Strategy & Metrics (SM) Practice

Domain-Specific Descriptions for AI-Operated Security Programs

HAIAMM Practice: Strategy & Metrics (SM) **Business Function:** Governance
Date: December 18, 2025 **Version:** 1.0

PRACTICE OVERVIEW

Strategy & Metrics (SM) is a foundational governance practice that establishes the strategic direction for AI-operated security programs and implements measurement systems to track AI agent effectiveness and security posture improvements.

Based on OWASP SAMM v1.0 Definition:

> *"Strategy & Metrics involves the overall strategic direction of the software assurance program and instrumentation of processes and activities to collect metrics about an organization's security posture."*

HAIAMM Translation:

> *"Strategy & Metrics involves the overall strategic direction of AI-operated security programs and instrumentation of AI agent activities to collect metrics about an organization's security posture across all domains."*

DOMAIN-SPECIFIC DESCRIPTIONS

1. STRATEGY & METRICS - SOFTWARE DOMAIN

SM.Software - AI-Operated Application Security Strategy & Metrics

Domain Focus: Software applications, code repositories, APIs, web applications, mobile applications, microservices

Practice Description:

Strategy & Metrics for the Software domain involves the **overall strategic direction of the AI-operated application security program** and **instrumentation of AI agent activities** to collect metrics about an organization's software security posture.

This practice establishes how organizations define strategic goals for AI agents performing software security work (code analysis, vulnerability scanning, secure code review, application testing), align AI security operations with business objectives, and measure the effectiveness of AI-driven software security activities.

Core Questions This Practice Answers:

- **Strategy:** What is our strategic vision for using AI agents to secure our software applications?
- **Alignment:** How do AI software security operations align with business risk and development velocity?
- **Metrics:** How do we measure whether AI agents are improving our application security posture?
- **ROI:** What value are AI security agents delivering to our software development lifecycle?

What AI Agents Do in This Domain:

- **AI Code Scanners:** Analyze source code for vulnerabilities (SAST)
- **AI Dependency Analyzers:** Scan libraries for known CVEs (SCA)
- **AI Security Reviewers:** Review code commits for security issues
- **AI Penetration Testers:** Test applications for exploitable vulnerabilities (DAST)
- **AI API Security Analyzers:** Monitor API endpoints for misconfigurations and attacks

Strategic Objectives Examples:

- Reduce application vulnerabilities by 50% using AI-driven static analysis
- Achieve <1% false positive rate from AI code security scanners
- Ensure AI agents scan 100% of code commits before production deployment
- Align AI security testing with OWASP Top 10 and business-critical applications
- Measure AI agent contribution to secure software delivery velocity

Key Metrics Examples:

Metric Category	Examples
Effectiveness	Vulnerabilities detected by AI agents, True positive rate, Critical vulns found per 1000 LOC
Coverage	% of repositories scanned by AI, % of code commits reviewed by AI, API endpoints monitored
Efficiency	Time to detect vulnerabilities, Cost per vulnerability found, Developer remediation time
Quality	False positive rate, False negative rate (validated by penetration testing)
Business Impact	Security incidents prevented, Production security bugs reduced, Compliance violations avoided

Maturity Progression:

- **Level 1:** Ad-hoc AI tool deployment; basic metrics (# of vulns found)
- **Level 2:** Defined AI scanning strategy aligned with SDLC; metrics tracked consistently
- **Level 3:** AI security strategy integrated with business objectives; predictive metrics and continuous optimization

Example Strategy Statement:

> *"Our AI-operated software security strategy is to achieve zero high-severity vulnerabilities in production by deploying AI security agents at every stage of the SDLC. We measure success through vulnerability detection rates, remediation velocity, and reduction in security incidents. AI agents must*

> *scan 100% of code commits with <2% false positive rate, enabling developers to ship secure code faster."*

---

2. STRATEGY & METRICS - INFRASTRUCTURE DOMAIN

SM.Infrastructure - AI-Operated Infrastructure Security Strategy & Metrics

Domain Focus: Cloud platforms (AWS/Azure/GCP), containers, Kubernetes, servers, networks, virtualization, IaC (Infrastructure as Code)

Practice Description:

Strategy & Metrics for the Infrastructure domain involves the **overall strategic direction of the AI-operated infrastructure security program** and **instrumentation of AI agent activities** to collect metrics about an organization's infrastructure security posture.

This practice establishes how organizations define strategic goals for AI agents performing infrastructure security work (configuration hardening, network monitoring, cloud security posture management, infrastructure-as-code security), align AI security operations with infrastructure reliability and scalability objectives, and measure the effectiveness of AI-driven infrastructure security activities.

Core Questions This Practice Answers:

- **Strategy:** What is our strategic vision for using AI agents to secure our infrastructure?
- **Alignment:** How do AI infrastructure security operations support business continuity and cloud migration?

- **Metrics:** How do we measure whether AI agents are reducing infrastructure attack surface?
- **ROI:** What value are AI security agents delivering to our infrastructure operations?

What AI Agents Do in This Domain:

- **AI Cloud Security Posture Management (CSPM):** Detect misconfigurations in AWS/Azure/GCP
- **AI Infrastructure Hardening Agents:** Enforce CIS Benchmarks and security baselines
- **AI Network Monitoring Agents:** Detect anomalous traffic patterns and lateral movement
- **AI Container Security Agents:** Scan Docker images for vulnerabilities and enforce runtime policies
- **AI IaC Security Scanners:** Analyze Terraform/CloudFormation for security issues

Strategic Objectives Examples:

- Achieve 100% cloud infrastructure compliance with CIS Benchmarks using AI CSPM
- Reduce infrastructure misconfigurations by 80% through AI-driven monitoring
- Ensure AI agents detect and remediate critical infrastructure vulns within 24 hours
- Align AI infrastructure security with zero-trust architecture principles
- Measure AI agent contribution to infrastructure resilience and availability

Key Metrics Examples:

Metric Category	Examples
Effectiveness	Misconfigurations detected, Critical infrastructure vulns found, Unauthorized access attempts blocked
Coverage	% of cloud accounts monitored, % of servers hardened, Network segments monitored by AI
Efficiency	Mean time to detect infrastructure issues, Mean time to remediate, Cost per misconfiguration fixed
Quality	False positive rate for network alerts, False negative rate (validated by red team)
Business Impact	Infrastructure downtime prevented, Compliance violations avoided, Breach attempts stopped

Maturity Progression:

- **Level 1:** Basic AI monitoring deployed; reactive metrics (alerts generated)
- **Level 2:** Proactive AI hardening strategy; metrics aligned with infrastructure teams
- **Level 3:** AI-driven infrastructure security integrated with DevOps/SRE; predictive threat metrics

Example Strategy Statement:

> *"Our AI-operated infrastructure security strategy is to maintain continuous compliance with zero-trust principles across all cloud and on-premises infrastructure. We measure success through misconfiguration detection rates, infrastructure hardening coverage, and prevented security incidents.*

> *AI agents must monitor 100% of cloud resources with automated remediation of critical issues within 1 hour."*

---

3. STRATEGY & METRICS - ENDPOINTS DOMAIN

SM.Endpoints - AI-Operated Endpoint Security Strategy & Metrics

Domain Focus: Laptops, desktops, mobile devices, IoT devices, workstations, BYOD devices

Practice Description:

Strategy & Metrics for the Endpoints domain involves the **overall strategic direction of the AI-operated endpoint security program** and **instrumentation of AI agent activities** to collect metrics about an organization's endpoint security posture.

This practice establishes how organizations define strategic goals for AI agents performing endpoint security work (endpoint detection and response, device compliance monitoring, mobile threat defense, behavioral analysis), align AI security operations with workforce productivity and remote work enablement, and measure the effectiveness of AI-driven endpoint security activities.

Core Questions This Practice Answers:

- **Strategy:** What is our strategic vision for using AI agents to secure endpoints across our workforce?
- **Alignment:** How do AI endpoint security operations balance security with user productivity?
- **Metrics:** How do we measure whether AI agents are protecting against endpoint compromises?

- **ROI:** What value are AI security agents delivering to our endpoint management?

What AI Agents Do in This Domain:

- **AI Endpoint Detection & Response (EDR):** Detect malware, ransomware, and anomalous endpoint behavior
- **AI Device Compliance Agents:** Enforce device security policies (encryption, patching, antivirus)
- **AI Mobile Threat Defense:** Protect mobile devices from app-based and network-based threats
- **AI User Behavior Analytics (UBA):** Detect compromised credentials and insider threats
- **AI Patch Management Agents:** Identify vulnerable endpoints and automate patching

Strategic Objectives Examples:

- Achieve 99% endpoint malware detection rate using AI EDR agents
- Ensure 100% endpoint compliance with security policies through AI monitoring
- Reduce endpoint security incident response time from hours to minutes with AI automation
- Align AI endpoint security with remote workforce enablement and BYOD policies
- Measure AI agent contribution to reducing endpoint-based breaches

Key Metrics Examples:

Metric Category	Examples
Effectiveness	Malware detections, Ransomware attempts blocked, Compromised credentials identified
Coverage	% of endpoints protected by AI EDR, % of devices compliant with policies, Mobile devices monitored
Efficiency	Mean time to detect endpoint compromise, Mean time to contain threat, Cost per endpoint protected
Quality	False positive rate for endpoint alerts, False negative rate (validated by penetration testing)
Business Impact	Ransomware attacks prevented, Data exfiltration attempts stopped, Compliance violations avoided

Maturity Progression:

- **Level 1:** Basic AI antivirus/EDR deployed; reactive metrics (threats detected)
- **Level 2:** Comprehensive AI endpoint monitoring strategy; proactive threat hunting metrics
- **Level 3:** AI-driven autonomous endpoint protection; predictive compromise detection and auto-remediation

Example Strategy Statement:

> *"Our AI-operated endpoint security strategy is to protect 100% of corporate and BYOD endpoints from malware, ransomware, and insider threats through autonomous AI agents. We measure success through threat detection rates, endpoint compliance levels, and incident response speed.*

> *AI agents must detect endpoint compromises within 5 minutes and contain threats automatically with <0.5% false positive rate."*

---

4. STRATEGY & METRICS - DATA DOMAIN

SM.Data - AI-Operated Data Security Strategy & Metrics

Domain Focus: Databases, data lakes, file storage, cloud storage (S3, Blob), data warehouses, sensitive information (PII, PHI, CUI)

Practice Description:

Strategy & Metrics for the Data domain involves the **overall strategic direction of the AI-operated data security program** and **instrumentation of AI agent activities** to collect metrics about an organization's data security posture.

This practice establishes how organizations define strategic goals for AI agents performing data security work (data classification, access monitoring, data loss prevention, encryption enforcement, data exfiltration detection), align AI security operations with data governance and privacy regulations, and measure the effectiveness of AI-driven data security activities.

Core Questions This Practice Answers:

- **Strategy:** What is our strategic vision for using AI agents to protect sensitive data?
- **Alignment:** How do AI data security operations support privacy compliance (GDPR, HIPAA, CCPA)?
- **Metrics:** How do we measure whether AI agents are preventing data breaches and unauthorized access?

- **ROI:** What value are AI security agents delivering to our data protection program?

What AI Agents Do in This Domain:

- **AI Data Classification Agents:** Auto-classify data as PII, PHI, CUI, confidential, public
- **AI Data Loss Prevention (DLP):** Monitor and block unauthorized data transfers
- **AI Data Access Monitoring:** Detect anomalous database queries and file access patterns
- **AI Encryption Enforcement Agents:** Ensure data-at-rest and data-in-transit encryption
- **AI Data Exfiltration Detectors:** Identify suspicious data movement to external destinations

Strategic Objectives Examples:

- Achieve 100% classification of sensitive data using AI classification agents
- Reduce data breach risk by 90% through AI-driven DLP and access monitoring
- Ensure 100% encryption of CUI/PII data enforced by AI agents
- Align AI data security with GDPR, HIPAA, and NIST SP 800-171 requirements
- Measure AI agent contribution to preventing data exfiltration incidents

Key Metrics Examples:

Metric Category	Examples
Effectiveness	Data exfiltration attempts blocked, Unauthorized access events detected, Unencrypted sensitive data found

Metric Category	Examples
Coverage	% of data classified by AI, % of databases monitored, % of sensitive data encrypted
Efficiency	Time to detect data access anomalies, Time to remediate unencrypted data, Cost per GB of data protected
Quality	False positive rate for DLP alerts, False negative rate (validated by red team data exfiltration tests)
Business Impact	Data breaches prevented, Privacy violations avoided, Regulatory fines prevented

Maturity Progression:

- **Level 1:** Basic AI DLP deployed; reactive metrics (data transfer blocks)
- **Level 2:** Comprehensive AI data classification and monitoring strategy; proactive anomaly detection
- **Level 3:** AI-driven autonomous data protection; predictive data breach prevention and auto-remediation

Example Strategy Statement:

> *"Our AI-operated data security strategy is to achieve zero unauthorized access to sensitive data (PII, PHI, CUI) through autonomous AI classification, monitoring, and protection agents. We measure success through data classification coverage, exfiltration prevention rates, and compliance with privacy regulations. AI agents must classify 100% of new*

> *data within 24 hours and block unauthorized data transfers with <1% false positive rate."*

---

5. STRATEGY & METRICS - PROCESSES DOMAIN

SM.Processes - AI-Operated Security Process Strategy & Metrics

Domain Focus: Security workflows, incident response, compliance monitoring, policy enforcement, security training, GRC (Governance, Risk, Compliance)

Practice Description:

Strategy & Metrics for the Processes domain involves the **overall strategic direction of the AI-operated security process program** and **instrumentation of AI agent activities** to collect metrics about an organization's security process effectiveness and maturity.

This practice establishes how organizations define strategic goals for AI agents performing security process work (incident detection and response, compliance monitoring, policy violation detection, security training delivery, risk assessments), align AI security operations with governance and compliance objectives, and measure the effectiveness of AI-driven security process automation.

Core Questions This Practice Answers:

- **Strategy:** What is our strategic vision for using AI agents to automate and improve security processes?
- **Alignment:** How do AI process automation operations support compliance and governance objectives?
- **Metrics:** How do we measure whether AI agents are improving security process efficiency and effectiveness?

- **ROI:** What value are AI security agents delivering to our GRC and incident response programs?

What AI Agents Do in This Domain:

- **AI Incident Response Orchestration:** Automate incident detection, triage, and initial response
- **AI Compliance Monitoring Agents:** Continuously assess compliance with SOC 2, ISO 27001, NIST, PCI-DSS
- **AI Policy Enforcement Agents:** Detect policy violations and trigger remediation workflows
- **AI Security Training Agents:** Deliver personalized security awareness training and phishing simulations
- **AI Risk Assessment Agents:** Identify and score security risks across the organization

Strategic Objectives Examples:

- Reduce incident response time from hours to minutes using AI orchestration
- Achieve 100% continuous compliance monitoring with AI agents (vs. annual audits)
- Automate 80% of routine security process tasks through AI agents
- Align AI process automation with audit and regulatory reporting requirements
- Measure AI agent contribution to reducing security process overhead and manual work

Key Metrics Examples:

Metric Category	Examples
Effectiveness	

Metric Category	Examples
	Incidents detected and responded to, Compliance violations identified, Policy violations detected
Coverage	% of security processes automated, % of compliance controls monitored continuously, % of staff trained
Efficiency	Mean time to detect incidents, Mean time to respond, Cost per compliance control assessed
Quality	False positive rate for compliance alerts, Incident response accuracy, Training effectiveness scores
Business Impact	Audit findings reduced, Regulatory compliance maintained, Security process costs reduced

Maturity Progression:

- **Level 1:** Basic AI monitoring for incidents; manual metrics collection
- **Level 2:** AI-driven incident response playbooks; automated compliance dashboards
- **Level 3:** Fully automated AI security processes; predictive risk analytics and proactive remediation

Example Strategy Statement:

> *"Our AI-operated security process strategy is to automate 80% of routine security workflows (incident response, compliance monitoring, policy enforcement) through autonomous AI agents, enabling the security team to focus on strategic initiatives. We measure success through process*

> *automation coverage, incident response speed, and continuous compliance scores. AI agents must detect security incidents within 5 minutes and maintain 100% real-time compliance visibility."*

---

6. STRATEGY & METRICS - VENDORS DOMAIN

SM.Vendors - AI-Operated Vendor Security Strategy & Metrics

Domain Focus: Third-party vendors, suppliers, cloud service providers, software vendors, outsourced services, supply chain partners

Practice Description:

Strategy & Metrics for the Vendors domain involves the **overall strategic direction of the AI-operated vendor security program** and **instrumentation of AI agent activities** to collect metrics about an organization's third-party risk and supply chain security posture.

This practice establishes how organizations define strategic goals for AI agents performing vendor security work (vendor risk assessments, continuous vendor monitoring, supply chain threat detection, contract compliance verification), align AI security operations with supply chain resilience and third-party risk management objectives, and measure the effectiveness of AI-driven vendor security activities.

Core Questions This Practice Answers:

- **Strategy:** What is our strategic vision for using AI agents to manage third-party and supply chain security risks?
- **Alignment:** How do AI vendor security operations support supply chain resilience and business continuity?

- **Metrics:** How do we measure whether AI agents are reducing third-party security risks?
- **ROI:** What value are AI security agents delivering to our vendor risk management program?

What AI Agents Do in This Domain:

- **AI Vendor Risk Assessment Agents:** Automate initial and ongoing vendor security assessments
- **AI Supply Chain Monitoring Agents:** Detect vendor security incidents, breaches, and compromises
- **AI Contract Compliance Agents:** Verify vendors meet security SLAs and contractual obligations
- **AI Software Supply Chain Scanners:** Detect malicious code in third-party libraries and dependencies
- **AI Vendor Security Scorecard Agents:** Continuously score vendor security posture

Strategic Objectives Examples:

- Achieve 100% vendor security assessment coverage using AI automation
- Reduce vendor security incident impact through AI-driven continuous monitoring
- Ensure all critical vendors maintain security scores >80/100 via AI scorecards
- Align AI vendor security with NIST SR (Supply Chain Risk Management) family requirements
- Measure AI agent contribution to preventing supply chain attacks

Key Metrics Examples:

Metric Category	Examples
Effectiveness	Vendor security incidents detected, Supply chain compromises identified, Non-compliant vendors flagged
Coverage	% of vendors assessed by AI, % of critical vendors monitored continuously, % of vendor contracts reviewed
Efficiency	Time to complete vendor assessments, Cost per vendor assessed, Vendor onboarding time
Quality	False positive rate for vendor alerts, Vendor security score accuracy, Risk prediction accuracy
Business Impact	Supply chain attacks prevented, Vendor-caused incidents reduced, Third-party compliance maintained

Maturity Progression:

- **Level 1:** Basic AI vendor questionnaires; manual metrics (vendors assessed per quarter)
- **Level 2:** Automated AI vendor risk monitoring; continuous vendor security scoring
- **Level 3:** Predictive AI supply chain threat detection; autonomous vendor risk mitigation

Example Strategy Statement:

> *"Our AI-operated vendor security strategy is to achieve continuous visibility into the security posture of all third-party vendors and supply chain partners through autonomous AI monitoring and risk scoring. We measure success*

> *through vendor assessment coverage, continuous monitoring adoption, and supply chain incident prevention. AI agents must assess 100% of new vendors within 48 hours and monitor critical vendors 24/7 with real-time risk alerts."*

SUMMARY TABLE: SM PRACTICE ACROSS DOMAINS

Domain	Strategic Focus	AI Agent Activities	Key Metrics Examples
Software	AI-operated application security strategy	Code scanning, vulnerability detection, secure code review	Vulnerabilities detected, false positive rate, code coverage
Infrastructure	AI-operated infrastructure security strategy	CSPM, network monitoring, infrastructure hardening	Misconfigurations found, infrastructure coverage, MTTR
Endpoints	AI-operated endpoint security strategy	EDR, device compliance, behavioral analysis	Malware detections, endpoint coverage, compromise detection time
Data	AI-operated data protection strategy	Data classification,	Data classified, exfiltration attempts

Domain	Strategic Focus	AI Agent Activities	Key Metrics Examples
		DLP, access monitoring	blocked, encryption coverage
Processes	AI-operated security process automation strategy	Incident response, compliance monitoring, policy enforcement	Incidents detected, compliance score, process automation %
Vendors	AI-operated vendor risk management strategy	Vendor assessments, supply chain monitoring, risk scoring	Vendor assessment coverage, security scores, supply chain incidents

CROSS-DOMAIN STRATEGIC THEMES

Theme 1: Alignment with Business Objectives All domains must align AI security strategy with business goals (velocity, resilience, compliance, cost reduction)

Theme 2: Metrics-Driven Decision Making All domains require quantifiable metrics to demonstrate AI agent effectiveness and ROI

Theme 3: Coverage and Completeness All domains strive for comprehensive coverage (100% of code, infrastructure, endpoints, data, processes, vendors)

Theme 4: Continuous Improvement All domains establish baseline metrics and track improvement over time (maturity progression)

Theme 5: Balance Automation and Human Oversight All domains must balance AI autonomy with human strategic direction and validation

---

USING THESE DESCRIPTIONS

For HAIAMM Assessments: These descriptions provide context for Strategy & Metrics questions in each domain assessment.

For Organizations: Use these descriptions to define your domain-specific AI security strategies and select appropriate metrics.

For Assessors: Reference these descriptions when evaluating organizational maturity in Strategy & Metrics practice.

For Tool Development: Use these descriptions to generate domain-specific Strategy & Metrics questions in the HAIAMM assessment tool.

Document Version: 1.0 **Last Updated:** December 18, 2025 **Next:** Create similar one-pagers for remaining 11 HAIAMM practices (PC, EG, TA, SR, SA, DR, CR, ST, EH, ML, IM)

Related Documents: - HAIAMM Fundamental Controls Maturity Roadmap - NIST-DFARS-CMMC Alignment Analysis