# Strategy & Metrics (SM) - Domain Descriptions

**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 Context:** 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.

| Domain | Description |
|---|---|
| **Software** | Involves the strategic direction of AI-operated application security programs and instrumentation of AI agent activities (code analysis, vulnerability scanning, secure code review, application testing) to collect metrics about software security posture. Aligns AI security operations with business objectives and measures effectiveness of AI-driven software security activities across the SDLC. |
| **Infrastructure** | Involves the strategic direction of AI-operated infrastructure security programs and instrumentation of AI agent activities (configuration hardening, network monitoring, cloud security posture management, IaC security) to collect metrics about infrastructure security posture. Aligns AI operations with infrastructure reliability and scalability objectives. |
| **Endpoints** | Involves the strategic direction of AI-operated endpoint security programs and instrumentation of AI agent activities (EDR, device compliance monitoring, mobile threat defense, behavioral analysis) to collect metrics about endpoint security posture. Aligns AI operations with workforce productivity and remote work enablement objectives. |
| **Data** | Involves the strategic direction of AI-operated data security programs and instrumentation of AI agent activities (data classification, access monitoring, DLP, encryption enforcement, exfiltration detection) to collect metrics about data security posture. Aligns AI operations with data governance and privacy regulations. |
| **Processes** | Involves the strategic direction of AI-operated security process programs and instrumentation of AI agent activities (incident response, compliance monitoring, policy enforcement, security training, risk assessments) to collect metrics about security process effectiveness and maturity. Aligns AI operations with governance and compliance objectives. |
| **Vendors** | Involves the strategic direction of AI-operated vendor security programs and instrumentation of AI agent activities (vendor risk assessments, continuous monitoring, supply chain threat detection, contract compliance verification) to collect metrics about third-party risk and supply chain security posture. Aligns AI operations with supply chain resilience and third-party risk management objectives. |