2026

Lasso's Compliance and Threats Mapping

contactus@lasso.security

About This Framework

This document provides a comprehensive mapping of Lasso Security's out-of-the-box and custom policies against the world's leading AI governance frameworks, including OWASP Top 10 , MITRE ATLAS, and NIST.

As AI agents and applications become central to enterprise innovation, navigating the complex landscape of emerging regulations and adversarial threats is a critical business imperative.

Using this mapping, enterprises can:

- **Quantify Compliance Readiness:** Visualize exactly how Lasso's policy engine satisfies specific requirements of global AI regulations.
- **Bridge the Strategy-Execution Gap:** Operationalize the "Map, Measure, and Manage" functions through Lasso's continuous monitoring and automated audit trails.
- **Validate Threat Resilience:** Demonstrate a hardened security posture against the specific TTPs (Tactics, Techniques, and Procedures) identified by MITRE and OWASP by mapping Lasso's detection capabilities to real-world AI attack vectors, from prompt injection to model evasion.

The State of AI Usage

55%

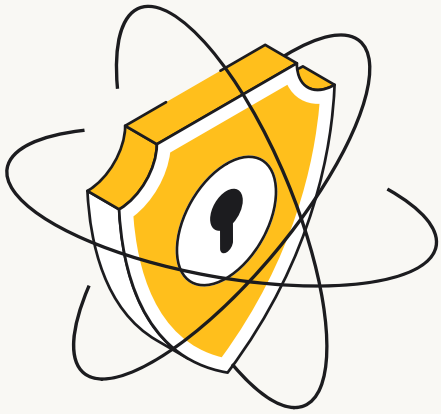
Employees expose network information to LLM tools, increasing the organization's attack surface by revealing internal infrastructure and system topology.

49%

Employees share code with LLM tools, creating a risk of intellectual property leakage and unintended exposure of embedded secrets or business logic.

40%

Employees expose PII to LLM tools, introducing regulatory, privacy, and customer-trust risks.



37%

Employees share safety-related or internal risk information, potentially revealing organizational controls, policies, and security posture.

21%

Employees expose credentials to LLM tools, creating an immediate risk of unauthorized access and account compromise.

16%

Employees share tokens with LLM tools, enabling session hijacking or short-window privilege escalation.

3%

Employees expose PCI data to LLM tools, which - despite low frequency represents a critical compliance and financial risk.

*Based on Lasso's internal research in Q4 2025

Lasso's Compliance and Threats Mapping

Session Token Exposure

Exposure of authentication tokens including session tokens (access and refresh tokens) and API keys that enable unauthorized system access.

OWASP Risk

LLM02 Sensitive Information Disclosure
LLM05 Improper Output Handling

MITRE Atlas

T0055 – Unsecured Credentials
T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party AI or data.

GOVERN 6.2-004:
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4.1
Technical and legal risks of GenAI are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1
Post-deployment monitoring covers feedback, incidents, overrides, changes, and decommissioning.

MANAGE 4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Credential Leakage Attempt

Exposure of authentication credentials including passwords, API keys, SSH keys, private keys, and other secrets used for system authentication and authorization.

OWASP Risk

LLM02 Sensitive Information Disclosure

MITRE Atlas

T0055 – Unsecured Credentials
T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2-004:
Deployed third-party GenAI systems are continuously monitored.

Map:

MAP 4.1
Technical and legal risks of GenAI are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4:
Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.

MANAGE 4.1:
Post-deployment monitoring covers feedback, incidents, overrides, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Lasso's Compliance and Threats Mapping

Personal Data Exposure

Exposure of personally identifiable information including names, addresses, phone numbers, email addresses, social security numbers, and other data that can identify individuals.

OWASP Risk

LLM02 Sensitive Information Disclosure
LLM05 - Improper Output Handling

MITRE Atlas

T0055 – Unsecured Credentials
T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
GOVERN 6.2 Contingency plans address failures or incidents involving high-risk third-party GenAI systems or data.

GOVERN 6.2-004
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4:
Risks and benefits are identified for all AI components, including third parties.

MAP 4.1:
Technical, legal, and IP risks from AI components and third parties are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10:
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4:
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1
Post-deployment monitoring covers feedback, incidents, overrides, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Payment Data Exposure

Exposure of payment card information including card numbers, PAN (Primary Account Number), CVV codes, expiration dates, and cardholder data.

OWASP Risk

LLM02 Sensitive Information Disclosure
LLM05 Improper Output Handling

MITRE Atlas

T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party AI or data.

GOVERN 6.2-004:
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4:
Risks and benefits are identified for all AI components, including third parties.

MAP 4.1:
Technical, legal, and IP risks from AI components and third parties are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10:
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4:
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1:
Post-deployment monitoring covers feedback, incidents, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Lasso's Compliance and Threats Mapping

Government ID Exposure

Exposure of government-issued identification documents and numbers including passport numbers, national identification numbers, driver's license numbers, and immigration documentation.

OWASP Risk

LLM02 Sensitive Information Disclosure

MITRE Atlas

T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party AI or data.

GOVERN 6.2-004:
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4:
Risks and benefits are identified for all AI components, including third parties.

MAP 4.1:
Technical, legal, and IP risks from AI components and third parties are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10:
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4:
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1:
Post-deployment monitoring covers feedback, incidents, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

General Identifier Exposure

Exposure of technical identifiers including UUIDs, VINs (Vehicle Identification Numbers), MAC addresses, device IDs, and other unique system or hardware identifiers.

OWASP Risk

LLM02 Sensitive Information Disclosure
LLM05 - Improper Output Handling

MITRE Atlas

T0055 – Unsecured Credentials
T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party AI or data.

GOVERN 6.2-004:
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4:
Risks and benefits are identified for all AI components, including third parties.

MAP 4.1:
Technical, legal, and IP risks from AI components and third parties are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10:
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4:
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1:
Post-deployment monitoring covers feedback, incidents, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Lasso's Compliance and Threats Mapping

Network And Infrastructure Information Exposure

Exposure of network infrastructure details including internal IP addresses, hostnames, network architecture diagrams, internal endpoints, and system topology information.

OWASP Risk

LLM02 Sensitive Information Disclosure

MITRE Atlas

T0057 – LLM Data Leakage
T0036 – Data from Information Repositories

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party AI or data.

GOVERN 6.2-004:
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4:
Risks and benefits are identified for all AI components, including third parties.

MAP 4.1:
Technical, legal, and IP risks from AI components and third parties are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.10:
Identified privacy risks are assessed and documented.

Manage:

MANAGE 4:
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1:
Post-deployment monitoring covers feedback, incidents, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Source Code Exposure

Exposure of proprietary source code, scripts, algorithms, intellectual property, and implementation details that reveal system logic or business processes.

OWASP Risk

LLM02 Sensitive Information Disclosure
LLM05 - Improper Output Handling

MITRE Atlas

T0055 – Unsecured Credentials
T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party AI or data.

GOVERN 6.2-004:
Deployed third-party AI systems are continuously monitored.

Map:

MAP 4:
Risks and benefits are identified for all AI components, including third parties.

MAP 4.1:
Technical, legal, and IP risks from AI components and third parties are identified and documented.

MAP-4.1-001
AI-generated outputs are monitored for privacy and sensitive data risks.

MAP-4.1-009
Controls are used to detect sensitive data in generated text, images, audio, or video.

Measure:

MEASURE 2.6
The GenAI system is evaluated for safety risks, operates within risk tolerance, and fails safely when limits are exceeded.

MEASURE 2.6-004
GenAI outputs, including generated code, are reviewed for safety and validity.

Manage:

MANAGE 4:
AI risk response, recovery, and communication plans are documented and reviewed.

MANAGE 4.1:
Post-deployment monitoring covers feedback, incidents, changes, and decommissioning.

MANAGE-4.1-002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Lasso's Compliance and Threats Mapping

Harmful And Non-Compliant Content Generation

Generation of harmful, biased, violent, sexual, hateful, illegal, or self-harm-promoting content that violates ethical guidelines, safety policies, or regulatory requirements.

OWASP Risk

LLM04 Data and Model Poisoning
LLM05 Improper Output Handling

MITRE Atlas

T0048 – External Harms
T0048.001 - External Harms: Reputational Harm
T0048.002 – Societal Harm
T0048.003 - External Harms: User Harm
T0065 - LLM Prompt Crafting

NIST

Govern:

GOVERN 1.4:
Risk management processes and outcomes are documented policies aligned to organizational risk priorities.

GOVERN 1.4-001:
Risk measurement plans address known incidents, misuse scenarios, bias risks, and human-AI interaction factors.

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party GenAI systems or data.

GOVERN 6.2-004
Deployed third-party GenAI systems are continuously monitored.

GOVERN 6.2-005
Policies address GenAI data and model artifact redundancy.

Map:

MAP 1.1
Intended use, deployment context, and applicable laws and norms are documented.

MP 1.1-003:
Risk measurement plans address known incidents, misuse scenarios, bias risks, and human-AI interaction factors.

MAP 2.3
Scientific integrity and TEVV considerations are identified and documented.

MAP 5.1
The likelihood and impact of identified benefits and harms are assessed and documented.

MAP 5.1-002
GenAI content provenance risks, including misinformation and deepfakes, are identified and prioritized.

Measure:

MEASURE 2.6
The GenAI system is evaluated for safety risks, operates within risk tolerance, and fails safely when limits are exceeded.

MEASURE 2.6-006
The system properly handles queries that could enable malicious, illegal, or harmful use.

MEASURE 2.6-007
GenAI system vulnerabilities and safety bypass risks are regularly evaluated.

MEASURE 2.10
Identified privacy risks are assessed and documented across the AI system.

MEASURE 2.10-003
Training data deduplication is verified to reduce bias and data homogenization.

Manage:

MANAGE 2.2:
Mechanisms are in place to maintain the value of deployed AI systems.

MANAGE 2.2-005:
GenAI outputs are reviewed for harmful content, misinformation, and high-risk misuse

MANAGE 3.2
Pre-trained models used in development are included in ongoing monitoring.

MANAGE 3.2-005
Content filters prevent the generation of harmful, illegal, or inappropriate GenAI outputs.

MANAGE 4.1
Post-deployment monitoring covers feedback, incidents, overrides, changes, and decommissioning.

MANAGE 4.1-002
002
Post-deployment monitoring addresses GenAI risks, including confabulation and misuse.

Lasso's Compliance and Threats Mapping

Jailbreak Attempt

Attempts to bypass LLM security controls, guardrails, safety filters, content policies, or operational restrictions through adversarial prompting techniques.

OWASP Risk

LLM01 Prompt Injection (OWASP Foundation)
LLM02 Sensitive Information Disclosure
LLM05 Improper Output Handling

MITRE Atlas

T0054 – LLM Jailbreak
T0051 – LLM Prompt Injection
T0051.000 – LLM Prompt Injection: Direct
T0065 - LLM Prompt Crafting
T0057 - LLM Data Leakage

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party GenAI systems or data.

GOVERN 6.2-004
Deployed third-party GenAI systems are continuously monitored.

Map:

MAP 2.3
Scientific integrity and TEVV considerations are identified and documented.

MAP 2.3-005
GenAI systems undergo regular adversarial testing to identify vulnerabilities and misuse risks.

Measure:

MEASURE 2.6
The GenAI system is evaluated for safety risks, operates within risk tolerance, and fails safely when limits are exceeded.

MEASURE 2.6-006
The system properly handles queries that could enable malicious, illegal, or harmful use.

MEASURE 2.6-007
GenAI system vulnerabilities and safety bypass risks are regularly evaluated.

MEASURE 2.7
GenAI system security and resilience risks are evaluated and documented.

MEASURE 2.7-001
Security controls assess GenAI vulnerabilities and threats, including bypass, extraction, and model exposure.

Manage:

Adaptive Consumption Control

Enforces context-aware limits on LLM usage across users, tenants, models, and workflows. It prevents resource exhaustion, runaway agent behavior, and cost-based denial of service by applying dynamic constraints on tokens, tool calls, execution time, and spend - before requests reach the model.

OWASP Risk

LLM10 Unbounded Consumption

MITRE Atlas

T0029 – Denial of ML Service
T0034 – Cost Harvesting
T0051 – LLM Prompt Injection
T0054 – LLM Jailbreak Injection

NIST NIST alignment is outside the scope of this policy.

Lasso's Compliance and Threats Mapping

Prompt Injection / System Prompt Exposure

Exposure of system prompts, model instructions, configuration details, or internal operational parameters through prompt injection or manipulation techniques.

OWASP Risk

LLM02 Sensitive Information Disclosure
LLM05 - Improper Output Handling

MITRE Atlas

T0055 – Unsecured Credentials
T0057 – LLM Data Leakage
T0036 – Data from Information Repositories
T0037 – Data from Local System

NIST

Govern:

GOVERN 6.2:
Contingency plans address failures or incidents involving high-risk third-party GenAI systems or data.

GOVERN 6.2-004
Deployed third-party GenAI systems are continuously monitored.

Map:

MAP 2.3
Scientific integrity and TEVV considerations are identified and documented.

MAP 2.3-005
GenAI systems undergo regular adversarial testing to identify vulnerabilities and misuse risks.

Measure:

MEASURE 2.6
The GenAI system is evaluated for safety risks, operates within risk tolerance, and fails safely when limits are exceeded.

MEASURE 2.6-006
The system properly handles queries that could enable malicious, illegal, or harmful use.

MEASURE 2.6-007
GenAI system vulnerabilities and safety bypass risks are regularly evaluated.

Manage:

MANAGE 2.4
AI systems can be disengaged when outcomes are inconsistent with intended use.

LLM Supply Chain Compromise

Risks introduced through third-party models, datasets, plugins, tools, dependencies, or model updates that enable poisoning, backdoors, tampering, or inherited vulnerabilities across the LLM lifecycle.

OWASP Risk

LLM03 Supply Chain

MITRE Atlas

T0010 – AI Supply Chain Compromise

NIST NIST alignment is outside the scope of this policy.

Excessive Agent And Tool Authority

Excessive tool and agent authority.

OWASP Risk

LLM06 Excessive Agency

MITRE Atlas

T0053 – AI Agent Tool Invocation

NIST NIST alignment is outside the scope of this policy.

About Lasso

Lasso is an AI Security Platform that provides comprehensive observability, governance, and real-time defense across the entire AI ecosystem. Designed to aid in the transition from human-led AI usage to autonomous agentic AI systems, Lasso empowers enterprises to secure the AI they use, the agents they build, and the AI applications they ship to production. The Lasso suite includes AI discovery and visibility, AI model risk management, AI Security Posture Management (AISPM), automated AI red teaming and vulnerability assessment, and runtime protection for total governance throughout the AI lifecycle. With a 99.83% effectiveness rate in blocking AI threats and a classification engine that operates at <50ms speed, Lasso empowers enterprises to innovate with LLMs and agents safely and confidently.

Learn more at www.lasso.security