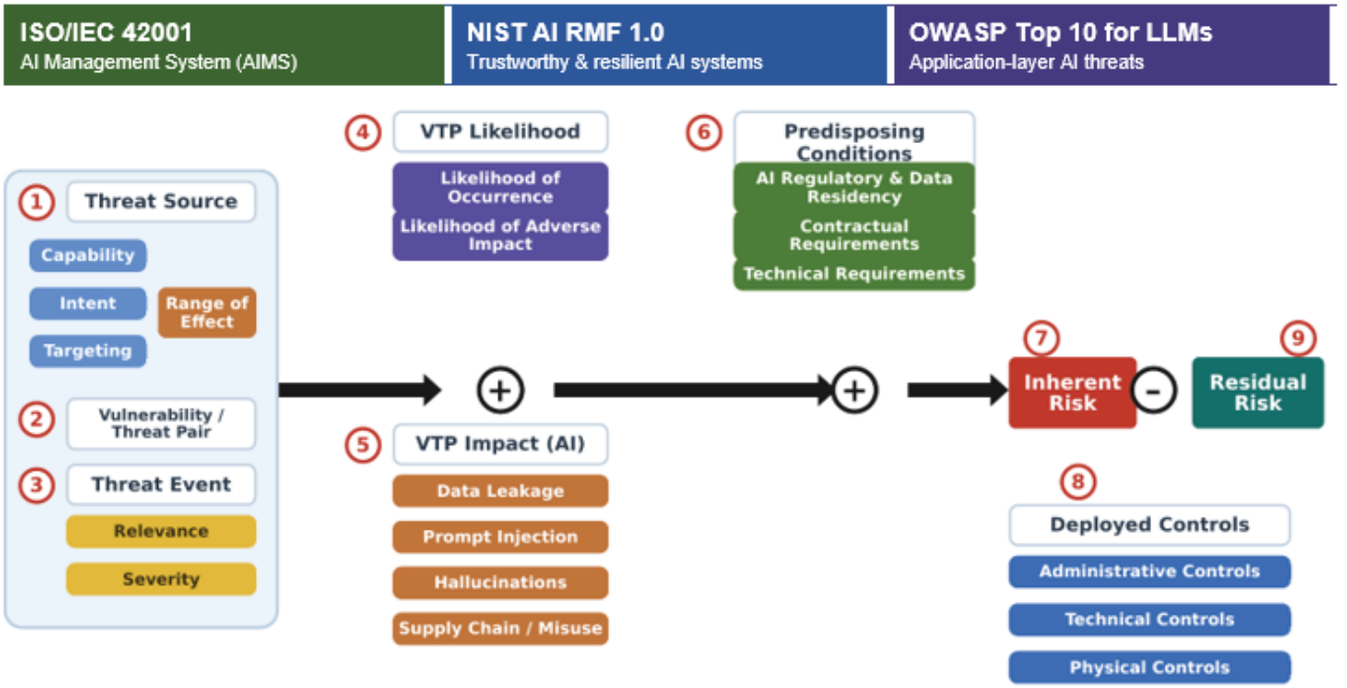
SHIELDRisk AI
Product Suite

INTENT

CTI's SHIELDRisk AI extends our proven SHIELDRisk methodology to the unique risks introduced by Artificial Intelligence (AI) agentic systems, Large Language Models (LLMs), and Generative AI. As executive leaders adopt these technologies, SHIELDRisk AI helps organizations identify, analyze, and document an acceptable risk posture for the data flows, business functions, and processes that AI touches. Each engagement delivers up to fifty (50) Vulnerability-Threat Pair (VTP) scenarios tailored to the deployment and integration of LLMs and Generative AI, with a specific focus on prompt injection, data leakage, and supply chain vulnerabilities. Assessments are governed by NIST SP 800-30, 37, and 39 and FIPS 200, and are mapped to the leading AI trust frameworks so leadership can align AI operations with an acceptable risk tolerance and build a defensible security roadmap.

PROCESS MAP



SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION

CTI| 1 Texas Station Court, Suite 325, Timonium, MD 21093 | www.webcti.com | 800-606-6060 | info@webcti.com

SHIELDRisk AI Product Suite

PROCESS SUMMARY

1. Create Vulnerability / Threat Pairs (VTPs) – CTI consultants develop up to fifty (50) VTP scenarios tailored to the organization's AI footprint, including the specific LLM and Generative AI models in use, the third-party platforms and API endpoints supporting them, and the corporate data those systems ingest or generate. Threats unique to AI – such as prompt injection, data leakage, and supply chain compromise – are combined with observed vulnerabilities to create focused, business-relevant VTPs.

2. VTP Likelihood – For each VTP, consultants evaluate the likelihood that the AI-related vulnerability will be exploited and adversely affect the organization, weighing threat-source capability and intent, the nature of the vulnerability, and the existence and effectiveness of current controls.

3. VTP Impact – CTI estimates the full spectrum and degree of impact a realized AI risk would have on operations, assets, individuals, other organizations, and the public – including exposure of sensitive corporate IP, regulatory and confidentiality violations, and erosion of trust from inaccurate or manipulated model output.

4. Inherent Risk Calculation – Documented Likelihood and Impact are combined to calculate the Inherent Risk for each scenario. Predisposing conditions – such as AI-specific regulatory obligations, data residency laws, and contractual requirements – are factored in where they further elevate risk.

5. Residual Risk Calculation – Consultants review the administrative, technical, and physical controls currently deployed around the AI systems and estimate their effectiveness in reducing likelihood and impact. From this, a residual risk level is discerned, prioritized, and presented to the customer with a comprehensive mitigation strategy for review and further risk treatment.

ADD-ON COMPONENTS (OPTIONAL)

1. Business Impact Analysis (AI)

- Define up to five (5) departments or business processes and their specific AI use cases.
- Interview department heads to understand how AI influences each workflow and the corporate data that supports it.
- Document the specific AI models (e.g., Claude, ChatGPT, Copilot), third-party platforms, and cloud-based API endpoints supporting each process.
- Identify the potential impact of AI vulnerabilities (e.g., prompt injection, hallucinations) on critical business functions.
- Capture legal and regulatory requirements, including AI data residency laws, and establish RTO, RPO, and maximum allowable downtime.

2. Data Classification (AI)

- Classify the data ingested by and generated by AI systems in accordance with the organization's Data Classification Policy.
- Identify where AI-interfacing data resides, using the Business Impact Analysis as a foundation.
- Ensure sensitive corporate IP is not inadvertently used in a way that violates compliance or confidentiality.

GOVERNING FRAMEWORK

SHIELDRisk AI evaluates threats and vulnerabilities against the frameworks purpose-built for artificial intelligence: **ISO/IEC 42001** for establishing an AI Management System (AIMS), the **NIST AI Risk Management Framework (RMF 1.0)** for trustworthy and resilient AI, and the **OWASP Top 10 for LLM Applications** for application-layer AI threats – all anchored to NIST SP 800-30, 37, 39 and FIPS 200.

SHIELD

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION