FROM SUPPLY CHAIN DISRUPTION TO APPLIED RISK MANAGEMENT

WRITTEN BY

Alston German, MBA

Sam German BSc, Hons

ARLACO LLC

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

Executive Summary

This proposal outlines a two-phase research and applied engagement that traces the evolution of academic research on supply chain disruption into a practical, standards-aligned risk management framework and tool, and then applies and validates that framework within a critical infrastructure context, with particular emphasis on transportation systems.

The work originates from the 20230706 Supply Chain Disruption Working Report V6b, which examined systemic risks affecting automotive supply chains operating across the US–Mexico border, with Texas as a focal logistics and transportation hub. While the research was well received for its identification and structuring of risk, feedback consistently noted a gap in practical, integrated, and repeatable guidance for managing those risks.

Subsequent real-world client engagements enabled the development of a TARA- and ISO 31000–aligned Risk Management Framework, supported by an operational risk register and governance tooling. This proposal returns to the academic roots of the work to formally document, apply, and validate that framework in a critical infrastructure environment, bridging theory, practice, and education.

Table of Contents

1. Background and Research Origins 1
2. Evolution from Research to Practical Risk Management 1
3. Returning to Critical Infrastructure and Academic Re-Engagement 2
4. Conceptual Framing: Governance, Oversight, and Risk (Mike's Thesis) 3
5. Complementarity Between Governance, Risk Management, and Emergency Management 4
   - 5.1. From Governance Intent to Operational Risk Management 4
   - 5.2. Cross-Cutting Overlays and Organizational Maturity 6
   - 5.3. Integration of Emergency Management Within the Governance Model 6
   - 5.4. Risk Domains as the Structuring Layer 7
   - 5.5. Evidence of Operationalization 7
6. Operationalizing Governance Across Risk Domains and Emergency Management 9
   - 6.1. Domain Risk Standards as the Bridge Between Governance and Execution 9
   - 6.2. Complementary Visual Models 10
7. Appendix A: Full Risk Management Landscape 12
   - 7.1. Integrating Emergency Management Within the Risk Governance Model 12
   - 7.2. Evidence of Operationalization 13
8. Appendix A: Anchor Standards by Domain 13

1. Background and Research Origins

In mid-2023, Alston German completed the Supply Chain Disruption Working Report V6b, focused on risks affecting cross-border automotive supply chains. The research highlighted:

- Structural dependencies between manufacturing supply chains and transportation systems
- Cascading risks driven by policy, labor, cyber, environmental, and geopolitical factors
- The critical role of Texas as a trade gateway and logistics corridor

The report received complementary feedback for its depth of analysis and clarity of risk identification. However, reviewers repeatedly observed that while risks were clearly articulated, there was limited guidance on how organizations should pragmatically manage those risks in an integrated and ongoing manner.

This feedback directly informed the next phase of work.

2. Evolution from Research to Practical Risk Management

Several months after completing the research, Alston was engaged by a client to design a practical risk management framework for an emerging FinTech portfolio. Drawing on the earlier supply chain research, he developed a framework grounded in:

- TARA (Threat Assessment and Risk Analysis)
- ISO 31000 Risk Management principles
- Explicit integration with business strategy, objectives, and governance

The framework evolved into a structured Risk Management Tool and Register that:

- Decomposes risk into threats and vulnerabilities
- Models inherent risk using Probability, Impact, and Proximity
- Explicitly distinguishes residual risk after mitigation
- Assigns executive ownership and accountability
- Embeds risk review within a real-time workflow coupled with a weekly Business Plan Review (BPR) cadence

This approach enables risk to be compared, prioritized, and discussed in economic and decision-relevant terms, rather than as a static register of issues. It also facilitates the integration of risk management into the regular business workflow and prevents it from being seen by staff as an administrative “add-on”. This is a critical component of the approach since most Operational Maturity Models (OMM) see this “elevated” approach

to risk management as contributing directly to efficiency, productivity and ultimately client satisfaction outcomes.

As the framework and tooling increased in complexity, Sam German, an experienced IT and business systems expert, assumed leadership of the platform development, ensuring scalability, consistency, and auditability.

3. Returning to Critical Infrastructure and Academic Re-Engagement

During a dinner meeting with Mike Aspland, Clyde Loll, and Heberto Villarreal of Sam Houston State University, Alston described:

- The original supply chain research
- The feedback received regarding the absence of practical risk management guidance
- The subsequent evolution of the work into an operational framework and tool

This discussion raised the question of whether a framework developed through real-world application could be taken back to its research roots and validated within a critical infrastructure context.

Mike was receptive to this idea and suggested a structured engagement that would document both the research-to-practice evolution and the applied validation of the framework.

4. Conceptual Framing: Governance, Oversight, and Risk (Mike's Thesis)

Following this discussion, Mike introduced a governance-focused thesis that frames organizational performance and risk as the outcome of a closed-loop system linking:

- Vision
- Governance
- Policy and procedures
- Oversight
- Accountability
- Operational practice
- Performance feedback

Risk, within this model, is not static but emerges dynamically based on organizational maturity and the effectiveness of governance and oversight mechanisms. Organizational culture acts as a pervasive influence across all layers of the model.

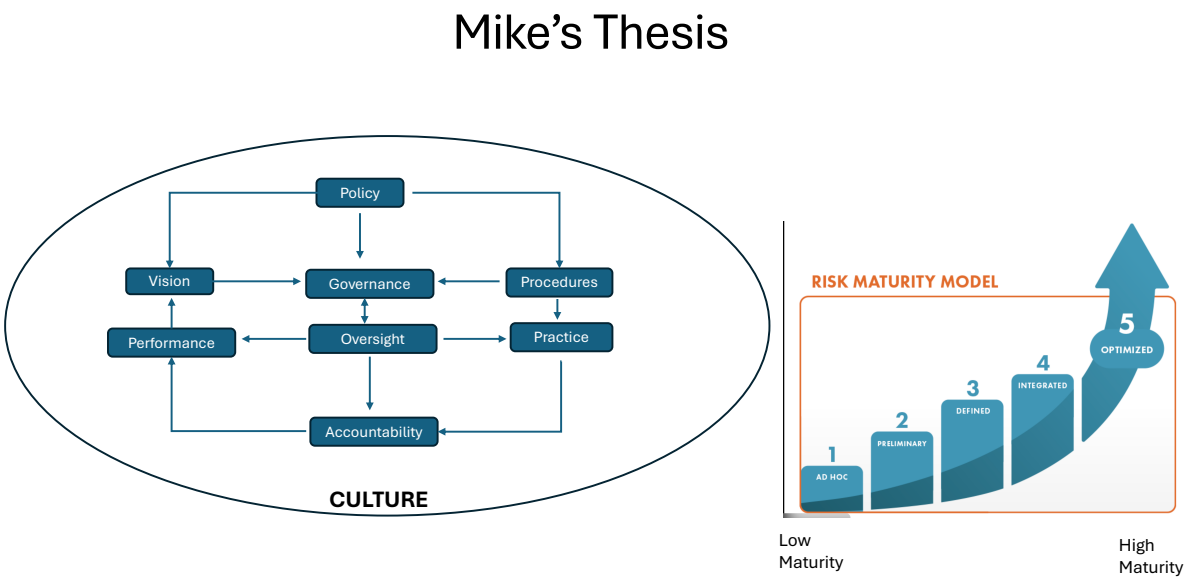


Figure 1: *Governance–Oversight Operating Model for Risk and Performance*

Figure 1: Illustrates the conceptual governance feedback loops that explain how risk and performance emerge within complex organizations.

5. Complementarity Between Governance, Risk Management, and Emergency Management

The governance-focused thesis introduced earlier provides a conceptual explanation for how risk and performance emerge within complex organizations. Within this model, outcomes are shaped by the alignment—or misalignment—between governance intent, oversight, accountability, and operational execution. Risk is therefore not treated as a static condition, but as a dynamic outcome influenced by organizational maturity and the effectiveness of governance and oversight mechanisms.

The applied risk management framework developed through subsequent client engagements is **complementary** to this thesis. While the governance model explains *why* risk materializes, the applied framework defines *how* risks are identified, assessed, prioritized, mitigated, and reviewed in practice. Together, they form a coherent theory-to-practice continuum that translates governance intent into operational behavior.

5.1. From Governance Intent to Operational Risk Management

Within the combined model, governance intent—expressed through organizational vision, objectives, and risk appetite—establishes the context within which risk is managed. Oversight and accountability mechanisms translate this intent into expectations for behavior, decision-making, and control effectiveness.

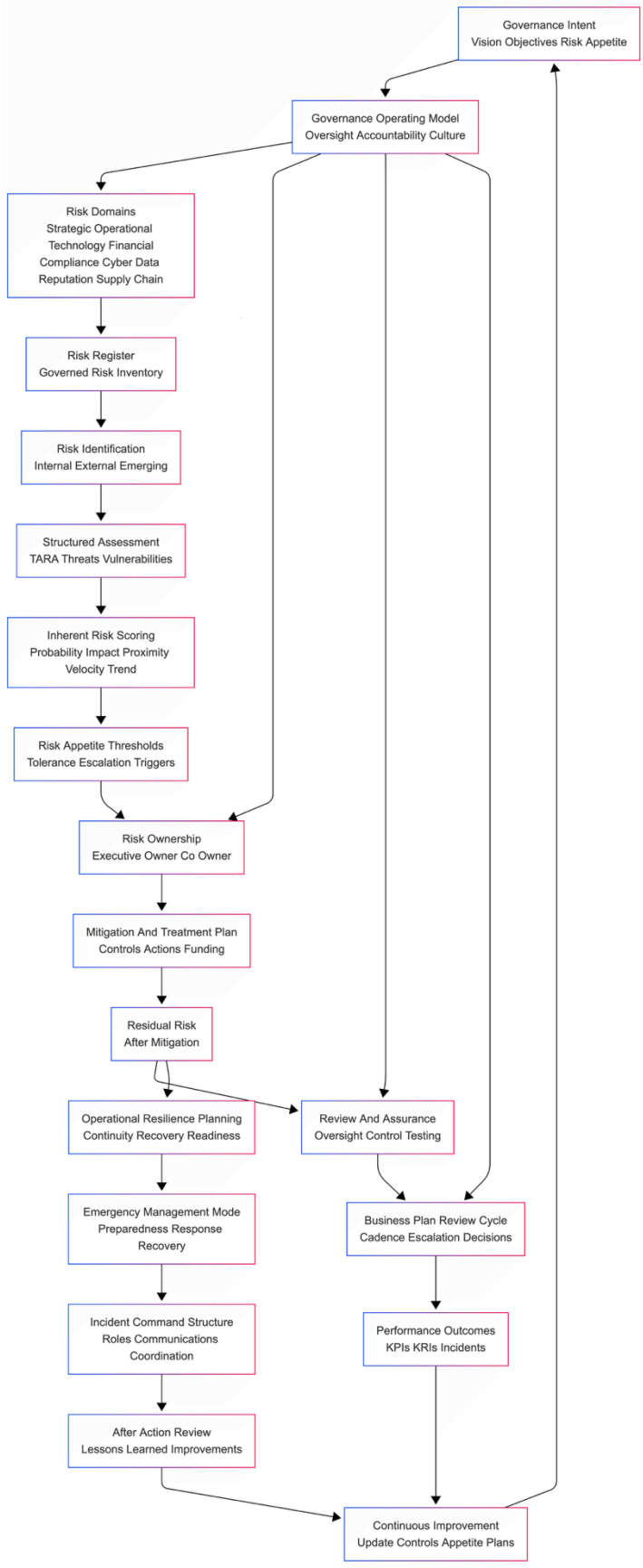
The applied framework operationalizes this intent through a structured risk lifecycle that includes:

- Definition of scope and context
- Identification and categorization of risk across defined domains
- Structured assessment of threats and vulnerabilities
- Prioritization based on consistent scoring attributes
- Assignment of ownership and accountability
- Implementation of mitigation and control actions
- Ongoing review, assurance, and feedback

This operationalization ensures that governance intent is not abstract, but observable and measurable in day-to-day practice.

Figure 2: Operationalization of Governance Intent Across Risk Domains

This figure shows how governance intent is translated into operational risk management through risk domains, a governed risk register, structured assessment, treatment, review, and performance feedback.



5.2. Cross-Cutting Overlays and Organizational Maturity

To ensure consistency across domains and operating contexts, the framework employs a set of **cross-cutting overlays** that apply uniformly across the risk lifecycle. These overlays represent enabling capabilities that influence how effectively governance intent is executed and how organizational maturity develops over time.

The key overlays include:

- **Governance and accountability**, defining decision rights, ownership, and escalation
- **Risk quantification and decision economics**, enabling prioritization and resource allocation
- Operational resilience and emergency management, supporting continuity under disruption
- **Data and AI model risk**, addressing information integrity and automated decision-making
- **Supply chain and ecosystem risk**, recognizing interdependencies beyond organizational boundaries

These overlays correspond directly to the feedback loops and maturity dynamics described in the governance thesis, providing practical mechanisms through which maturity reduces unmanaged risk exposure.

5.3. Integration of Emergency Management Within the Governance Model

In critical infrastructure environments, risk management must function across two operating modes: steady-state governance and crisis-state response. Emergency management represents a distinct but integrated operating mode within the same governance framework.

While steady-state risk management focuses on anticipation, prevention, and preparedness, emergency management is activated when predefined thresholds are exceeded or when disruptive events materialize. Under such conditions, decision-making becomes time-compressed and consequence-driven, requiring clear command structures, predefined escalation criteria, and coordinated action across organizational and public-sector stakeholders.

The framework integrates emergency management by:

- Identifying risks with potential emergency implications in advance
- Embedding preparedness, response, and recovery considerations within operational resilience planning
- Defining escalation triggers that activate emergency management modes
- Maintaining continuity of ownership and accountability before, during, and after incidents
- Feeding post-incident lessons learned back into governance, risk appetite, and control design

This integration ensures that emergency management is not treated as an ad hoc or isolated function, but as an extension of governance intent under stressed conditions.

5.4. Risk Domains as the Structuring Layer

Risk domains play a critical role in bridging governance intent and operational execution. Domains define the scope of risk governance, ensure coverage across organizational activities, and enable aggregation and reporting at appropriate levels of oversight.

Within the framework:

- Governance bodies approve risk appetite and tolerance by domain
- Risks are recorded in the risk register within an approved domain structure
- Oversight and assurance activities are conducted with reference to domain-level exposure and trends

This structuring prevents the risk register from becoming an unprioritized list of issues and enables consistent interpretation of risk across strategic, operational, technology, financial, compliance, and related domains.

5.5. Evidence of Operationalization

The applied framework has been implemented in a working risk management toolset that supports structured risk registers, quantified scoring, executive ownership, and review workflows. These artefacts provide evidence that the combined governance, risk management, and emergency management model is operational, repeatable, and auditable.

While the tooling itself is not the primary research output, it demonstrates that the framework can be executed in practice and provides a concrete basis for validation activities within critical infrastructure environments.

The governance-focused thesis provides a conceptual explanation for how risk and performance emerge within complex organizations, particularly where misalignment

exists between governance intent, oversight, accountability, and operational execution. Within this model, risk is not treated as a static condition but as a dynamic outcome influenced by organizational maturity and the effectiveness of governance and oversight mechanisms.

The applied risk management framework developed through client engagements is **complementary** to this thesis. While the governance model explains *why* risk materializes, the applied framework defines *how* risks are identified, assessed, prioritized, mitigated, and reviewed in practice. Together, they form a coherent theory-to-practice continuum.

In critical infrastructure environments, this continuum must also encompass emergency management, which represents a distinct but integrated operating mode. Governance and risk management primarily function in a steady-state context, establishing structures, priorities, and controls over time. Emergency management, by contrast, operates under time-compressed, high-consequence conditions, requiring rapid decision-making, clear command structures, and effective coordination across organizational and public-sector boundaries.

The applied framework explicitly supports this transition by ensuring that:

- Risks with potential emergency implications are identified and owned in advance
- Escalation thresholds and decision rights are clearly defined
- Preparedness, response, and recovery considerations are embedded within operational resilience planning
- Post-incident review and feedback inform governance, strategy, and risk appetite adjustments

The cross-cutting overlays used in the applied framework—governance and accountability, risk quantification and decision economics, operational resilience and emergency management, data and AI model risk, and supply chain ecosystem risk—directly correspond to the feedback loops and maturity dynamics described in the governance thesis. These overlays ensure that governance intent is translated into both proactive risk management and effective emergency response, rather than treating emergency management as a disconnected or purely tactical activity.

By integrating governance, risk management, and emergency management within a single operating model, the framework enables critical infrastructure organizations to move beyond compliance-driven or reactive approaches and toward a mature, resilient posture capable of anticipating disruption, responding effectively to incidents, and learning systematically from adverse events.

6. Operationalizing Governance Across Risk Domains and Emergency Management

To translate governance intent and risk appetite into consistent operational practice, the framework applies a structured approach across defined risk domains and integrates emergency management as a governed operating mode. This ensures that risk management functions effectively both in steady-state conditions and during disruptive, high-consequence events typical of critical infrastructure environments.

The approach combines:

- A domain-based structuring of risk
- Cross-cutting governance and resilience overlays
- Explicit integration of emergency management within the same governance framework

Together, these elements enable consistent execution of governance intent, scalable oversight, and continuous organizational learning.

6.1. Domain Risk Standards as the Bridge Between Governance and Execution

To support consistent interpretation and application of governance and risk models across the organization, a Domain Risk Standards model has been developed. This model groups enterprise and critical infrastructure risks into a defined set of risk domains, each anchored to a small number of internationally recognized standards and frameworks.

The purpose of this model is not to assert compliance, but to provide a shared reference architecture that enables governance bodies, oversight functions, and risk owners to operate with a common vocabulary across strategic, operational, technology, financial, compliance, and related domains. By doing so, it ensures that governance intent can be translated into operational action in a structured and repeatable manner.

The Domain Risk Standards model acts as a bridge artefact, explicitly connecting:

- Governance intent and oversight structures
- The operationalization of risk management processes
- The structured risk register and supporting dashboards

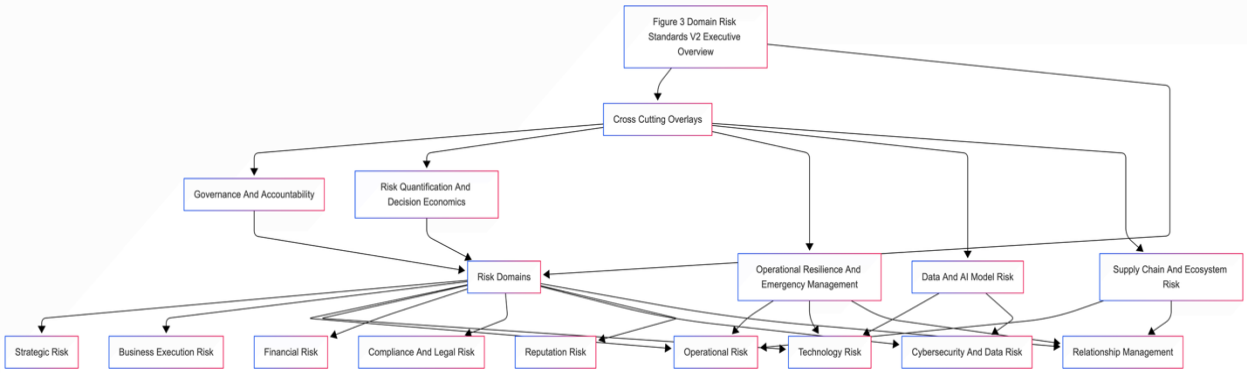


Figure 3: Domain Risk Standards V2 – Executive Overview

This figure presents the executive-level view of risk domains and cross-cutting overlays used to structure risk governance and execution.

6.2. Complementary Visual Models

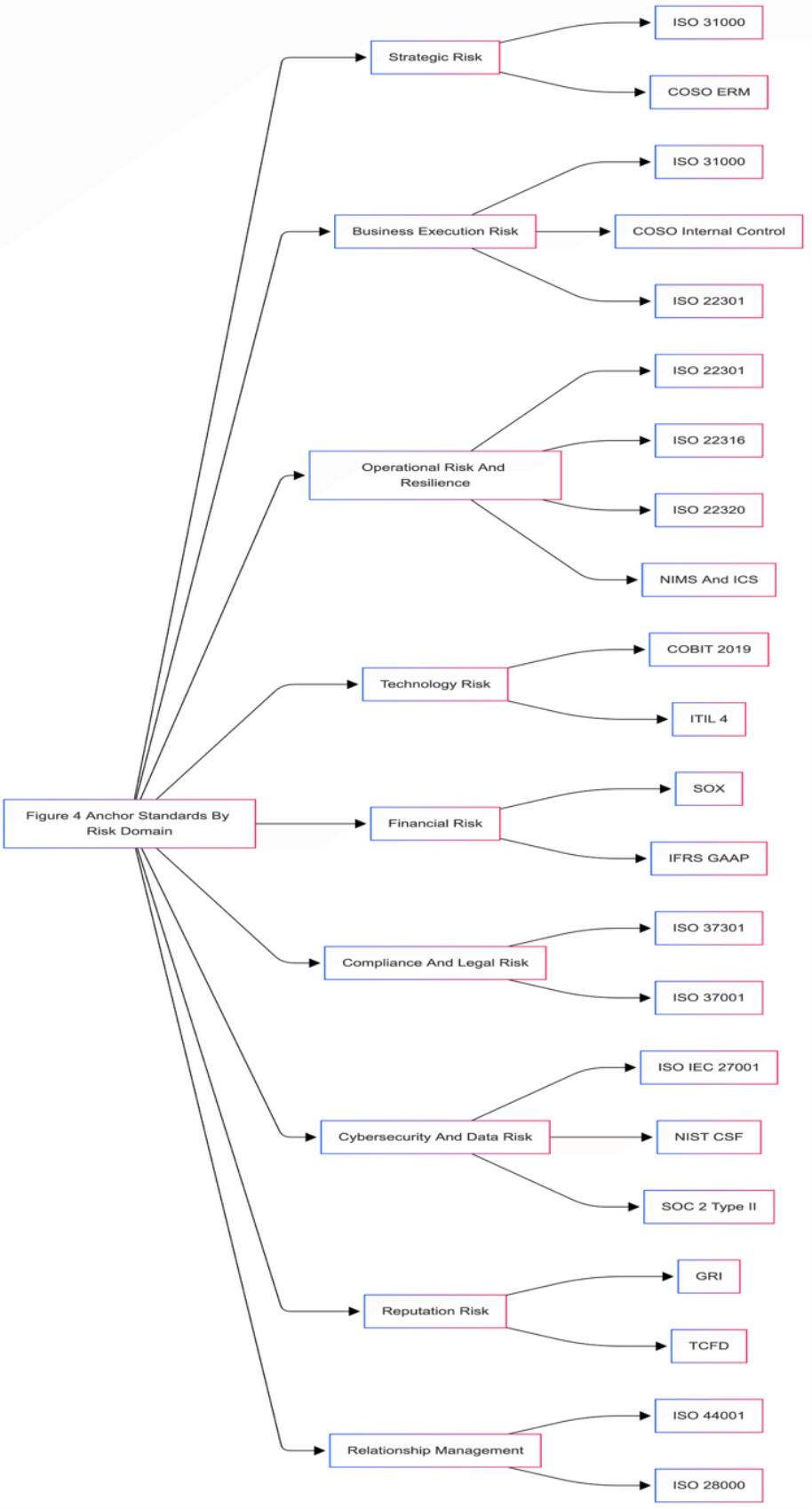
Three complementary visual models are used within this work to support different audiences and levels of detail:

- An **Executive Overview** showing risk domains and cross-cutting overlays, intended for senior leadership and board-level discussion.
- An **Anchor Standards by Domain** view, identifying primary reference standards associated with each risk domain.
- A **Full Risk Management Landscape** view, retained as an appendix, showing the complete mapping of domains, overlays, and reference standards.

This layered visual approach ensures that complexity is intentional and managed, allowing stakeholders to engage at an appropriate level of depth while maintaining a coherent underlying structure.

Figure 4: Anchor Standards by Risk Domain

This figure highlights the primary standards and frameworks associated with each risk domain.



7. Appendix A: Full Risk Management Landscape

This appendix provides the complete domain, overlay, and standards mapping for reference and completeness.

7.1. Integrating Emergency Management Within the Risk Governance Model

In critical infrastructure environments, risk management must extend beyond steady-state governance and control activities to include **emergency management**, which represents a distinct but integrated operating mode. While governance and risk management establish structures, priorities, and controls over time, emergency management operates under time-compressed conditions requiring rapid decision-making, clear command structures, and effective coordination across organizational and public-sector boundaries.

Within this framework, emergency management is treated as a **governed capability**, activated when predefined risk thresholds are exceeded or when disruptive events materialize. The same governance structures that define risk appetite, escalation criteria, ownership, and accountability in steady-state conditions provide the foundation for effective emergency response.

Emergency management within the framework encompasses:

- **Preparedness**, including scenario planning, readiness assessments, and alignment with external emergency management agencies
- **Response**, including defined command structures, decision rights, and communication protocols
- **Recovery**, including restoration of services, stabilization of operations, and transition back to steady-state governance

This approach ensures continuity between risk management and emergency response by:

- Identifying risks with potential emergency implications in advance
- Defining escalation thresholds that trigger emergency management modes
- Maintaining clear ownership and accountability before, during, and after incidents
- Feeding post-incident lessons learned back into governance, risk appetite, and control design

Emergency management considerations are primarily situated within the **Operational Risk and Resilience domain**, but necessarily cut across multiple domains, including technology, cyber and data, supply chain, and reputation risk. By embedding emergency management within the same domain structure used for enterprise risk management, preparedness and response capabilities become integral components of the organization’s overall risk posture rather than isolated or reactive functions.

This integrated approach aligns with internationally recognized standards for business continuity, organizational resilience, and emergency management (including ISO 22301, ISO 22316, and ISO 22320), while remaining compatible with national incident management frameworks where applicable.

7.2. Evidence of Operationalization

The applied framework has been implemented in a working risk management toolset, supporting structured risk registers, executive dashboards, and review workflows. These artefacts provide evidence of operationalization and are used to support analysis and validation activities, but they are not themselves the primary research output.

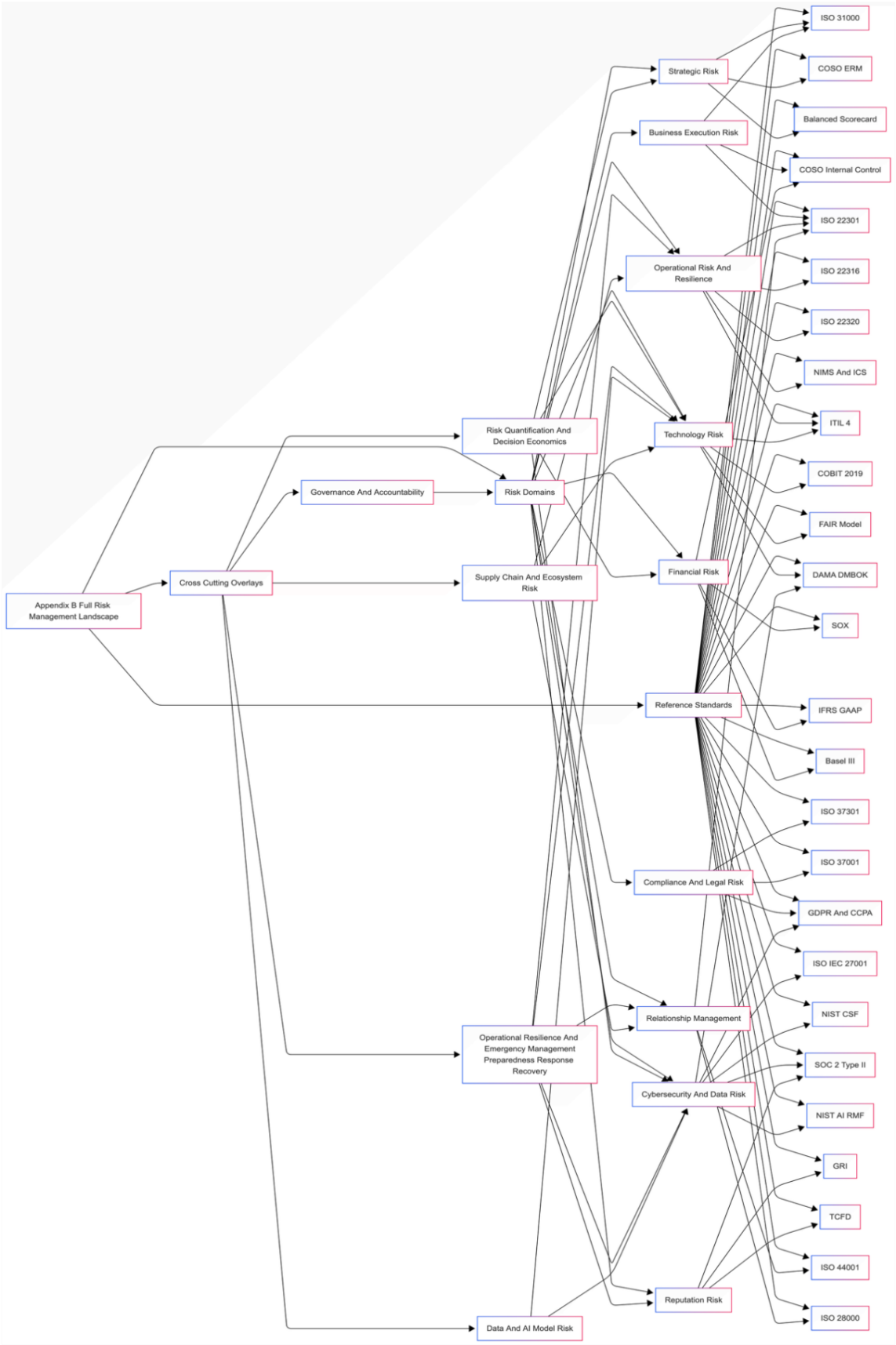
Their role within this work is to demonstrate that the governance, risk, and emergency management model can be executed in practice in a repeatable and auditable manner.

Diagram Placement Summary (for Editor Reference)

- **Figure 3:** Domain Risk Standards V2 – Executive Overview (Section 7.1)
- **Figure 4:** Anchor Standards by Risk Domain (Section 7.2)
- **Appendix B:** Full Risk Management Landscape

8. Appendix A: Anchor Standards by Domain

The chart on the next page presents a context-sensitive Risk Management Landscape, showing the complete mapping of risk domains, cross-cutting overlays, and reference standards. In critical infrastructure contexts, operational resilience explicitly incorporates emergency and incident management as governed response capabilities, aligned with international resilience and emergency management standards.


Appendix B Full Risk Management Landscape
Cross Cutting Overlays
Governance And Accountability
Risk Quantification And Decision Economics
Risk Domains
Supply Chain And Ecosystem Risk
Operational Resilience And Emergency Management Preparedness Response Recovery
Data And AI Model Risk
Strategic Risk
Business Execution Risk
Operational Risk And Resilience
Technology Risk
Financial Risk
Reference Standards
Compliance And Legal Risk
Relationship Management
Cybersecurity And Data Risk
Reputation Risk
ISO 31000
COSO ERM
Balanced Scorecard
COSO Internal Control
ISO 22301
ISO 22316
ISO 22320
NIMS And ICS
ITIL 4
COBIT 2019
FAIR Model
DAMA DMBOK
SOX
IFRS GAAP
Basel III
ISO 37301
ISO 37001
GDPR And CCPA
ISO IEC 27001
NIST CSF
SOC 2 Type II
NIST AI RMF
GRI
TCFD
ISO 44001
ISO 28000

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

© 2026 The Sam Houston State University Institute for Homeland Security.

German, A., German S. (2026). From Supply Chain Disruption to Applied Risk Management. (Report No. 2026-1042). The Sam Houston State University. Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/D572B

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY