ASI-VSS

Vulnerability Scoring Standard v1.0

Carrier Brief

Why AI Risk Defies Traditional Underwriting

Cyber insurance was built for network intrusions and data breaches — deterministic events with historical actuarial data. A ransomware payload either deploys or it does not; a data breach either exposes records or it does not. The loss models underpinning most cyber policies assume bounded, classifiable events with precedent. AI systems violate every one of these assumptions.

Modern AI deployments introduce non-deterministic risk at an entirely different order of magnitude. Autonomous agents can cascade failures across enterprises in minutes, making loss containment nearly impossible once a compromise is underway. Model poisoning corrupts decision-making at scale — silently and persistently — before any loss event is visible. Attack vectors such as prompt injection, RAG poisoning, and Model Context Protocol (MCP) exploits have no meaningful loss history, leaving actuaries without the data required for credible pricing.

The most acute challenge for carriers is scoring granularity. Without a purpose-built vulnerability scoring standard, underwriters cannot differentiate a prompt injection (VSS 53) from an autonomous agent compromise (VSS 81) — yet the coverage implications differ by orders of magnitude. Business Interruption, Cyber Liability, and D&O exposure can trigger simultaneously in an agent compromise scenario. Traditional CVSS scores compress both events into a 7–9 range, providing no actionable actuarial signal.

> KEY FINDING
> Our incident database reveals that AI-native vulnerability categories — Agent Compromise (avg 80.5), Cascading Agent Failures (avg 80.3), and Memory & Context Poisoning (avg 75.0) — trigger the most severe insurance loss scenarios: Business Interruption, Cyber Liability, and D&O exposure simultaneously. Traditional CVSS scores compress these into the 7–9 range, providing no actuarial signal.

Scoring Architecture for Insurance Decision-Making

ASI-VSS decomposes AI vulnerability severity into five independent dimensions, each scored 0–20, summing to a 0–100 composite. The formula is straightforward:

```
VSS = D1 + D2 + D3 + D4 + D5        (scale: 0 - 100)
```

D4: Enterprise & Financial Impact — Insurance Loss Category Sub-Factor

Dimension 4 is purpose-built for insurance decision-making. Its four sub-factors include quantified financial loss, regulatory and compliance exposure, reputational damage, and — critically — an Insurance Loss Category mapping that translates each scored vulnerability directly to coverage triggers and indicative claim ranges.

Score	Coverage Trigger	Typical Claim Range
5	Business Interruption + Cyber Liability + D&O;	>$50M
4	Cyber Liability + Regulatory Defense	$10M–$50M
3	Cyber Liability + Data Breach Notification	$1M–$10M
2	First-Party Data Recovery	$100K–$1M
1	Incident Response Costs Only	<$100K
0	No insurable loss	—

Severity Tiers and Carrier Implications

Severity Tier	Score Range	Insurance Implication
CRITICAL	85–100	Mandatory carrier notification
SEVERE	70–84	Material risk event — assess coverage
ELEVATED	50–69	Monitored risk — log for renewal
MODERATE	30–49	Standard risk management
LOW	0–19	Informational only

174 Incidents. Real Loss Signals.

ASI-VSS scores are calibrated against 174 analyst-verified AI security incidents collected by our intelligence team from January 2025 through March 2026. Each incident was independently scored by our analysts using the full sub-factor rubrics, with disagreements resolved through structured adjudication. For carriers, this dataset represents the first empirical foundation for AI vulnerability pricing.

DATASET DISTRIBUTION

Score Range	Mean Score	Std Dev	Critical	Severe	Elevated	Moderate
35 – 87	55.3	11.1	2	19	103	50

AIRS Domain Impact — Insurance-Relevant View

AIRS Domain	Code	Avg Score	Incidents	Range
Data Protection	DP	66.9	14	44–85
Third-Party Risk	TPR	59.2	30	38–84
Data Architecture	DA	59.0	55	43–87
Model Risk	MR	57.3	58	47–87
Data Governance	DG	56.1	34	38–81
Model Integrity	MI	55.3	79	35–87
Operational Resilience	OR	54.7	48	35–84
Regulatory Compliance	RC	54.2	37	43–63
Compliance & Legal	CL	48.5	45	35–64

Each AIRS domain maps directly to insurance coverage areas. Data Protection's elevated average (66.9) signals disproportionate cyber liability exposure across the incident dataset. Third-Party Risk (59.2 across 30 incidents) reflects the growing supply chain attack surface that is increasingly difficult to underwrite without empirical benchmarks.

From Vulnerability Scores to Underwriting Decisions

Vulnerability scores provide the empirical risk signal that feeds into our AI Insurance Readiness Score (AIRS) — a composite underwriting assessment across 9 insurance-relevant domains. The integration workflow below describes how carriers can move from raw vulnerability data to actionable underwriting decisions.

Carrier Integration Workflow

1. Score vulnerabilities with ASI-VSS

Apply the 5-dimension sub-factor rubrics to AI system vulnerabilities in the insured portfolio. Each dimension is scored 0–20 by trained analysts; the composite VSS provides a precise, repeatable severity signal.

2. Map D4 sub-factors to coverage triggers

The Insurance Loss Category sub-factor within D4 translates directly to coverage triggers and claim range estimates. Underwriters can extract loss category assignments from scored incidents without additional interpretation.

3. Aggregate by AIRS domain for portfolio assessment

Scored incidents aggregate into our AI Insurance Readiness Score (AIRS) across 9 insurance-relevant domains. Portfolio-level AIRS composites feed directly into underwriting models and pricing engines.

4. Feed AIRS composites into underwriting models

AIRS scores integrate with existing underwriting platforms. Domain scores and composite AIRS provide both granular and summary risk signals compatible with standard pricing architectures.

5. Monitor severity trends and rescore quarterly

The AI threat landscape evolves rapidly. Our analysts recommend rescoring high-severity findings quarterly, or immediately following material changes to model version, tool integrations, or deployment architecture.

AIRS Benefits for Carriers

> AIRS gives carriers what CVSS cannot: portfolio-level AI risk quantification with direct coverage trigger mapping, built on empirical incident data.
>
> - Portfolio-level risk quantification across 9 insurance-relevant domains
> - Standardized risk language across carrier submissions
> - Empirical benchmarking against 174 real-world scored incidents
> - Direct mapping to coverage triggers for claims forecasting

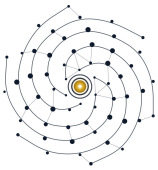
Reinsurance note: Treaty terms can reference AIRS thresholds — for example, requiring cedants to maintain a minimum portfolio-weighted AIRS of 60 to qualify for favorable treaty terms.

Get Started

ASI-VSS v1.0 and the AIRS framework are available to carriers under licensing arrangements suited to organizational scale and underwriting use case. The following resources are available from our intelligence team.

- 1. Access the ASI-VSS Scored Database
  Benchmarking data for 174 incidents with AIRS domain mappings and insurance loss category assignments. Available for actuarial analysis and portfolio risk modeling.
- 2. AIRS Underwriting Integration
  Our intelligence team supports carriers integrating AIRS scoring into existing underwriting platforms. From API-level integration to custom risk models.
- 3. Contact Our Intelligence Team
  Licensing inquiries, actuarial data partnerships, and embedded intelligence arrangements. From single-assessment support to ongoing portfolio monitoring.

> Contact
> info@aisecurityintelligence.com · aisecurityintelligence.com



About AI Security Intelligence LLC

AI Security Intelligence LLC provides the intelligence infrastructure for quantifying AI security risk. Our Vulnerability Scoring Standard, Threat Severity Score, and AI Insurance Readiness Score form an integrated platform serving security practitioners, insurance carriers, and regulators worldwide. Our analysts combine deep expertise in AI systems security, enterprise risk management, and actuarial modeling to deliver intelligence that is both technically rigorous and operationally actionable.