ivanti

Exposure Management Maturity Model

A DIY Guide to Benchmarking Your Maturity and Creating a Targeted Plan for Growth

Contents

1 Prologue and scope

How this guide helps you champion exposure management

As a reader, this guide equips you to translate operational detail into business-level advocacy. By using the Maturity Model and Metrics Matrix, you can:

1. Frame the conversation: “Our current risk posture is X. Our business appetite is Y. The gap is Z.”
2. Show the path: Use the 6×4 matrices to illustrate exactly what Stage 3 or Stage 4 maturity looks like.
3. Demonstrate ROI: Link improvements to reduced downtime, targeted remediation cycles and measurable reductions in exploitable risk.
4. Propose a roadmap: Present a balanced plan of quick wins (visible in one quarter) and long-term projects that align with strategic goals.

Not only does this guide give you a playbook just for maturing patchable vulnerability management, but also for advocating maturity as a strategic priority that directly supports enterprise risk goals.

Why start with patchable vulnerabilities on endpoints?

Even though exposure management (EM) spans many types of issues, unpatched software remains the most common root cause of breaches. Endpoints (e.g., laptops, servers, mobile devices) are:

- **Pervasive:** Every organization has them.
- **Controllable:** IT teams can easily automate patching them.
- **Impactful:** Eliminating patch gaps measurably reduces real-world attack surface.

This makes patchable vulnerabilities the most practical entry point for building an EM program.

This guide does not attempt to solve all exposure types. Instead, it focuses on patchable vulnerabilities as the most immediate, controllable starting point for building an exposure management practice.

Additionally, the lessons explained here extend to cloud, SaaS and non-patchable exposures at higher maturity stages.

What is exposure management?

Exposure management is the discipline of continuously identifying, assessing, prioritizing, validating and remediating potential vulnerabilities across the enterprise.

Unlike traditional vulnerability management (VM), which focuses on detecting known host/infrastructure flaws, EM takes a broader, risk-based view:

- Assets: Not just servers and laptops, but also SaaS apps, cloud resources, identities and even digital brand exposure.
- Exposures: Not limited to CVEs, but also misconfigurations, leaked credentials, unmanaged devices and ineffective controls.
- Context: Vulnerabilities are weighed against exploitability, business criticality and possible mitigation, and the effectiveness of mitigating controls.
- Lifecycle: EM runs continuously (not in quarterly scan-and-patch cycles).

The key difference is that exposure management conveys context in addition to quantifying risk. Where VM tells you, "You have 10,000 CVEs," EM tells you, "50 of those are exploitable, five affect critical systems and fixing them reduces breach likelihood by 80%."

Risk posture vs. risk appetite

To understand EM's role in enterprise security, we need to clarify two risk-related terms that Gartner and regulators use frequently:

Risk posture

The organization's current exposure level given its assets, vulnerabilities and controls.

Example:
"We have 20% of endpoints missing critical patches, which creates elevated ransomware exposure."

Risk appetite

The amount of risk the organization is willing to accept in pursuit of business objectives.

Example:
"We accept that non-critical kiosks may patch on a 90-day cycle, but payroll systems must patch within 14 days."

EM bridges the two by measuring posture (current exposure) and enforcing appetite (aligning remediation with what the business is willing to tolerate).

At low maturity, these concepts remain disconnected: IT patches what it can, Security reports what it finds and executives make decisions without a shared baseline. By Stage 4 maturity, exposure management closes that gap:

- Visibility is drift-resilient.
- Prioritization is predictive.
- Validation is continuous.
- Remediation blends patching and compensating controls.
- Governance elevates exposure reduction into enterprise risk management.

At this point, posture is no longer a static snapshot and appetite is no longer a vague statement — they are linked in a continuous cycle of measurement, decision and action that makes cyber risk truly manageable.

Limits of the model

The scope of this guide is deliberately narrow to ensure it is practical, actionable and relevant to most IT and Security teams today.

We'll cover the following:

- Patchable vulnerabilities on laptops, servers and mobile devices.
- Relevant associated practices (e.g., asset visibility and importance, vulnerability assessment, prioritization, remediation).
- Data flows, governance structures and KPIs tied to patch management.

Limiting the scope of our discussion to these topics makes sense because:

- Patchable endpoints remain the most common breach vector, and every organization has them.
- They are also the most controllable surface area, typically managed by IT operations.
- Focusing here provides a practical entry point to build an exposure management workflow without overwhelming teams with too many categories at once.

Though they are part of the broader attack surface, other exposure categories not explicitly covered here include:

- Cloud misconfigurations and cloud-native exposures.
- SaaS misconfigurations, shadow IT and SaaS-to-SaaS risks.
- Identity and credential exposures (e.g., leaked API keys, password dumps).
- Digital risk (e.g., social media account takeovers, domain abuse, brand spoofing).
- Third-party and supply chain exposures.

You can apply the same maturity-based approach to these other attack surface categories as your organization progresses. For example, you can integrate cloud and SaaS exposures once visibility tooling matures, or score and prioritize supply chain risk using the same business impact framework.

2

Maturity model goals

Exposure management is a set of interconnected capabilities that allow organizations to identify, evaluate and reduce cyber exposure in a continuous manner that aligns with the business. Each capability has a distinct role, but together they create the foundation for aligning technical visibility and risk management with business outcomes.

The six core capabilities are:

1. Asset visibility
2. Asset importance
3. Real-world vulnerability assessment
4. Business-driven vulnerability prioritization
5. Operationally balanced remediation
6. Data / workflow integration

Asset visibility — *What do you have, and can you monitor it?*

What it is: Asset visibility is the ability to maintain a complete, accurate and up-to-date inventory of all digital assets in your organization's environment. This includes traditional IT endpoints and servers, but also cloud workloads, SaaS applications, operational technology (OT), mobile devices and even unmanaged or shadow IT assets.

Why it's important: Visibility is the foundation of EM. An incomplete or outdated view of assets means critical exposures will remain undetected, and downstream prioritization or remediation activities will fail. As infrastructure becomes more ephemeral (e.g., cloud instances spun up and down in minutes), static inventories are no longer sufficient.

Typical technologies/practices:

- CMDBs and IT asset management tools for traditional IT estates.
- Attack surface management (ASM) platforms to consolidate and normalize asset data across tools.
- External attack surface management (EASM) to identify internet-facing assets visible to adversaries.
- Cloud-native discovery through CSPM, KSPM or API integrations.
- Continuous discovery scans and passive monitoring to capture transient or unmanaged assets.

Asset importance — *Which assets matter most to your business?*

What it is: Asset importance captures the value and criticality of assets in relation to business processes, revenue streams and operational resilience. It moves beyond "what exists" to "what matters."

Why it's important: Not all assets are equal. A vulnerability on a development server is not as impactful as one on a payroll system, an e-commerce platform or an industrial control system. Prioritization without context leads to wasted resources and misaligned risk management.

Typical technologies/practices:

- Business impact mapping, linking IT assets to processes and applications.
- Dependency mapping tools that model relationships between applications, infrastructure and services.
- Criticality scoring frameworks that classify assets (e.g., crown jewels, sensitive data stores, customer-facing systems).
- Ownership assignment within CMDB or ASM systems to ensure accountability.

Real-world vulnerablity assessment — *Which exposures are actually exploitable? and can you monitor it?*

What it is: Real-world vulnerability assessment goes beyond identifying known vulnerabilities (CVEs) to evaluate their exploitability, likelihood and potential attack paths in context.

Why it's important: Traditional vulnerability scanning produces long lists of issues, most of which are never exploited. Teams are overwhelmed, leading to remediation fatigue and "tick-the-box" compliance. By focusing on what is exploitable and likely, organizations reduce noise and address real risks.

Typical technologies/practices:

- CISA KEV and similar regional or country-based lists.
- Traditional vulnerability scanning (agent-based and network-based).
- Exploit Prediction Scoring System (EPSS) or other probability-driven models.
- Threat intelligence integration to identify vulnerabilities that are actively weaponized.
- Attack path modeling and exposure validation (e.g., adversarial simulation, breach and attack simulation, red teaming).
- Context enrichment from configuration, identity and control telemetry to reduce false positives.

Business-driven vulnerability prioritization — *What should you fix first?*

What it is: Business-driven prioritization is the process of ranking exposures by their business impact, exploitability and the presence (or absence) of mitigating controls. It answers the question: "Which exposures matter most right now?"

Why it's important: No organization can fix everything. Prioritization ensures resources are directed at the exposures that pose the greatest risk to business outcomes. Without it, security teams drown in vulnerability backlogs while critical risks remain open.

Typical technologies/practices:

- Risk scoring engines that combine vulnerability data with asset criticality, threat intelligence and control effectiveness.
- Exposure aggregation platforms to deduplicate and normalize findings across multiple scanners and domains.
- Business risk alignment tools that translate exposure data into financial or operational impact.
- Dashboards and reporting tailored for different audiences (technical, operational, executive).

Operationally balanced remediation — *Can you close exposures at scale without breaking the business?*

What it is: Operationally balanced remediation is the ability to fix or mitigate exposures in a way that is both effective and practical. It balances security urgency with IT operational realities, like system uptime, patch testing and business continuity.

Why it's important: Identifying exposures has no value if you cannot remediate them. Equally, forcing remediation without considering operational impact can create downtime, resistance and exceptions that undermine security goals. Balance is the key.

Typical technologies/practices:

- Patch management systems integrated with vulnerability data.
- Configuration management and hardening tools.
- Compensating controls for non-patchable vulnerabilities.
- ITSM integration in larger organizations to track SLAs and manage exceptions.
- Remediation orchestration platforms that automate ticketing, patch deployment and reporting.

Data and workflow integration — *Do IT, security and business teams work from the same data and processes?*

What it is: Data and workflow integration connects the dots between detection, prioritization and action by linking security, IT and business stakeholders into shared processes and systems.

Why it's important: Exposure management cannot succeed in silos. Security teams may detect, but IT teams must remediate and executives must understand how exposure management supports business outcomes. Without integration, efforts stall in handoffs and trust gaps.

Typical technologies/practices:

- Exposure assessment platforms that aggregate vulnerability, asset and threat data.
- Bidirectional integration with ITSM systems for ticketing and SLA tracking.
- Dashboards that unify technical and business views of exposure risk.
- ERM system integration to link exposure management into enterprise risk governance.
- Automated data normalization and deduplication across multiple sources.

Practical considerations and capability prioritization

The path through the maturity model is not the same for all organizations. Practical factors (e.g., company size, overarching business goals, baseline capabilities) shape both the starting point and the speed of progression. Not all capabilities can mature simultaneously, and sequencing is essential.

By company size:

- Smaller organizations should start with essentials (i.e., inventory, classification and a consistent vulnerability assessment process). Attempting continuous validation or advanced orchestration too early can overwhelm lean teams. Progression to higher maturity levels should focus on automating foundational tasks to maximize limited staff capacity.
- Mid-sized organizations typically have broader attack surfaces and more specialized staff. Their priority is building consistent cross-functional workflows — linking IT and Security with common KPIs, and ensuring visibility extends into cloud and SaaS assets.
- Large enterprises are best positioned to operate at advanced levels across multiple capabilities, but even they must prioritize. Advanced practices like adversarial validation, full ERM integration and audited impact alignment are achievable only if foundational elements are already strong.

By overall goals:

- Regulatory or compliance-driven programs should emphasize visibility, classification and SLA tracking. These deliver demonstrable audit readiness and measurable compliance progress.
- Risk reduction and resilience goals call for investment in validation, prioritization and balanced remediation. The focus is reducing the likelihood and impact of breaches rather than simply proving control coverage.
- Executive alignment requires prioritization of metrics, dashboards and workflow integration. Here, the emphasis is on translating technical progress into clear business outcomes.

By organizational capabilities:

- If asset inventories are fragmented or unreliable, the first priority is normalizing and reconciling discovery data.
- If scanning and detection are mature but closure is inconsistent, the emphasis should shift to shared KPIs, SLA compliance and exception management.
- If telemetry is strong but stakeholder buy-in is weak, focus on business alignment, executive dashboards and integration with enterprise risk reporting.
- If advanced practices are in place but uneven across teams, invest in workflow integration to create consistency and eliminate silos.

3 Maturity pathways & progression

This section describes how each of the six capabilities mentioned above progresses across four phases of maturity. Each phase includes:

- **Maturity expectations** — What the capability looks like at that level.
- **Applicable metrics** — What you can realistically measure.
- **Next steps** — The actions needed to advance maturity.

Capability summary table

	Phase 1	Phase 2	Phase 3	Phase 4
Asset visibility	Unknown	Incomplete	Critical mass / complete	Drift resilient
Asset importance	Not tracked	Basic classification	Business process-linked	Verified asset criticality
Real-world vulnerability assessment	CVSS-driven	Multi-factor scoring	Likelihood-driven	Regularly validated
Business-driven vulnerability prioritization	Not considered	Asset value / risk calculated	Business impact / risk-driven	Impact prioritization-audited
Operationally balanced remediation	Ad hoc prioritization	Case-by-case collaboration	Shared KPI-driven	Audited retrospectives
Data / workflow integration	Isolated data and processes	Formalized sharing and handoffs	Shared platform	Fully integrated workflows

Asset visibility

	Phase 1 Unknown	Phase 2 Incomplete	Phase 3 Critical mass / complete	Phase 4 Drift-resilient
Expectations	Inventory is incomplete and siloed. Teams rely on ad hoc lists or scanner outputs. Shadow IT and SaaS remain invisible.	CMDB or asset tool exists but lacks security enrichment. Cloud and OT are excluded.	Internal and external discovery integrated. Deduplication and ownership established. Visibility covers most enterprise assets.	Inventory continuously updated, reconciled within hours or days. Single source of truth for IT and Security.
Metrics	■ % of assets without owners ■ % of discovered assets not in CMDB ■ % of shadow IT or unmanaged devices identified ad hoc	■ % of critical assets represented in CMDB ■ frequency of updates ■ % of coverage across core IT-managed endpoints	■ % of asset classes covered (servers, endpoints, cloud, SaaS) ■ % of assets with business owners assigned ■ Asset inventory reconciliation accuracy rate	■ Time lag between asset creation and inventory capture ■ % accuracy verified against validation scans ■ % of assets discovered automatically (vs. manually added).
Next steps	■ Establish a central inventory baseline. ■ Reconcile tool outputs. ■ Begin active and passive discovery of unmanaged endpoints.	■ Integrate CMDB with discovery tools. ■ Add SaaS and cloud connectors. ■ Establish ownership tags.	■ Expand automation for continuous updates. ■ Cross-check against threat intel for exposed assets.	■ Automate reconciliation with ITSM. ■ Implement drift detection. ■ Extend monitoring to OT and supply chain environments.

Asset importance

	Phase 1 Not tracked	Phase 2 Basic classification	Phase 3 Business process-linked	Phase 4 Verified asset criticality
Expectations	All assets treated equally. Patch urgency follows scanner severity only.	Assets grouped broadly (e.g., server vs. endpoint). Categories exist but lack linkage to business processes.	Assets tied to processes and owners. Security teams can articulate which applications drive revenue or support critical ops.	Inventory continuously updated, reconciled within hours or days. Single source of truth for IT and Security.
Metrics	■ % of remediation decisions based solely on CVSS or vendor severity	■ % of assets tagged with at least one classification attribute ■ % of assets mapped to service tiers	■ % of crown jewel assets formally mapped ■ % of remediation tickets tied to business services ■ % of asset owners validated by business units	■ % of asset classifications validated in the last 12 months ■ Number of resilience exercises conducted (testing asset criticality) ■ % of assets linked to risk appetite categories (e.g., 14-day patch vs. 90-day patch)
Next steps	■ Begin classifying assets into production vs. development, critical vs. non-critical.	■ Identify business service owners. ■ Link high-value applications to infrastructure components.	■ Build dependency maps. ■ Validate classifications with business continuity planning.	■ Establish recurring review with process owners. ■ Integrate classifications into enterprise risk reporting.

Real-world vulnerability assessment

	Phase 1 CVSS-driven	**Phase 2** Multi-factor scoring	**Phase 3** Likelihood-driven	**Phase 4** Regularly validated
Expectations	Assessment is scan-centric. Results are reported by CVSS only. Volume overwhelms capacity.	Exploit prediction, threat intelligence, and limited control context applied.	Assessments weight vulnerabilities by exploit likelihood and attack path analysis.	Findings continuously tested via adversarial validation, BAS or red teaming. False positives minimized.
Metrics	■ # of vulnerabilities identified vs. # remediated ■ % of vulnerabilities scored only by CVSS	■ % of vulnerabilities enriched with EPSS/CISA KEV or similar context ■ % of vulnerabilities triaged using multiple factors (e.g. asset value, exposure, exploit status)	■ % of vulnerabilities with likelihood scores ■ # of validated attack paths mapped ■ % of vulnerabilities linked to active exploit campaigns in the wild	■ % of high-risk vulnerabilities validated as exploitable ■ # of simulated attack scenarios conducted per quarter ■ % of validated false positives vs. total findings
Next steps	■ Incorporate exploit intelligence feeds. ■ Start tracking patch rates on high-severity vulnerabilities.	■ Integrate threat intelligence into scanning. ■ Apply basic context filters (internet-facing, critical systems).	■ Deploy attack path modeling. ■ Introduce exposure validation for priority assets.	■ Automate validation testing. ■ Integrate results into prioritization dashboards.

Business-driven vulnerability prioritization

	Phase 1 Not considered	**Phase 2** Asset value / risk-calculated	**Phase 3** Business impact / risk-driven	**Phase 4** Impact prioritization-audited
Expectations	Prioritization is reactive, first-in-first-out or scanner severity.	Basic formulas combine vulnerability severity with asset criticality.	Prioritization integrates exploitability, asset importance and compensating controls.	Prioritization logic formally audited and validated by business units.
Metrics	■ % of tickets prioritized without business context	■ % of prioritized tickets using a risk score ■ Mean time to prioritize after detection	■ % of remediated vulnerabilities tied to business risk thresholds ■ % of high-value assets protected within defined SLA windows ■ % alignment of prioritization rules with risk appetite statements	■ % of prioritization rules reviewed annually ■ Audit results accepted by risk committees ■ % of exposures reprioritized based on changing busness impact
Next steps	■ Introduce asset criticality into ticketing workflows.	■ Standardize risk formula. ■ Align on prioritization metrics with IT operations.	■ Introduce executive dashboards. ■ Validate prioritization logic with business stakeholders.	■ Institutionalize review process. ■ Integrate results with enterprise risk management.

Operationally balanced remediation

	Phase 1 Ad hoc prioritization	**Phase 2** Case-by-case collaboration	**Phase 3** Shared KPI-driven	**Phase 4** Audited retrospectives
Expectations	Remediation is inconsistent. Exceptions are undocumented.	Security and IT coordinate on specific fixes. Exceptions are handled manually.	Joint KPIs are established. Exceptions are logged and reviewed. Operational impacts are considered.	Formal retrospectives on missed SLAs, exception justifications and mitigations. Continuous improvement loop in place.
Metrics	■ % of vulnerabilities past SLA ■ % of exceptions undocumented	■ % of high-priority vulnerabilities remediated within SLA ■ # of exception requests logged ■ Median time to remediate (MTTR) for critical vulnerabilities	■ SLA compliance rate ■ MTTR by severity tier ■ % of exception requests reviewed by Security & IT jointly	■ # of retrospectives held ■ % of exceptions with documented compensating controls ■ % reduction in repeat exceptions over timed
Next steps	■ Document basic remediation SLAs. ■ Track exceptions manually.	■ Formalize SLA tracking. ■ Assign ownership for exceptions.	■ Automate SLA measurement. ■ Introduce post-remediation reporting.	■ Institutionalize retrospectives. ■ Expand remediation coverage to configuration and compensating controls.

Data / workflow integration

	Phase 1 Isolated data and processes	**Phase 2** Formalized sharing and handoffs	**Phase 3** Shared platform	**Phase 4** Fully integrated workflows
Expectations	IT and Security operate independently. Tickets lack context.	Workflows defined between Security and IT. Limited integration.	Exposure data, prioritization logic, and SLAs managed on shared platforms.	EM woven into enterprise risk management. Bidirectional data flow across component operational and enterprise systems.
Metrics	■ % of tickets missing asset criticality ■ # of duplicate tickets created	■ % of remediation tickets generated automatically ■ # of SLA breaches tracked	■ % of vulnerabilities triaged within shared dashboards ■ % of closed tickets with validated status ■ % of workflow steps automated vs. manual	■ % of risk reports sourced from unified data ■ % of exposures linked directly to enterprise risk appetite categories ■ % of integration coverage across component operational and enterprise systems
Next steps	■ Define basic handoffs. ■ Start linking tickets to asset data.	■ Connect scanning tools to ITSM. ■ Introduce bidirectional ticket updates.	■ Expand platform adoption. ■ Build dashboards tailored to executives and IT.	■ Embed exposure reporting into ERM cycles. ■ Automate normalization across sources.

About Ivanti

Ivanti is an enterprise software company that provides a comprehensive IT and security cloud-based platform. Ivanti provides software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing security risk. The Ivanti Neurons platform is cloud-native and is designed as a foundation of unified and reusable services and tools for consistent visibility, scalability and secure solution delivery. Over 34,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and we are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.