A Standards-Based Practical and Systematic Approach for AI Ecosystems' Risk Management

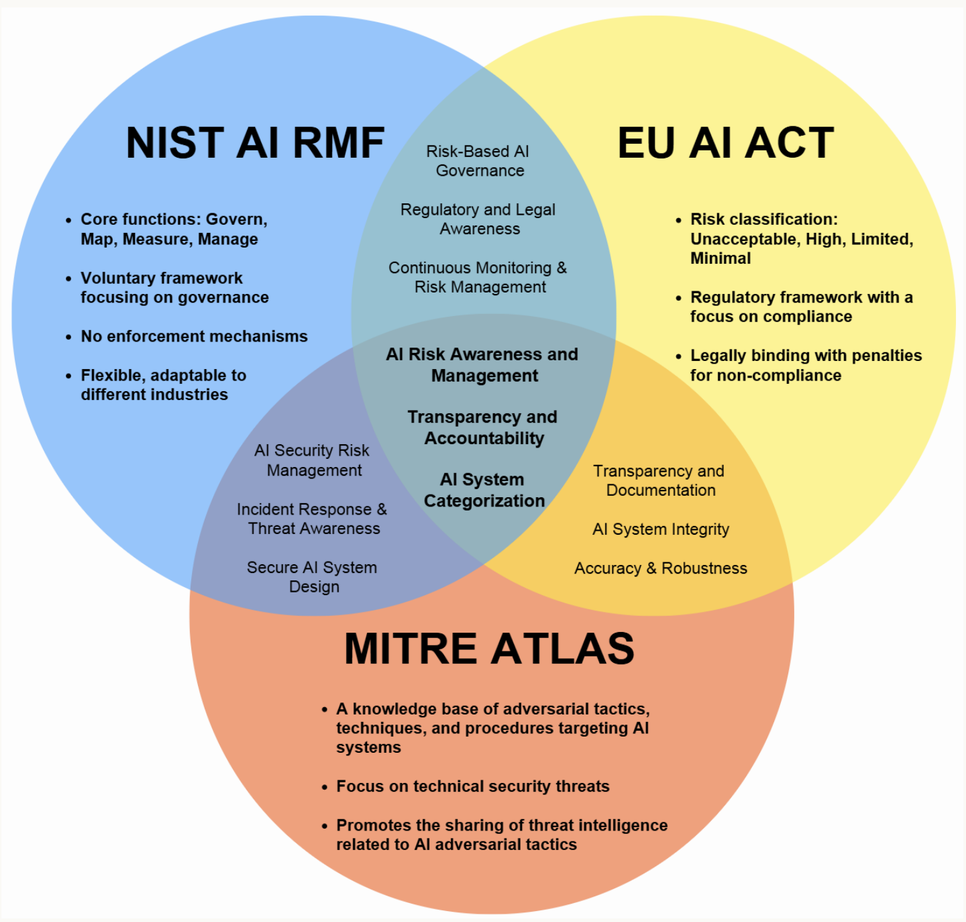
Divya Shreshta Gajula, Divyanshu Singh, Richa Sharma, and Sanika Jade
Advisor: Dr. Eman Hammad

Texas A&M University, College Station, Texas

Problem Statement

As AI adoption grows, governments and organizations are developing governance frameworks to manage AI risks. However, frameworks like NIST AI RMF, the EU AI Act, and MITRE ATLAS approach these risks from complementary angles, making it **difficult for organizations to implement a unified risk management strategy for AI systems**. This lack of coherence creates challenges in ensuring AI system security, compliance, and reliability.

Background & Motivation

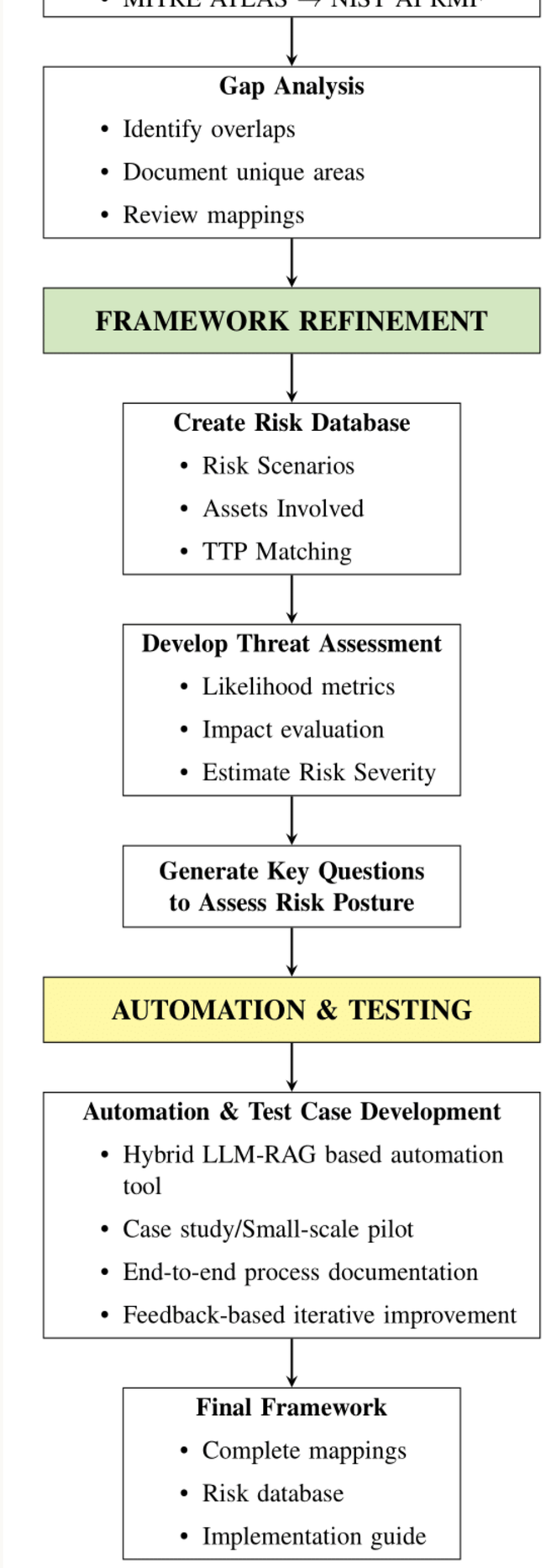


From a cyber risk management perspective:
NIST AI RMF – A voluntary governance framework integrating security into risk management.
EU AI Act - Mandates technical robustness, security, and risk mitigation measures for high-risk AI applications.
MITRE ATLAS - A knowledge base of AI-specific adversarial threats.

Objective: A well-structured Risk Management Framework to help:

- Create a common language for AI risks
- Evaluate AI systems risks consistently
- Provide an approach to identify, assess, & mitigate risks
- Support documentation and transparency for stakeholders.

Methodology



Results

- Identifies **areas of overlap, similarities**, and the requirement for additional controls across all chosen frameworks.
- Significant reduction in control redundancy and compliance assessment efforts.
- Accelerated AI governance implementation enabling **faster time-to-market**.
- Cross-functional collaboration between technical, legal and business teams.

Risk Scenario

Training an ML Model to Perform a Data Poisoning Attack

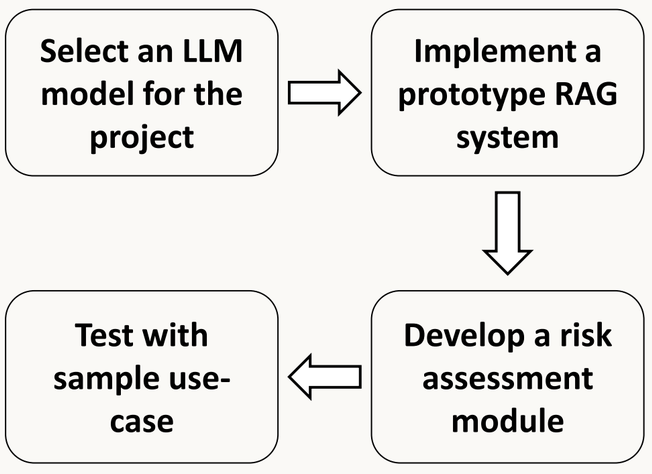
NIST AI RMF:
Measure 1.2: Assessment of Controls Effectiveness and AI Metric Appropriateness
Measure 2.1: Documentation of test sets, metrics, and tools used during test, evaluation, validation, and verification (TEVV)
Measure 2.11: Evaluation of Fairness and Bias

MITRE ATLAS:
Tactics: Resource Development, Persistence
Technique: Poison Training Data (AML.T0020)
Case Studies: 2020 VirusTotal Poisoning, Tay Poisoning

EU AI Act:
Article 9: Risk Management System
Article 10: Data and Data Governance
Article 15: Accuracy, Robustness and Cybersecurity
Article 16: Obligations of Providers of High-Risk AI Systems

Conclusion and Future Work

This framework views governance and compliance as **enablers of responsible innovation** rather than as obstacles. Its unified approach contributes to the evolving field of AI governance by serving multiple organizational objectives simultaneously.



References

1. NIST, "AI RMF Playbook," Artificial Intelligence Risk Management Framework, 2023. [Online: https://airc.nist.gov/airmf-resources/playbook/]
2. European Union, "AI Act Explorer," Artificial Intelligence Act, 2024. [Online]. Available: https://artificialintelligenceact.eu/ai-act-explorer/.
3. MITRE, "ATLAS Matrix," MITRE ATLAS, 2025. [Online]. Available: https://atlas.mitre.org/matrices/ATLAS.