Campaigns are systemic and risk-informed. Vulnerabilities are clustered not only by product family, but also by attack path or chained exposures (e.g., privilege escalation combined with misconfigurations). Campaign performance is tracked with metrics such as coverage, time to completion, and reduction of systemic risk.	Clustering and campaigns are continuous, intelligence-driven, and prioritized by business and threat context. Advanced analytics identify compound exposure chains across environments, guiding holistic campaigns. Results are used to eliminate root causes, harden environments, and inform future preventive controls. Campaign outcomes are reported to governance as systemic risk reduction, not just patch counts.
	Third-Party Risk Identification	3 - Strategic	The organization does not assess or track vulnerability risk associated with third-party systems, software, or services. Dependencies remain unidentified or unmanaged.	Some third-party risks are recognized through contracts or security questionnaires, but there is no consistent process to identify or track vulnerability exposure across external relationships.	A formal process exists to identify and assess vulnerability risk tied to third-party software, platforms, and services. Risk acceptance or mitigation strategies are documented for high-impact dependencies.	Third-party risk insights are integrated with asset inventories, threat intelligence, and prioritization workflows. Vendors are required to report vulnerability status and remediation actions as part of standard engagement.	Third-party risk exposure is continuously monitored using automated tools, threat feeds, and contractual obligations. Identified risks influence internal remediation decisions and trigger coordinated response or escalation processes. Risk insights feed into procurement, renewal, and strategic planning decisions.
	Governance & Escalation Reporting	1 - Foundational	There is no formal mechanism for escalating unresolved vulnerabilities, missed SLAs, or repeated exceptions. Governance bodies are not informed of VM risks or delays.	Escalation occurs occasionally through informal channels or personal outreach, but there is no structured reporting or governance involvement.	A defined escalation process exists for overdue remediation, high-risk exceptions, or repeated failures. Reports are reviewed by operational leadership or risk committees on a regular basis.	Escalation thresholds, timelines, and roles are clearly defined and enforced. Reporting includes trend data, systemic blockers, and risk exposure. Governance groups actively review unresolved issues and track actions to resolution.	Escalation and governance reporting are integrated with enterprise risk management and leadership dashboards. Reports include metrics on remediation velocity, exception trends, and cross-team accountability. Insights are used to allocate resources, resolve structural barriers, and drive continuous program improvement.
	Metrics & Performance Reporting	1 - Foundational	No consistent performance metrics are reported. Vulnerability management activities are invisible outside security teams, with only anecdotal updates or tool-based counts.	Basic reports or spreadsheets are produced manually, usually on request. Metrics are limited to simple counts (e.g., open vulnerabilities, patches applied) with no consistency or standard cadence.	Core program metrics—such as SLA compliance, scan coverage, vulnerability aging, and remediation timelines—are reported regularly. Standard dashboards or reports are shared across IT and security stakeholders for accountability.	Role-based dashboards provide tailored insights for executives, business leaders, and technical teams. Reporting covers both lagging indicators (e.g., MTTR, SLA adherence, closure rates) and leading indicators (e.g., exploit exposure, backlog trends, vulnerability density). Metrics are reviewed in governance cycles and used to influence prioritization.	Metrics are predictive, risk-informed, and directly aligned with business objectives. Exposure intelligence (EPSS, KEV, exploit maturity) and contextual risk data feed into automated dashboards. Benchmarking and forecasting highlight systemic issues and guide investment. Reporting demonstrates measurable impact on business resilience and overall risk posture.
Communicate							
	Alerting & Operational Notification	2 - Enhanced	No formal alerting or notification mechanism exists for vulnerability findings. Operational teams may be unaware of high-risk issues until manually informed.	Basic notifications are sent by email or system logs, but delivery is inconsistent and lacks urgency, targeting, or confirmation of receipt.	A defined notification process is in place for critical vulnerabilities. Alerts are routed to appropriate operational owners based on asset assignment or severity, with confirmation mechanisms in place.	Alerts are automated, prioritized by risk level, and integrated into operational tools such as ticketing, chat, or incident platforms. Notification delivery is monitored, and escalation paths are enforced for unacknowledged issues.	Notification systems are dynamic and adaptive, tailored by risk profile, asset type, and stakeholder role. Alert fatigue is managed through tuning and suppression logic. Metrics track delivery success, response time, and downstream action.
	Stakeholder Engagement & Risk Framing	2 - Enhanced	Communication is limited to technical teams, with little or no engagement from business stakeholders. Risks are framed using technical jargon, not business impact.	Some outreach occurs to non-technical stakeholders, but messaging is inconsistent and not tailored to business roles or concerns. Risk framing is still primarily technical.	A communication plan is in place to engage relevant stakeholders across business, IT, and security. Risks are translated into business terms, such as impact on services, customers, or compliance.	Stakeholder-specific messaging is delivered regularly and includes visualizations, trend data, and actionable insights. Feedback loops help tailor communications and align on risk framing. Engagement influences prioritization and resourcing.	Risk framing is dynamic, audience-specific, and embedded in enterprise decision-making processes. Stakeholder engagement is proactive and strategic, with VM insights shaping risk appetite, investment decisions, and organizational priorities. Communication effectiveness is tracked and improved continuously.
	Exception & Risk Acceptance Communication	3 - Strategic	Exceptions and risk acceptances are undocumented or handled informally. There is no visibility into what risks have been accepted or why.	Some exceptions are tracked, but documentation is inconsistent and not communicated beyond the immediate team. Decisions lack review or expiration criteria.	A formal process exists for submitting, reviewing, and approving exceptions. Accepted risks are documented with rationale, timelines, and communication to relevant stakeholders. Periodic reviews are conducted.	Exceptions are tied to asset and risk context, and tracked centrally. Communication is structured and includes business, security, and compliance stakeholders. Expiration dates and compensating controls are monitored.	Risk acceptance is integrated into governance and performance reporting. Communication is proactive, with dashboards showing accepted risks by business unit, risk level, and expiration status. Exceptions influence strategic planning and program improvement.
	Vulnerability Disclosure Management	3 - Strategic	The organization has no process for receiving or responding to external vulnerability reports. Security researchers and third parties lack a defined reporting channel.	Disclosures are occasionally received via informal means (e.g., support tickets or social media), but responses are inconsistent and lack ownership or coordination.	A formal vulnerability disclosure process (VDP) is documented and published, including clear intake channels, response expectations, and assigned ownership. Reports are tracked and resolved through defined workflows.	Disclosure handling is integrated with internal remediation processes, legal review, and stakeholder communications. Coordinated disclosure efforts include acknowledgements, timelines, and public statements when appropriate.	Disclosure management is proactive, transparent, and fully embedded in enterprise risk communication. The organization collaborates with researchers, regulators, and partners to manage coordinated disclosures, and leverages insights to improve internal practices. Metrics are tracked on response time, resolution, and disclosure volume.

Treat	Patch Management	1 - Foundational	Patching is irregular, decentralized, and largely left to individual teams. No visibility exists into coverage, timelines, or outstanding risk. Vulnerability findings are often disconnected from patching activity.	Patching follows basic schedules or vendor cycles but is inconsistently tied to vulnerability severity or asset criticality. Coverage reporting is manual and incomplete. Cloud services and containers may be overlooked.	Patch SLAs are defined by vulnerability severity and enforced for critical platforms. Coverage is reported regularly, with dashboards tracking compliance across teams. Vulnerability findings are directly linked to patching workflows.	Patch cycles are prioritized by risk, incorporating exploitability data (e.g., KEV, EPSS), asset value, and business impact. Cloud workloads, containers, and ephemeral systems are included. Metrics track patch latency, backlog, and exposure duration.	Patching is adaptive, automated, and risk-driven. Pre-deployment readiness is validated during asset provisioning (e.g., golden images, hardened baselines). Patch effectiveness and speed are measured continuously, with dashboards showing exposure reduction as a business outcome. Remediation integrates seamlessly into CI/CD pipelines and orchestration tools.
	Remediation Validation & Closure	1 - Foundational	There is no formal validation that vulnerabilities have been remediated. Closure is assumed once action is taken, with no follow-up or confirmation.	Some validation occurs manually, often as part of troubleshooting or compliance audits. Results are not tracked consistently, and findings may remain unresolved.	A defined process exists for validating remediation actions, such as rescanning or configuration checks. Closure requires confirmation and is logged in the tracking system.	Validation is integrated with vulnerability management workflows. Automated scans or control checks confirm remediation success, and failed validations trigger follow-up actions. Closure metrics are reviewed by stakeholders.	Remediation validation is continuous, risk-aware, and automated across all environments. Results inform performance metrics, influence escalation processes, and are embedded in governance reporting. Closure quality is monitored to reduce recurrence and improve control effectiveness.
	Change Management Integration	2 - Enhanced	Vulnerability fixes are applied with no coordination to change management. Remediation introduces untracked risk, outages, or configuration drift. Failed changes are rarely reviewed.	Some vulnerability-driven changes are raised during CAB or change meetings, but security is treated as an afterthought. Coordination is ad hoc, with inconsistent documentation and prioritization.	Critical vulnerability fixes are consistently logged in the change management system with clear justification. Emergency change procedures exist, and risk ratings influence prioritization of urgent remediations.	Vulnerability-driven changes are formally embedded into change workflows. Patch windows and SLAs are aligned with asset criticality and business risk. CAB processes reference risk data, and delays trigger review or escalation.	Change management is risk-informed, automated, and synchronized with CI/CD pipelines and orchestration tools. Pre-approved changes (e.g., for high-risk vulnerabilities) are executed automatically, with rollback safeguards. Dashboards provide real-time visibility into pending, approved, and completed remediation activities tied to change tickets.
	Compensating Controls	2 - Enhanced	No compensating controls are considered or applied. Vulnerabilities that cannot be patched remain unaddressed.	Technical teams occasionally apply informal workarounds or restrictions, but there is no documentation, validation, or tracking of effectiveness.	A defined process exists for implementing compensating controls when remediation is not feasible. Controls are risk-informed, approved, and documented with owner accountability and review timelines.	Compensating controls are standardized, mapped to control frameworks, and validated for effectiveness. They are tracked in asset and vulnerability tooling and reviewed periodically by risk and compliance teams.	Controls are dynamically selected based on context, threat modeling, and risk thresholds. Effectiveness is continuously monitored, and metrics are used to guide improvement. Controls are integrated with risk acceptance, reporting, and program strategy.
	Configuration Management	2 - Enhanced	No formal configuration requirements exist. Changes are applied manually by administrators or developers, often leading to drift, misconfigurations, or inconsistent security posture.	Basic configuration standards are defined for specific platforms or environments, but adoption is uneven. Enforcement depends on individual teams, and deviations are not systematically tracked.	Configuration baselines are defined across major platforms. Compliance with baselines is measured, and deviations are logged and reviewed. Some automation assists with detection or correction of drift.	Enterprise-wide baselines exist for all supported platforms, including cloud and container environments. Drift detection and remediation are automated. Configurations are validated through IaC templates, CSPM tools, and CI/CD pipelines. Metrics on deviation frequency and remediation speed are reported.	Configuration management is continuous, adaptive, and intelligence-driven. Baselines evolve based on incident data, threat intelligence, and business requirements. Automated validation occurs at provisioning, and resilience testing ensures secure defaults. Effectiveness is measured by reduced exposure, not just compliance rates.
	Remediation Orchestration & Automation	2 - Enhanced	Remediation is manual, decentralized, and uncoordinated. Each team addresses vulnerabilities in isolation, with no shared tools or workflows.	Some teams use scripts or tools to automate basic remediation tasks, but orchestration is inconsistent and not integrated with vulnerability data or change controls.	A defined remediation process exists with standardized workflows for ticket generation, ownership assignment, and status tracking. Limited automation is used for repetitive or low-risk tasks.	Remediation is orchestrated across systems and teams, with automation triggered by vulnerability risk ratings, asset criticality, or predefined rules. Processes are integrated with ITSM and infrastructure tooling.	Remediation is adaptive, scalable, and policy-driven. Automation includes patching, configuration changes, or control deployment based on dynamic risk signals. Remediation pipelines are monitored for effectiveness and aligned with continuous delivery and zero-trust strategies.
	Risk Acceptance Governance	3 - Strategic	Risk acceptance is informal and undocumented. Individuals or teams may choose not to remediate findings without oversight or justification.	Some risk acceptances are recorded, but approval processes are inconsistent and not reviewed for alignment with risk tolerance or business impact.	A formal process exists for requesting, approving, and tracking vulnerability risk acceptances. Requests require documented rationale, defined timeframes, and designated approvers.	Risk acceptances are centrally tracked and linked to asset criticality, business impact, and risk thresholds. Periodic reviews and expiration policies are enforced. Governance bodies oversee high-risk or repeated exceptions.	Risk acceptance is fully integrated with enterprise risk management and program governance. Acceptance trends are monitored for systemic issues, and metrics inform strategic decisions. Risk tolerance alignment is audited regularly and influences policy and control investment.

Prepare

- **Context**
- **Zero-Day Readiness**
- **Policy & Standards**
- **Program Governance**
- **Risk Appetite & Tolerance Definitions**
- **Security Ecosystem Integration**
- **VM Roles & Responsibilities**
- **Crisis Communication Readiness**
- **Data Quality & Source of Truth**
- **Third-Party VM Readiness**

Identify

- **Ephemeral & Short-Lived Asset Discovery**
- **External Vulnerability Intelligence Ingestion**
- **Manual Discovery & Analyst Testing**
- **Asset Inventory & Classification**
- **Shadow IT & Rogue Asset Detection**
- **Third-Party Asset Discovery**
- **Automated Vulnerability & Exposure Scanning**
- **Application & Service Discovery**

Analyze

- **Business Impact Modeling**
- **Exploitability Assessment**
- **False Positive & Suppression Validation**
- **Risk-Based Prioritization**
- **Third-Party Risk Identification**
- **Root Cause Analysis**
- **Threat Intelligence Correlation & Exploit Analys**
- **Vulnerability Aging & Exposure Tracking**
- **Vulnerability Clustering & Campaigns**

Communicate

- **Alerting & Operational Notification**
- **Exception & Risk Acceptance Communication**
- **Governance & Escalation Reporting**
- **Metrics & Performance Reporting**
- **Stakeholder Engagement & Risk Framing**
- **Vulnerability Disclosure Management**

Treatment

- **Change Management Integration**
- **Compensating Controls**
- **Configuration Management**
- **Patch Management**
- **Remediation Orchestration & Automation**

Remediation Validation & Closure
Risk Acceptance Governance

Establishes a shared understanding of the organization's mission, environment, threat profile, and critical a
Evaluates readiness to detect, assess, and respond to zero-day threats and crisis-level vulnerabilities under
Assesses the completeness, enforcement, and integration of VM-related policies, standards, and technical b
Measures how VM governance is structured, including accountability, oversight, and integration with risk
Evaluates how well the organization has defined and communicated its risk appetite and tolerance as it rela
Assesses the extent of integration between the VM function and other IT/security systems, tools, and busin
Defines and assigns clear roles, responsibilities, and ownership across security, IT, business, and external s
Assesses the maturity of processes to coordinate internal and external communication during high-risk or t
Evaluates how the organization establishes, maintains, and reconciles authoritative sources for asset and vu
Assesses whether vulnerability management expectations, SLAs, and disclosure requirements are defined i

Measures the ability to discover assets that are short-lived, containerized, or dynamically deployed, often in
Evaluates the ingestion and use of external vulnerability sources (e.g., CISA KEV, vendor advisories, threa
Assesses the organization’s use of pen testing, bug bounty, red teaming, or manual analyst testing to discov
Measures the organization's ability to maintain a comprehensive, accurate inventory of all assets with prop
Measures the ability to detect unauthorized, unmanaged, or miscategorized assets that fall outside approve
Evaluates how the organization identifies assets and systems hosted or operated by third-party vendors or p
Measures the breadth, depth, frequency, and authentication methods of automated vulnerability scanning a
Evaluates the organization's ability to identify and catalog web applications, APIs, microservices, SaaS pla

Assesses whether and how the organization models potential business consequences of exploited vulnerab
Evaluates how technical exploitability is measured, using data such as EPSS, CVSS, proof-of-concept ava
Assesses the process to review, suppress, and validate false positives or de-prioritized vulnerabilities to rec
Measures how well the organization ranks vulnerabilities based on threat intelligence, business impact, exp
Assesses the organization’s ability to discover and assess third-party risk tied to vendor-hosted platforms, S
Evaluates whether the root causes of vulnerabilities (e.g., coding flaws, misconfig, process gaps) are invest
Measures how well external threat intelligence and exploit information are correlated with internal finding
Assesses whether vulnerability age, recurrence, and ongoing exposure are tracked and used to inform risk t
Evaluates the ability to recognize, track, and respond to coordinated campaigns or clusters of vulnerabilitie

Measures how alerts and vulnerability-related notifications are delivered to the right stakeholders with app
Assesses how well risk acceptances and remediation exceptions are communicated, tracked, and revalidate
Evaluates whether the escalation of unresolved or systemic issues is governed through defined channels to
Assesses how well metrics and performance indicators are captured, reported, and used to improve VM de
Evaluates how effectively the VM team communicates risks to business stakeholders, framing issues in co
Assesses how the organization receives, triages, and coordinates vulnerability disclosures from external re

Assesses how well patching and remediation processes are aligned with existing change management gove
Evaluates how compensating controls (e.g., GPOs, firewalls, EDR) are defined, approved, applied, and tra
Measures how secure configurations are defined, enforced, validated, and continuously monitored to preve
Evaluates the maturity of patch identification, testing, deployment, tracking, and validation processes for v
Assesses how remediation tasks are automated, orchestrated, and integrated across tools and teams for scal

Measures how well remediation actions are verified, logged, and formally closed, including re-scanning an
Assesses whether risk acceptance decisions follow a structured, governed process and are tied to overall er

in contracts and enforced with vendors, suppliers, and third-party service providers.