Strategy & Metrics (SM) Practice Descriptions

HAIAMM Domain-Specific Context

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

PRACTICE OVERVIEW

Based on OWASP SAMM v1.0:

> *"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 DESCRIPTIONS

1. SOFTWARE DOMAIN

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

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—including code analysis, vulnerability scanning, secure code review, and application testing—align those AI security operations with business objectives, and measure the effectiveness of AI-driven software security activities across the software development lifecycle.

---

2. INFRASTRUCTURE DOMAIN

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

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—including configuration hardening, network monitoring, cloud security posture management, and infrastructure-as-code security—align those AI security operations with infrastructure reliability and scalability objectives, and measure the effectiveness of AI-driven infrastructure security activities.

---

3. ENDPOINTS DOMAIN

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

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—including endpoint detection and response, device compliance monitoring, mobile threat defense, and behavioral analysis—align those AI security operations with workforce productivity and remote work enablement objectives, and measure the effectiveness of AI-driven endpoint security activities.

---

4. DATA DOMAIN

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

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—including data classification, access monitoring, data loss prevention, encryption enforcement, and data exfiltration detection—align those AI security operations with data governance and privacy regulations, and measure the effectiveness of AI-driven data security activities.

---

5. PROCESSES DOMAIN

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

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—including incident detection and response, compliance monitoring, policy violation detection, security training delivery, and risk assessments—align those AI security operations with governance and compliance objectives, and measure the effectiveness of AI-driven security process automation.

---

6. VENDORS DOMAIN

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

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—including vendor risk assessments, continuous vendor monitoring, supply chain threat detection, and contract compliance verification—align those AI security operations with supply chain resilience and third-party risk management objectives, and measure the effectiveness of AI-driven vendor security activities.

Document Version: 1.0 **Last Updated:** December 18, 2025 **Purpose:** Provide concise domain-specific descriptions of Strategy & Metrics practice for HAIAMM assessments