EY

Shape the future with confidence

Cybersecurity Performance Management

Risk based Vulnerability Management

Compromisability and Attack Graphs

CTEM and Attack Surface Management

Cyber Risk Quantification

Data and AI Risk Security Posture Management

Continuous Control Management

Enabling Cyber Decision Intelligence

ANALYZE | VISUALIZE | GOVERN

Platform by EY Cyber AI and Product Engineering COE

End-to-end cyber risk management

Unified platform for siloed environment

Identify

- Asset discovery (IT, OT, IoT, AI, cloud)
- Automated Asset Management
- BOM (Software, AI, crypto, API)

Protect

- Threat vs. Control mapping
- Threat modelling

Detect

- Vulnerability Assessment
- Attack Surface Management
- Continuous Control Management

Measure

- Cyber Risk Quantification
- Financial impacts
- Operational impacts

Respond

- Workflow and Ticketing Management
- Hyper automation with SOAR, TIP, TH and Alert Triaging

Recover

- Patch Management
- Configuration Management
- Automated Incident Response

Proactive

- Continuous Threat Exposure Management
- Compromisability and Exploitability
- Breach Attack Simulation
- Attack graphs and Red teaming

All modules are powered by pre-built EY CPM Co-Pilot

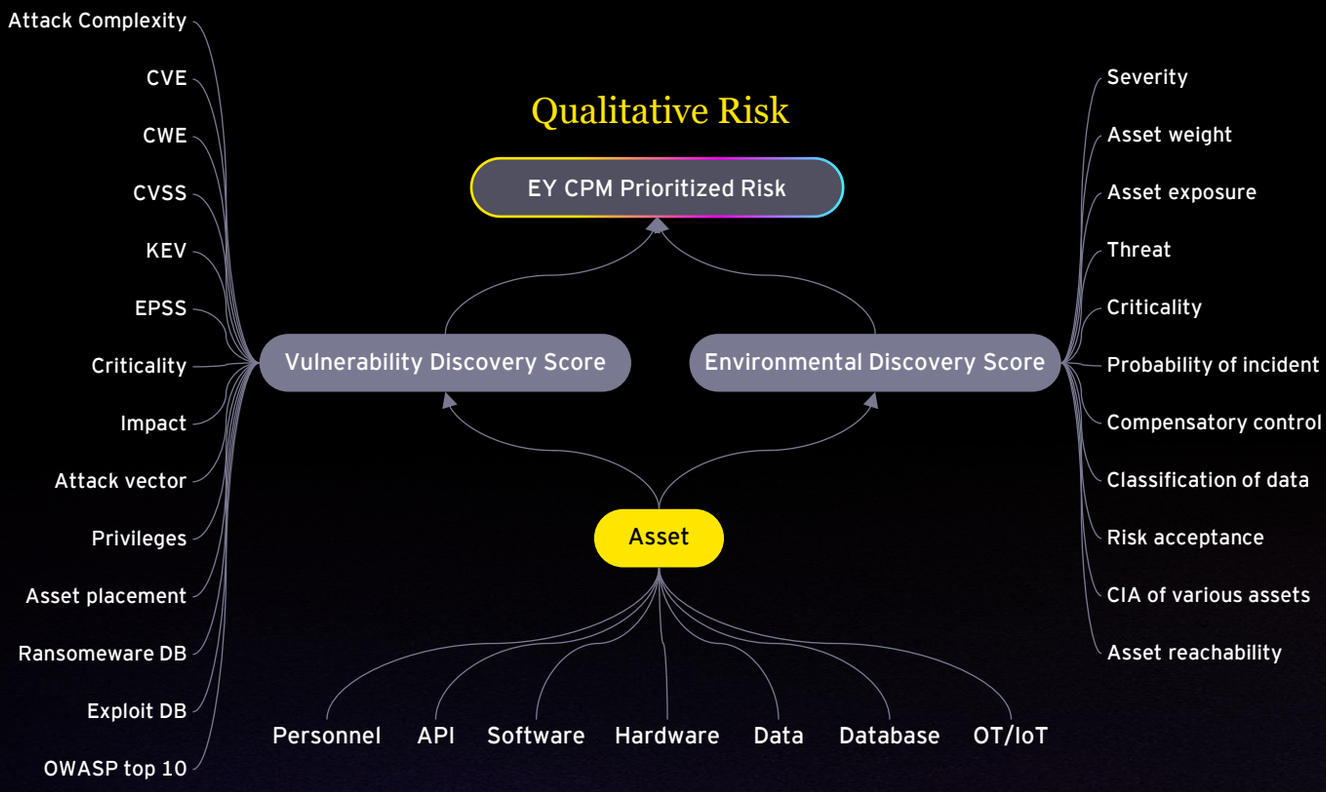
Qualitative risk: *Cyber Risk Visibility Management (CRVM)*

Inherent Risk Factors

- Asset criticality and business classification
- Environment and compliance benchmarks
- Baseline vulnerabilities and compensatory controls

Adversarial Risk Factors

- Threat actor profiling and mapping to enterprise
- MITRE ATT&CK, D3FEND, ATLAS and AppSec Matrix
- Exploit availability, hacker's skillset and Ransomware strain



Benefits

- **Shadow components:** Blind spot detection and near real-time discovery and risk prioritization
- **Noise reduction 45-60%:** De-dupe, exploit-aware triage and TI confidence scoring
- **MTTR 30-50%:** Co-Pilot playbooks + Workflow + Auto-ticketing + Attack simulation
- **Coverage:** Comprehensive ATT&CK, D3FEND t and ATLAS techniques monitored/blocked
- **Critical paths:** Reduced blast radius and MTTC; visualize end-to-end attack routes to crown jewels
- **Efficiency advantage:** FTE efficiency 50-65%; MTTR 30 -50%

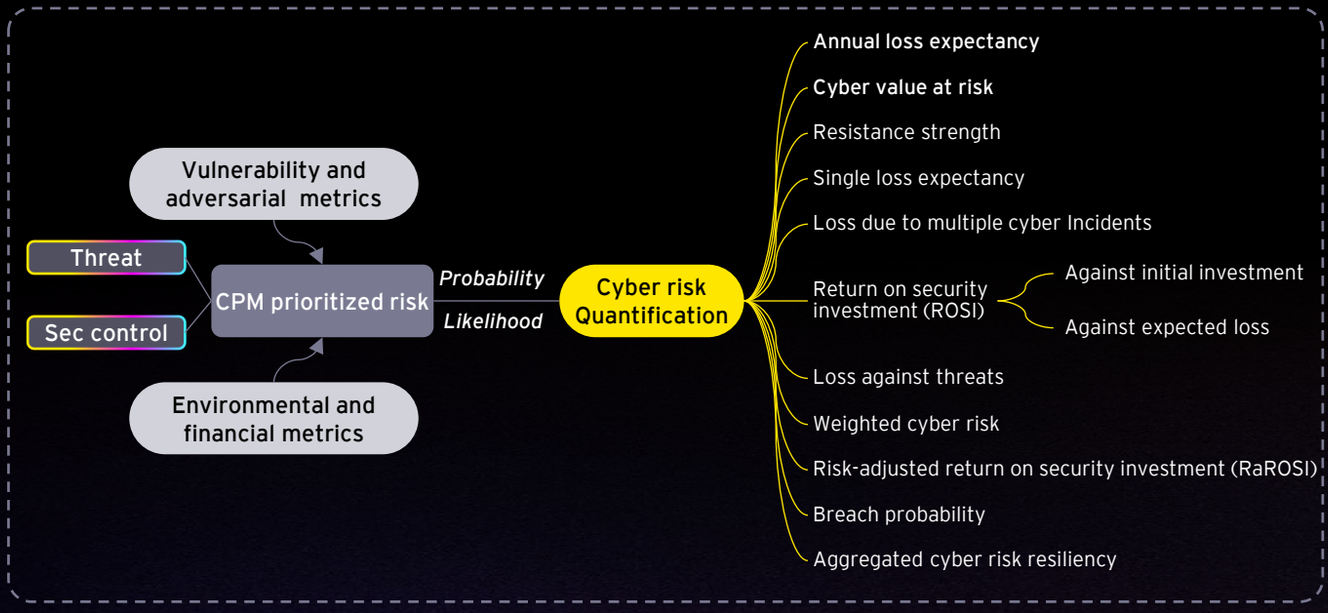
Quantitative risk: *Cyber Risk Quantification (CRQ)*

Quantitative Risk & Financial Metrics

- **Annual Loss Expectancy (ALE):** Estimate expected annual losses by combining incident frequency with financial impact.
- **Cyber Value at Risk (CVaR):** Model worst-case scenarios using probabilistic simulations (95th percentile loss).
- **Return on Security Investment (ROSI):** Calculate ROI by comparing risk reduction against control costs.
- **Risk-adjusted return on capital (RaROC):** Align security spending with corporate capital efficiency.

Benefits

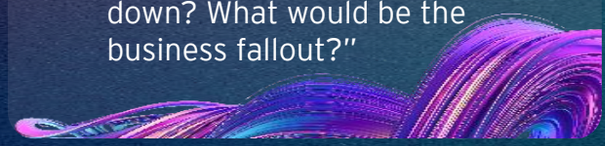
- Justify cybersecurity budgets with rigorous dollar-based models.
- Compare "invest US$1million here vs. US$2 million there" in terms of risk reduction.
- Demonstrate CFO-friendly metrics for boardroom visibility.



- **Business Context:** Map assets to business functions (sales, R&D, supply chain).
- **Operational Criticality:** Assign risk categories based on uptime requirements, SLA commitments.
- **Reputational & Regulatory Exposure:** Qualitative narratives for brand damage, customer trust, and compliance fines.
- **Risk Appetite & Tolerance Levels:** Executive-defined thresholds ("Acceptable residual risk = 2% of annual revenue").

Benefits

- Bridge the gap between technical vulnerabilities and executive priorities.
- Provide "storytelling" dashboards for board members and C-suite.
- Support "what-if" scenarios: "What if this critical system goes down? What would be the business fallout?"



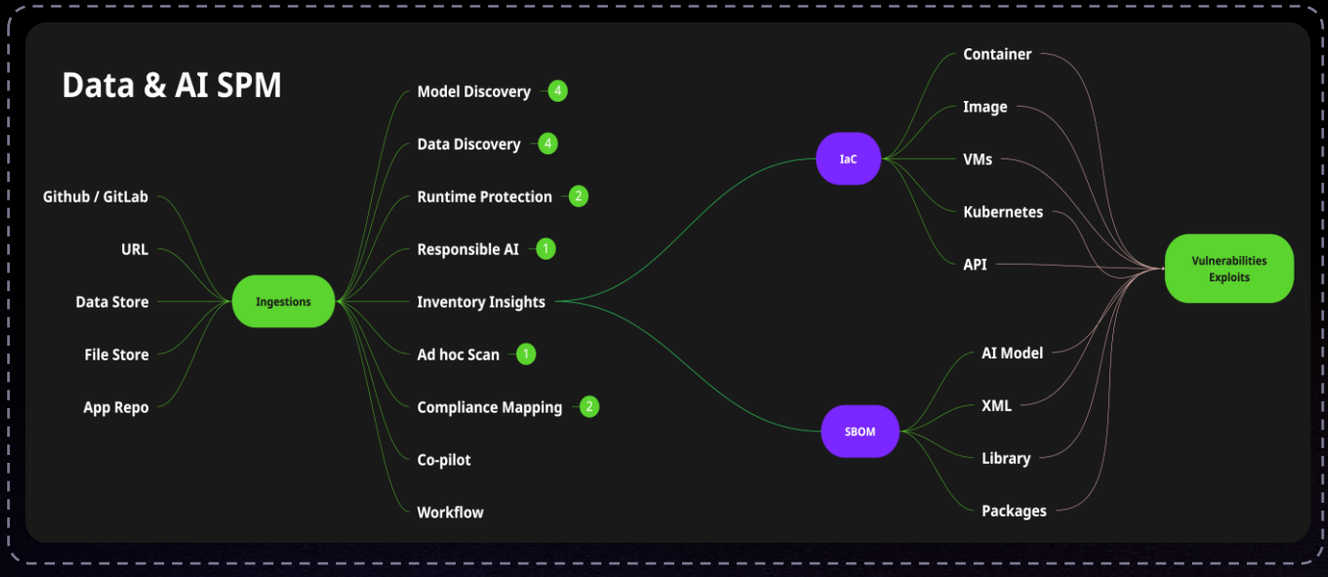
Data and AI *Risk Security Posture Management (AI & R SPM)*

Enterprise Data Security

- **Sensitive Data Discovery & PII Redaction:** Always-on scans across stores and streams; auto-redacts PII before it hits prompts, logs, or analytics.
- **Access Governance & Secrets Hygiene:** Zero-trust, least-privilege policies with repo/CI secret scanning, auto key rotation, and field-level encryption.
- **Context-Aware DLP for LLMs:** Inline guardrails prevent sensitive prompt/response leakage, block outbound data exfil, and trigger instant remediation.

Benefits

- Data Lineage, Retention & Audit Evidence End2End Lineage from Source to Model.
- automated retention / erasure workflows, & immutable evidence for compliance.
- Demonstrate CTO-friendly metrics for boardroom visibility.



- **Continuous Asset & Shadow AI Control:** Auto-discover models, agents, prompt stores, endpoints, and keys—flag unsanctioned apps before they become risk.
- **Misconfiguration & Exposure Guard** Detect public endpoints, over-privileged tokens, open prompt logs, risky dataset links, and weak runtime settings—then harden to baseline.
- **Drift, Attack-Path & Blast-Radius Analytics:** Track config/permission/model-behavior drift; across data → model → agent

Benefits

- AI Resilience Platform unifies discovery, testing, and governance across every model, dataset, endpoint, and agent.
- Privacy, fairness, and explainability are built-in—PII redaction, differential privacy budgets, bias metrics, and SHAP/LIME insights.
- Aligned to audit-ready to NIST AI RMF, ISO 23894, and EU AI Act.

EY CPM modules

Significant Enhancement On Risk Visibility

Auto-Asset Discovery

Discover your entire asset landscape automatically with confidence

Do you know your unknown?
With auto-asset discovery you gain near real-time visibility across all assets eliminating blind spots and hidden components. The module automatically identifies every assets so your risk management strategy stays accurate, comprehensive and continuously updated.

Inherent Risks on an Asset

Understand the baseline exposure of your assets

What's your true risk exposure?
Our Inherent Risk Assessment module provides an unfiltered view of your assets' vulnerabilities before any controls are applied, helping you make smarter, data-driven decisions right from the start.

Adversarial Risk on an Asset

Focus on malicious actors exploiting your asset vulnerabilities

How proactively you identify low-hanging assets?
Our adversarial risk mapping simulates threats, offering visibility on how attackers might exploit your weaknesses and prepare you for the worst-case scenarios.

Threat vs Control Mapping

Map threats to existing security controls for targeted defense

Are your security controls strong enough?
Threat vs. control mapping allows benchmarking of your defenses; against real-world threats, pinpointing gaps and recommending maximum protection where it is needed the most.

Asset Compromisability, Exploitability and Attack Graphs

Visualize potential attack paths and MTTC

Are you aware, how attacker might breach your environment?
Asset compromisability along with attack graphs; visualize potential attack paths, showing where your defenses are weakest and keeping you pre-informed before an attack happens.

EY CPM Modules

Significant Enhancement On Cyber Risk Visibility

Continuous Threat Exposure Management (CTEM)

Real-time identification and prioritization of cyber exposures

Are you informed on all your digital exposure?
CTEM uncovers and validates vulnerabilities, misconfigurations and attack paths across on your environment. By highlighting critical exposures, it reduces attack surface and helps security teams stay ahead of emerging threats.

Secure configuration and patch management

Remediate and resolve with automation in a single platform

Can you detect configuration drift before attackers do?
Solution continuously hardens enterprise systems with policy-driven configuration baselines, eliminating drift and exposure. Also, automated patch intelligence accelerates remediation of high-risk vulnerabilities, enabling compliance and resilient infrastructure posture.

Cyber Risk Quantification

Translate risk into financial terms for better decision-making

What attack technique / threat will cost you more if compromised?
Our Cyber Risk Quantification module helps translate risks into clear financial terms, giving you the insights you need to prioritize investments and optimize your security budget effectively.

Data and AI Risk Security Posture Management (Data and AI RSPM)

Secure your AI. Protect your data

Struggling to qualify risks across your AI and data ecosystem?
EY Data and AI Risk Security Posture Management provides full-spectrum visibility by monitoring data flows, AI BOMs, model exposure, red-teaming insights, privacy violations, RAI and AI risks delivering real-time clarity on weaknesses and guardrails.

Continuous Controls Management (CCM)

Unified, automated compliance and audit management.

Looking to simplify compliance across multiple regulations?
CCM unifies requirements from the DPDP Act, EU AI Act, NIST and other global standards into a single control library. It automates control mapping, streamlines audits, centralizes evidence and provides real-time insights reducing manual effort and keeping teams audit ready.

EY Cybersecurity Performance Management (CPM)

Murali Rao
Partner and National Leader
Cybersecurity Consulting,
EY India

Shivaprakash Abburu
Partner, TAC & Cyber AI COE Leader
Cybersecurity Consulting,
EY India

Sidharth Sood
Partner, Cyber AI COE
Cybersecurity Consulting,
EY India

B Vijay
Director, Cyber AI COE
Product Leader
Cybersecurity Consulting,
EY India

Reach us

Sidharth.Sood@in.ey.com

B.Vijay@in.ey.com

Enabling Cyber Decision Intelligence

ANALYZE | VISUALIZE | GOVERN

Ernst & Young LLP
EY | Building a better working world

EYIN2511-031
SA1

EY
Shape the future with confidence