EXSUM Executive Summary (POC SWOPE, JASON)

TASK. Research executive guidance in the safe and secure use of AI.
PURPOSE. Present a definitive and quantifiable Governance, Risk, and Compliance (GRC) trajectory for NIST, establishing a clear and measurable pathway to enhance performance and effectiveness by fully capitalizing on the latest advancements in AI technology, facilitating substantial growth, and improving scalable outcomes through operational efficiency.
PROBLEM. Awareness and acceptance of Artificial Intelligence (AI) across various public-private Operational Environments (OEs) with a clear focus on the safe and secure use of AI.
RESEARCH. How can public-private organizations use the transformative power of GenAI, LLMs, and GPTs to bridge the gap between Artificial Intelligence (AI) technical expertise and business acumen to achieve strategic objectives safely and securely while maintaining a competitive advantage in pre- and post-Artificial General Intelligence (AGI) Operational Environments (OEs)?
ENHANCED VALUE. In Executive Order (EO) 14110 Sec. 10. *Advancing Federal Government Use of AI*. (b)(ii) the **Chief Artificial Intelligence Officers' (CAIO)** roles, responsibilities, seniority, position, and reporting structures; and (d)(vii) assume each CAIO is a capable SES possessing Executive Core Qualifications (OPM, 2024), especially **ECQ 4: Business Acumen** ensures that every EO 14110 mandated CAIO needs this novel GRC AI tooling to **systematically bridge AI "technical" to "business" tribes and "smash silos."**
NEXT STEPS. Operationalize GRC AI RMF tooling (*transition from PoC to MVP*). Correlate NIST AI RMF V1.0/100-1 (*in Version 2.0*) ontology/nexus to GRC policy (EO 14110) & industry (ISO, UCF, et al.). Reproduce and scale with other emerging RMF standards such as NIST CSF 2.0 & CMMI 3.0 (2024). Share with NIST to maximize value for all stakeholders. Use NIST success to expand to other markets/areas comprising DoD doctrine, Army ADP 3-13 *Information (Warfare)* et al. USAF AFDP 3-13 (2023), USMC MCDP 8 & MCDP 8-10 (2024).

EXECUTIVE ORDER 14110 NIST RFI

Safe, Secure, and Trustworthy Development and Use of AI

Jason Swope

Elham Tabassi, NIST Chief AI Advisor

Author Note

Jason Swope. https://orcid.org/0009-0008-9350-2881

There are no known conflicts of interest to disclose.

Correspondence concerning this artifact should be addressed to Jason Swope.

MSc CJS-Homeland Security; *practice concentrations in Cyber, AI, & Quantum*

DoD AI Work Role IDs: 111, 331, 623, 672, 733, 753, especially 901 (Cyber) & 902 (AI)

Email: EO14110NISTAIRMF@gmail.com

Background

This submission, in response to the National Institute of Standards and Technology's (NIST) Request for Information (RFI) dated December 21, 2023 (USG, 2024a), focuses on Executive Order (EO) 14110 (USG, 2024b), Sections 4.1(a)(i) (A) *developing a companion resource to the AI Risk Management Framework, NIST AI 100–1, for generative AI;* and (C) *launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity.* Adhering to the 25-page RFI response limit sans references, it concentrates on offering "specific and actionable" improvements to guidelines, standards, and best practices in the safe and secure use of Artificial Intelligence (AI), with a particular emphasis on tribalism, silos, Generative AI (GenAI) and Large Language Models (LLMs). The document is designed to provide strategic insights and support practical actions for operationalizing a robust public-private AI Risk Management Framework (AI RMF). This targeted approach aligns directly with the objectives of EO 14110, enhancing NIST's work in establishing a thorough and effective AI RMF (Tabassi, 2023), fulfilling the executive order's goals, and aiding in its successful execution across all government and commercial entities. This response explicitly states that the AI Governance, Risk, and Compliance (GRC) tooling is subject to copyright, ensuring compliance with legal standards and respect for intellectual property rights with a willingness to offer it to NIST at no cost.

Purpose

This response presents a definitive and quantifiable Executive Order 14110 compliant Governance, Risk, and Compliance (GRC) trajectory for NIST. It establishes a clear and measurable pathway to enhance performance and effectiveness by fully capitalizing on the latest

Artificial Intelligence (AI) technology advancements, facilitating substantial growth, and improving scalable outcomes through operational efficiency. It doesn't matter if you are in the business of warfighting, national security, or commercial ventures; business fundamentals remain the same: business is business. Barreto et al. (2023) noted that this operational mindset is pivotal for maximizing the State-of-the-Art (SOTA) role of Generative AI (GenAI) in organizations. It empowers leaders to address inherent business risks and capitalize on opportunities, harnessing GenAI's power for a strategic advantage in any sector. The exploration of GenAI's impact and applications, highlighted by Wang et al. (2023) and Wu et al. (2023), is not just about technological innovation but also encompasses ethical applications and risk mitigation. The objective, or opportunity, is to bridge the gap between technical expertise and business acumen, transforming challenges into growth, resilience, and profitability. The significance of this response lies in its potential to shape GRC AI strategies, aligning technological advancements with business objectives for sustainable and ethical progress.

Problem, Prioritization, & Strata

We must solve the underlying problem between “technical” and “business” tribes first. Under Executive Order 14110, Sections 4.1(a)(i) (A) and 2. *Policy and Principles* (d), aligning Artificial Intelligence (AI) policies with the NIST AI Risk Management Framework (NIST AI RMF 1.0 or NIST 100-1) is crucial for addressing the issue of tribalism and siloed approaches in AI Governance, Risk, and Compliance (GRC) development. Wu et al. (2023) highlighted the imperative to bridge the gap between AI technical expertise and business applications. Their research showed a divide where technical experts view AI as an innovation, while business leaders are cautious due to its organizational and market impacts. The problem reflects a deeper tribalism issue exacerbated by siloed mentalities impeding collaborative progress, policy

adoption, and widespread acceptance and use of the NIST AI RMF. Bridging these perspectives is essential for balancing views, overcoming resistance to change, and breaking down sociocultural barriers in GRC AI adoption. The onset of policy adoption and enforcement requires recognizing AI as both a technological advancement and a strategic business asset, promoting a significant shift in cultural, ethical, and organizational thinking. Such a sociocultural shift is vital for fostering responsible AI development, ensuring safety and security, bridging the sociotechnical and tactical-strategic divides, and advancing equity and civil rights.

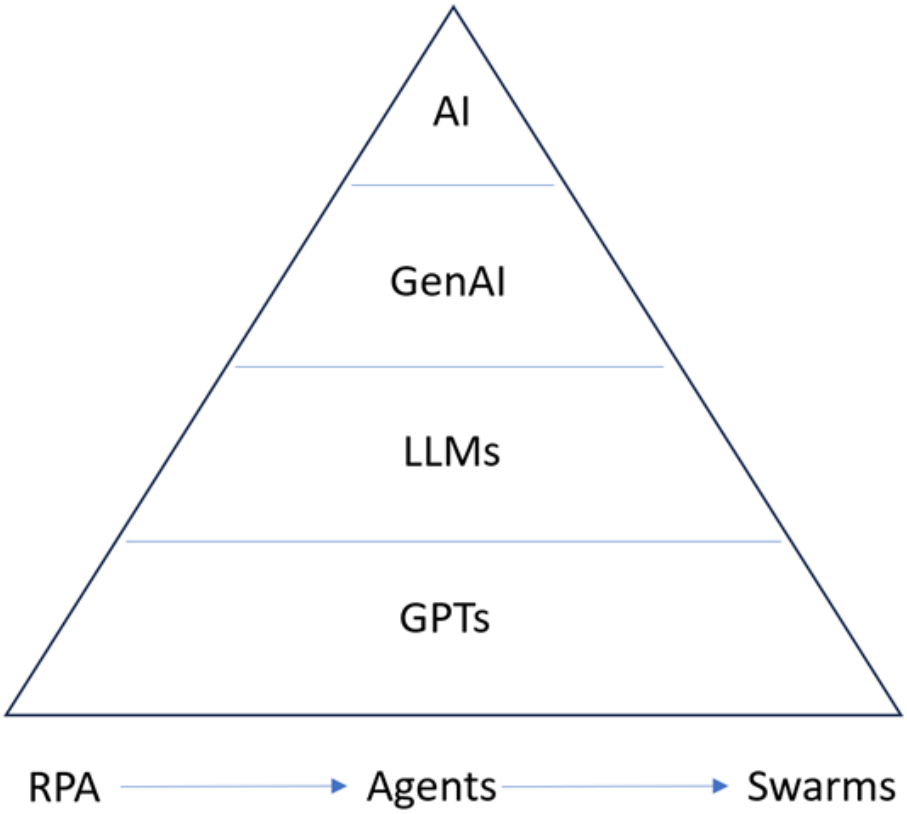

Figure 1. AI Paradigm With Underlying Risks & Opportunities

The paradigm in Artificial Intelligence (AI), encompassing technologies like Generative AI (GenAI), Large Language Models (LLMs), Generative Pretrained Transformers (GPTs), Robotic Process Automation (RPA), intelligent agents, and agent swarms, presents a multifaceted challenge of minimizing strategic risk, maximizing business value, and driving

innovation. Transformation is not merely technical but also deeply sociocultural, demanding a reevaluation of traditional assumptions about creativity and the human versus machine role in artistic and intellectual endeavors. Bruni and Comacchio (2023) explained Tom Freston's notion that innovation stems from combining existing elements in novel ways, resonating profoundly in this response context. AI's recent advancements challenge this view by generating content indistinguishable from human craftsmanship. This development necessitates a fundamental shift, recognizing AI as a collaborator in creativity and innovation rather than a mere tool. Such a transition involves addressing ethical, legal, and societal implications, ensuring that AI's integration into these domains is responsible and beneficial. Organizations must navigate this new landscape, balancing the potential for unprecedented innovation with the need for robust Governance, Risk, and Compliance (GRC) strategies and ethical considerations. The challenge lies in harnessing AI's capabilities to augment human creativity and productivity, transforming industries while respecting and preserving the intrinsic value of human input and oversight.

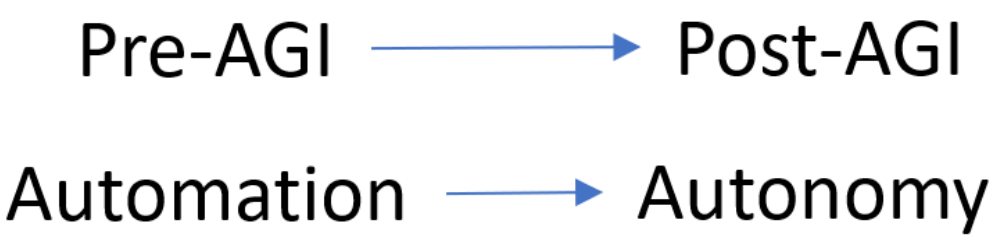

Figure 2. Business World, Shift

The world is on the cusp of a shift from pre-Artificial General Intelligence (pre-AGI) to post-Artificial General Intelligence (post-AGI). In the pre-AGI phase, AI systems specialize in specific tasks, significantly improving efficiency and accuracy in business automation. Xie et al. (2023) suggested that the emergence of AGI, capable of performing any intellectual task that humans can, represents a quantum leap from mere automation to full autonomy. In the pre-AGI

era, AI-supported human decision-making resides within set boundaries, but in post-AGI, AI could independently devise and implement complex strategies, surpassing human abilities. This evolution from a human-simulated cognitive supportive role to efficient business processes machine-led leadership poses essential questions about the future of work, human control, and ethical concerns surrounding AI independence. Organizations need to adapt, creating strategies that utilize AI's growing capabilities while mitigating the risks of increased autonomy. This evolution necessitates reevaluating organization Governance, Risk, and Compliance (GRC) structures and strategies to stay competitive and ethical in an impending AGI-dominated world. Embracing this change will ensure resiliency in a rapidly evolving market and unlock unprecedented innovation and value-creation opportunities.

Methodology

This response introduces a methodology that combines the Artificial Intelligence (AI) Risk Management Framework (RMF) by Tabassi (2023) with the Department of Defense's (DoD) (2023) emerging work roles based on the presumptive classification of individuals or entities as "technical" or "business." The AI RMF's functions of GOVERN, MAP, MEASURE, and MANAGE, alongside the seven characteristics of trustworthy AI systems (valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed), provide a comprehensive enterprise approach to evaluating risks and opportunities that promote trustworthy AI systems. This integration systematically addresses technical and business communities' sociocultural differences and perspectives, eliminating human bias. Emerging work roles ranging from AI Adoption Specialist to AI Innovation Leader are introduced, bridging technical expertise with business acumen, emphasizing role specialization, ethical compliance, and strategic leadership in a dynamic AI

environment. This methodology prioritizes breaking down tribalism and silos, fostering a collaborative AI environment that enhances cyber resilience, drives innovation, and informs executive decision-making in safe and secure AI systems. Building on this, the next generation AI RMF and work role evolution leveraging applied AI, GenAI, LLM, and GPT automation, encompassing Robotic Process Automation (RPA), intelligent AI agents, and agent swarms, is set to revolutionize this field, further enhancing operational capabilities and efficiency.

Design

Adopting an exploratory qualitative design, integrating ethnography, netnography, and phenomenology, centered on thematic analysis, presents a comprehensive investigative framework. Thomas and Lawal (2020) proposed that using an Exploratory Research Design (ERD) is productive in obtaining background information and clarifying research problems, particularly in cases involving poorly understood phenomena. Addeo et al. (2019) stressed that ethnography and netnography facilitate immersive engagement in the sociocultural contexts of technical and business tribes in both physical and online environments, a concept mirrored in the emphasis on netnography's versatility and effectiveness in studying experiential online communities and practices within social science research. Phenomenology complements this by examining individual experiences, offering insights into the collective perceptions and interpretations of operational environments shared by technical and business tribes. A thematic analysis identifies and interprets patterns in the qualitative data, focusing on baseline themes emerging from the subjects' interactions and experiences. This systematic, methodical approach untangles the complex web of sociocultural factors that influence interactions and efficacy within these interconnected yet distinct tribes at the intersection of technology, culture, and business practices in the cyber domain, enabling a concentration on Artificial Intelligence (AI).

Setting and Framework

The methodology focuses on Governance, Risk, and Compliance (GRC) by operationalizing AI risk management using the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF) version 1.0 and its accompanying AI RMF Playbook (NIST, 2023). At the center, the AI RMF Core encompasses four core functions: GOVERN, MAP, MEASURE, and MANAGE. These functions facilitate a comprehensive approach to managing AI risks and developing trustworthy AI systems. The GOVERN function establishes a risk management culture and integrates governance throughout the AI risk management process. The MAP function provides a context for framing AI-related risks, emphasizing the importance of understanding the various stages of the AI lifecycle and their interdependencies. The MEASURE function employs various tools and methodologies to analyze and monitor AI risks, informed by the risks identified in the MAP function. The MANAGE function involves allocating resources to manage these risks effectively, guided by the policies and procedures established in the GOVERN function. The AI RMF Playbook serves as an online resource to guide organizations in applying these functions contextually, allowing for tailored approaches to AI risk management. This framework encourages the inclusion of diverse, multidisciplinary work roles and perspectives, emphasizing continuous risk management throughout the AI system's lifecycle. This approach to AI risk management is integral to creating trustworthy AI systems and aligning them with organizational values and strategic priorities.

A focus on AI RMF Profiles, emphasizing the importance of developing novel Governance, Risk, and Compliance (GRC) tooling that includes prescriptive profile templates with executive dashboards, is critical to short and long-term organizational success. This approach is vital for informed executive decision-making. AI RMF Profiles are tailored,

reproducible, and scalable implementations of the AI RMF's core functions, GOVERN, MAP, MEASURE, and MANAGE, specific to an organization's context, constituting its risk tolerance, sector, or technology use. These profiles, which include current and target states of AI risk management activities, help identify gaps and develop action plans for risk mitigation. Creating novel GRC tools, including prescriptive profile templates with executive dashboards, is critical in this methodology. Tool features enabling executives to visualize and comprehend the complex landscape of AI risks helps progress toward their leadership and management goals. Such visualizations aid in prioritizing actions and allocating resources effectively, thereby facilitating strategic decision-making. The flexibility inherent in the AI RMF's approach to profile templates allows for customized solutions that align with different organizations' unique needs and goals, enhancing the effectiveness of AI risk management strategies.

AI Actor Tasks underscore the significance of emerging Governance, Risk, and Compliance (GRC) Artificial Intelligence (AI) work roles. As the Department of Defense (2023) posited, work roles such as AI Adoption Specialist, AI Innovation Leader, AI Risk & Ethics Specialist, AI Test & Evaluation Specialist, AI/ML Specialist, and All-Source Analyst are pivotal in managing GRC effectively. These specialized roles, each with distinct Knowledge, Skills, Abilities, and Tasks (KSATs), cater to different aspects of AI system development and management, from design to deployment and operation. Their expertise covers a broad spectrum, including cybersecurity, risk management, legal and ethical compliance, cloud computing models, and quantum. Integrating these roles into the AI RMF's lifecycle phases, from AI design to deployment and operation, facilitates a resilient and robust GRC approach. This methodology is vital for safeguarding businesses and stimulating growth across various organizational GRC applications, including warfare, justice, security, and commercial for-profit enterprise. The

diverse expertise and comprehensive understanding these roles bring are essential for navigating the complexities of AI systems and ensuring their secure, ethical, and effective deployment, thereby protecting businesses and fostering innovation in a rapidly evolving AI landscape.

Procedures

The process starts by presumptively classifying practicing *GRC AI RMF* Cyber or AI human resources in an organization as "technical" or "business," aligning individuals with their expertise. Utilizing the Artificial Intelligence (AI) Risk Management Framework (RMF), we then apply the core functions of GOVERN, MAP, MEASURE, and MANAGE to novel Governance, Risk, and Compliance (GRC) tools. The method integrates seven essential AI traits with technical and business priorities for a balanced, robust approach. Work roles like AI Adoption Specialists and AI Innovation Leaders are activated, crucial in combining technical and business knowledge to break down internal barriers for a unified work environment. This strategy leads to an executive decision-making framework, enabling the implementation of AI systems that are safe, secure, and strategically aligned. Key to success is executive dashboards, which visually represent complex data, making it accessible and actionable for decision-makers. This streamlined GRC approach not only boosts operational efficiency but also maximizes GRC's business value, placing the organization at the cutting edge of innovation and securing its long-term success in the AI-driven digital landscape.

Data Collection

During the data collection phase, using a novel Governance, Risk, and Compliance (GRC) tool that adheres to the NIST Artificial Intelligence (AI) Risk Management Framework (RMF), we start by presumptively categorizing participant respondents as "technical" or "business." Each individual is aligned with their specific expertise and placed in a role-based

hierarchy as a practitioner, manager, or leader. This basic human-terrain mapping is critical for effectively implementing the RMF's core functions: GOVERN, MAP, MEASURE, and MANAGE. The tool then combines these functions in qualitative and quantitative survey responses based on the seven key characteristics of trustworthy AI systems—validity, safety, security, accountability, transparency, interpretability, privacy, and fairness. This approach is critical to conducting a thorough enterprise-level AI risk assessment with profile summation.

NIST AI RMF V1.0 PROFILE SCORECARD ©

Govern GV	**62.4%**	
	Govern 1 *Effective Governance* GV.1	53.6%
	Govern 2 *Accountability Structures* GV.2	75.0%
	Govern 3 *Inclusive Workforce* GV.3	62.5%
	Govern 4 *Cultural Commitment* GV.4	58.3%
	Govern 5 *Engagement Processes* GV.5	62.5%
	Govern 6 *Policies and Procedures* GV.6	62.5%
Map MP	**67.3%**	
	Map 1 *Context Understanding* MP.1	70.8%
	Map 2 *System Categorization* MP.2	83.3%
	Map 3 *Capabilities Assessment* MP.3	70.0%
	Map 4 *Risk Mapping* MP.4	62.5%
	Map 5 *Impact Characterization* MP.5	50.0%
Measure MS	**64.1%**	
	Measure 1 *Metrics Application* MS.1	75.0%
	Measure 2 *Trustworthiness Evaluation* MS.2	73.1%
	Measure 3 *Risk Tracking* MS.3	58.3%
	Measure 4 *Feedback Assessment* MS.4	50.0%
Manage MG	**31.3%**	
	Manage 1 *Risk Management* MG.1	25.0%
	Manage 2 *Strategic Implementation* MG.2	25.0%
	Manage 3 *Third-Party Management* MG.3	25.0%
	Manage 4 *Risk Treatments* MG.4	50.0%

Figure 3. GRC AI RMF Profile Scorecard

Using the GRC tool, we then meticulously assess and compile the organization's AI risk profile, which comprises 4 Functions, 19 Categories, and 72 Subcategories, comparing the current organizational practices, performance levels, and expectations against these standards. Astute observers will note that in *Figure 3*, we added a two-word and alphameric nomenclature to standardize summary reference, making the system more efficient. For example, we extend the function of Govern to *Govern GV*, with the category of Govern 1 to *Govern 1 Effective Governance GV.1*, and corresponding subcategories such as *GV.1.1*. The resulting assessment encompasses comprehensive knowledge of current policies, procedures, and AI systems. Well-defined emerging work roles, such as AI Adoption Specialists and AI Innovation Leaders, are activated, critically linking the GRC tooling to technical expertise with business acumen. This structured, unbiased, holistic approach to data collection helps remove organizational sociocultural and technical barriers, creating a unified and effective AI ecosystem that empowers executives to make informed decisions aligned with business strategies.

Data Analysis

The novel Governance, Risk, and Compliance (GRC) tool's qualitative responses, organized under NIST AI RMF's 4 Functions, 19 Categories, and 72 Subcategories, are quantitatively analyzed in the data analysis phase. Binary responses to 360 survey questions assess compliance with Risk Management Framework (RMF) guidelines. Human-centric responses can and should eventually be automated by machines and machine outputs. Artificial Intelligence (AI) Robotic Process Automation (RPA) enhances the analysis by converting binary data into percentile-based statistical estimations. This accuracy in data processing transforms qualitative responses into quantifiable metrics, emphasizing 100% truth and accountability while presenting opportunities for structured, unbiased Key Performance Indicators (KPIs) and Key

Risk Indicators (KRIs). Essential for executive dashboards, these percentile estimations offer a transparent, detailed view of organizational alignment with AI RMF standards, including financial actuarial data expressed in dollars. Consistent, reliable, reputable insight into AI performance, risk levels, and compliance status empowers executives with more accurate decision-making tools. The dashboards, displaying complex data visually, significantly improve decision-making accuracy and contribute to robust, strategically aligned AI governance and management.

Visualization

Leveraging the novel Governance, Risk, and Compliance (GRC) tool's capability to quantify Artificial Intelligence (AI) status in percentiles combined with visualization through Business Intelligence (BI) dashboards like Microsoft SharePoint and PowerBI is vital in executive decision-making. These dashboards transform complex statistical data derived from the AI RMF's 4 Functions, 19 Categories, and 72 Subcategories into clear, visual formats.

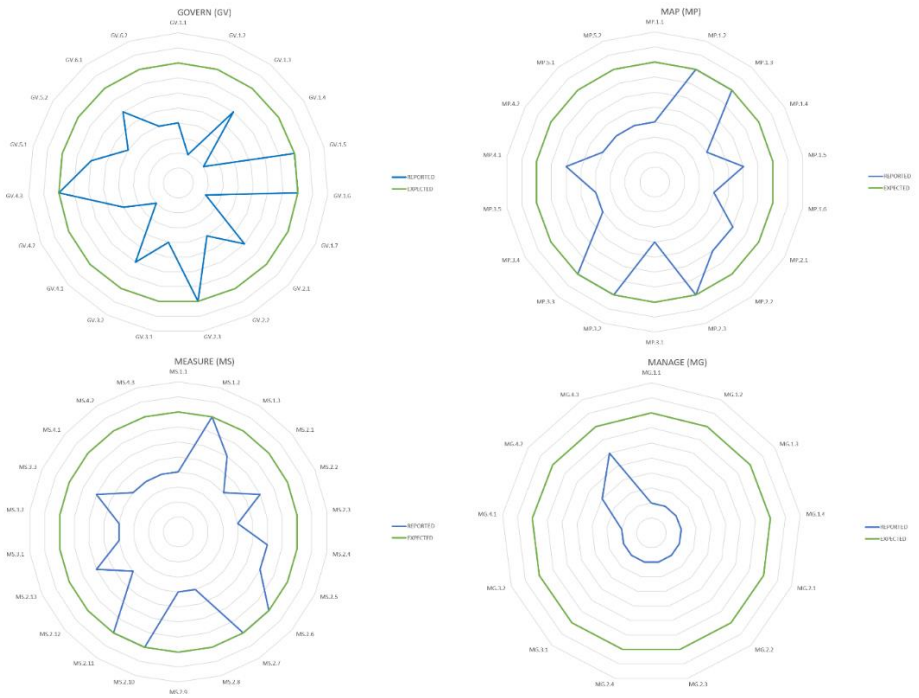

Figure 4. GRC AI RMF Executive Dashboard

Dashboards help executive strategic decision-makers quickly understand AI performance, risk levels, and compliance status. Integrating the GRC tool with BI platforms ensures the framework provides consistent, reliable, accurate, and reputable insights, translating percentile estimations and financial actuaries into actionable intelligence. This comprehensive visualization helps leaders identify strengths, potential risks, and compliance issues, offering a holistic view of AI governance and management. Executives can make more informed, data-driven decisions, enhancing the strategic alignment of AI initiatives with organizational goals. This approach improves decision-making accuracy decisively, contributing to a more robust, efficient AI ecosystem.

Trustworthiness

This response emphasizes the correlation between trustworthy Artificial Intelligence (AI) characteristics and minimizing negative AI consequences. By focusing on AI systems that are valid and reliable, we ensure accuracy and robustness, reducing business risks associated with inaccuracy or unreliability. Safety is prioritized to prevent endangerment to human life, health, property, or the environment. Security and resilience are essential, with systems designed to withstand adverse events and maintain confidentiality, integrity, and availability. We advocate for accountability and transparency, ensuring information about AI systems and their outputs is accessible and understandable, enhancing trust, and enabling responsible decision-making. An ability to easily explain and interpret the data is critical, allowing users to understand AI mechanisms and outputs and fostering informed interactions with AI systems. Privacy enhancement is incorporated to safeguard human autonomy and identity, balancing privacy with other AI characteristics like accuracy and fairness. The approach addresses fairness by managing harmful bias, ensuring equality and equity, and preventing discrimination. This comprehensive

focus on trustworthiness in AI aligns with the Risk Management Framework's (RMF) guidance, significantly lowering the likelihood and impact of adverse AI outcomes.

Ethics

The response is thematically grounded in the standards and publications of NIST AI RMF et al., especially in ethnography, and is committed to upholding the highest standards of ethics. This position as an organizational commitment ensures responsible and trustworthy Artificial Intelligence (AI) development and use across the enterprise. By aligning with the NIST AI RMF, we ensure that business-oriented methodologies and practices in AI systems are human-centric, socially responsible, and sustainable. Adhering to ethical standards emphasizes the importance of considering the impacts of AI decisions and activities on society and the environment, promoting transparency and ethical behavior. In ethnographic research, this translates to a respectful and conscientious approach toward data collection and analysis, safeguarding the dignity and autonomy of individuals and communities involved. This research adheres to these ethical standards and ensures that the AI systems we study and develop are not only technically proficient but also equitable and accountable, respecting the rights and values of all stakeholders. This ethical lens is crucial for minimizing potential harms and maximizing the benefits of AI, fostering trust and confidence in AI technologies and their applications.

Summary

This response integrates the NIST AI Risk Management Framework (RMF) to establish a comprehensive Governance, Risk, and Compliance (GRC) trajectory for NIST. Focused on enhancing performance through Artificial Intelligence (AI) technologies, the methodology blends ethnography, netnography, and phenomenology within a thematic analysis framework. Aligning with the NIST AI RMF, it incorporates core functions such as GOVERN, MAP,

MEASURE, and MANAGE, alongside seven critical characteristics of trustworthy AI. This approach effectively bridges the gap between AI technical expertise and business acumen, which is crucial for achieving strategic objectives in pre- and post- Artificial General Intelligence (AGI) Operational Environments (OEs). The model introduces emerging roles like AI Adoption Specialists and AI Innovation Leaders, fostering a collaborative AI OE that enhances cyber resilience and drives innovation. Advanced AI technologies, including Robotic Process Automation (RPA), intelligent AI agents, and agent swarms, are leveraged to revolutionize operational capabilities and efficiency. This strategic alignment informs executive decision-making, expanding the transformative power of GenAI, LLMs, and GPTs beyond traditional business applications to encompass critical areas such as warfare strategy, critical infrastructure management, and commercial for-profit ventures. This broadened scope recognizes these technologies' potential to revolutionize corporate efficiency and innovation and provide groundbreaking solutions in national defense, infrastructure resilience, and profit-driven market dynamics.

The methodology ensures rigorous and transparent data collection and analysis, adhering to Risk Management Framework (RMF) guidelines, and focuses on organizational compliance, performance, and policy assessments. Utilizing Business Intelligence (BI) dashboards such as Microsoft SharePoint, and PowerBI is central to visualizing Artificial Intelligence (AI) status and risks, significantly improving executive decision-making. This multidimensional approach emphasizes the trustworthiness of AI systems, ensuring they are valid, reliable, safe, secure, accountable, transparent, explainable, and privacy-enhanced. Ethical considerations are paramount, with the study upholding the highest standards of ethics in alignment with NIST AI RMF and other authoritative standards. This ethical commitment ensures responsible AI

development and usage, fostering AI systems that are equitable and accountable. Minimizing potential harms and enhancing trust in AI applications, the methodology provides a robust framework for effectively using AI technologies in business. This strategic application of AI ensures safe, secure, and efficient operational outcomes, maintaining a competitive edge in the rapidly evolving business world and digital landscape.

Cybersecurity Use Case

In Cybersecurity, bridging the gap between the business tribe, focusing on strategic aspects like business risk and adversarial threats within the NIST Artificial Intelligence (AI) Risk Management Framework's (RMF) (2023) functions, categories, and subcategories, and the technical tribe, centered on tactical elements like technical risk and adversarial Tools, Techniques, and Procedures (TTPs) within MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems' (ATLAS) (2023) tactics, techniques, and subtechniques, is crucial. Both tribes, encompassing role characteristics from *Strategic, BISO, Fusion, CRISC, ERM, Intelligence Analysis* to *Tactical, CISO, SOC, CISSP, CSRM, and Incident Responders*, often operate in silos, a challenge highlighted by De Waal et al. (2019) as fostering a "silo mentality" akin to tribal allegiances, impeding collaboration and organizational learning. Bolton (2020) underscores that such entrenched modalities mirror inter-tribal conflicts, reinforcing misperceptions and tribalism, while Bento et al. (2020) stressed that these mentalities hinder organizational performance, sustainability, and growth. Addressing this requires an exploratory qualitative approach integrating ethnography, netnography, and phenomenology, focusing on thematic analysis, to transcend traditional barriers, fostering a collaborative environment crucial for effective risk management and cybersecurity resilience in any organization, public or private.

Integrating the NIST AI RMF's (2023) 4 functions, 19 categories, and 72 subcategories with MITRE ATLAS's (2023) 14 attack tactics, 56 techniques, and numerous sub-techniques presents a holistic framework for AI risk management. NIST AI RMF's comprehensive coverage, ranging from governance, accountability, and risk mapping to impact characterization, aligns strategically with MITRE ATLAS's focus on technical security aspects, including adversarial threat TTPs and vulnerabilities. For example, the "Govern *GV*" function in NIST AI RMF, emphasizing clear policies and responsibility, complements ATLAS's tactics like Reconnaissance, which involves identifying vulnerabilities through public research or websites. This synergy enables the Strategic, BISO, and ERM to align their focus on business risks and adversarial threat actors with the Technical, CISO, and CSRM to align their focus on adversarial threat TTPs, vulnerabilities, and the attack surface. Such an integrated approach is vital for public and private organizations, transcending operational and financial limits and ensuring a robust, comprehensive AI risk management strategy combining strategic business considerations with technical security measures.

Systematically bridging the gap between the business and technical tribes in cybersecurity, as exemplified by integrating NIST AI RMF and MITRE ATLAS frameworks, effectively dismantles silos, significantly enhancing the efficiency and precision of business operations. This integration blends strategic business risk management with tactical, technical security, aligning functions like Govern from NIST AI RMF with tactics such as Reconnaissance in MITRE ATLAS. This cross-cultural approach fosters understanding and collaboration across tribes, breaking down the "silo mentality" that De Waal et al. (2019) identified as a barrier to organizational learning and growth. Bolton (2020) noted that overcoming these entrenched modalities reduces inter-tribal conflicts and misperceptions, promoting a more unified

organizational culture. Bento et al. (2020) further emphasized that breaking down these silos is crucial for enhancing organizational performance and sustainability. A cohesive strategy from this synergy, transcending traditional operational and financial constraints, is crucial for the public and private sectors, ensuring a comprehensive, robust Governance, Risk, and Compliance (GRC) AI framework. This systemic collaboration not only bolsters cybersecurity resilience but also drives overall business efficiency and effectiveness, proving that smashing silos is not just a theoretical ideal but a practical, beneficial necessity for modern organizations.

Innovation and Correlation Smashes Silos

To create a system and method for Key Risk Indicators (KRIs) that inform Key Performance Indicators (KPIs), we first must align each MITRE ATLAS Tactic with one or more NIST AI RMF Functions. This alignment helps identify specific business Governance, Risk, and Compliance (GRC) concerns within each function, providing a systematic approach.

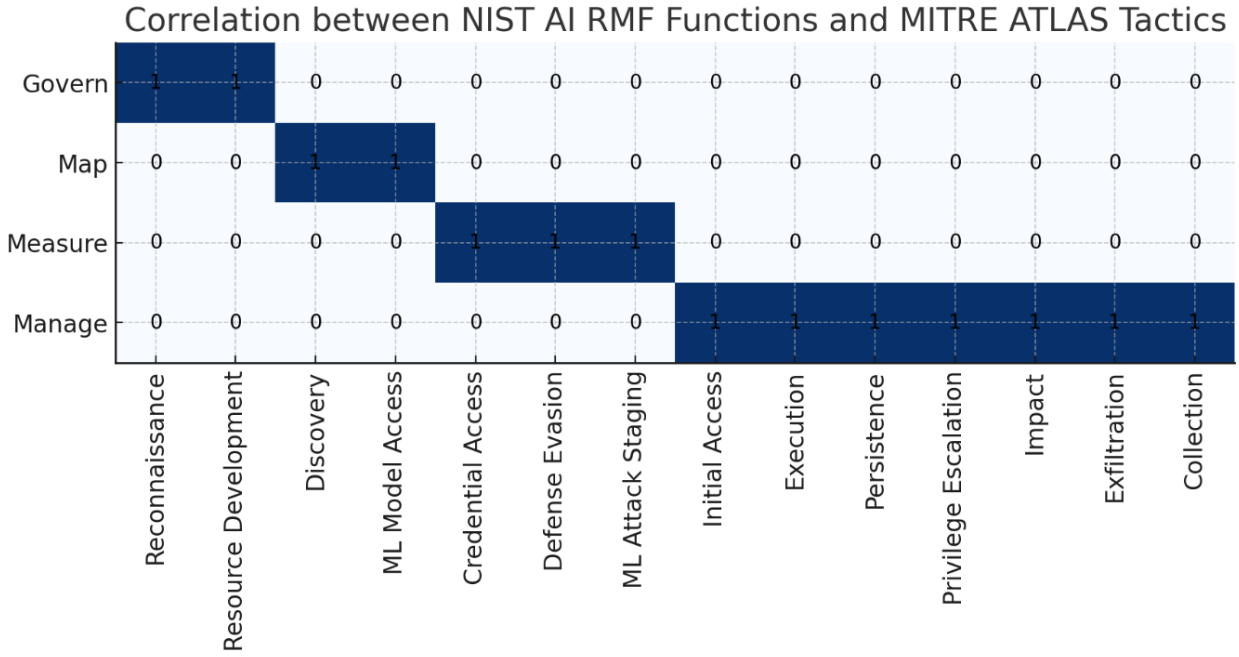

Figure 5. NIST AI RMF correlation with MITRE ATLAS

By aligning MITRE ATLAS tactics with the corresponding NIST AI RMF functions, organizations can develop specific KRIs, which inform the development of effective KPIs for overall Enterprise Risk Management (ERM) AI strategic business risk. This alignment ensures a comprehensive approach to managing Cybersecurity Risk Management (CSRM) AI technical security risks, covering critical factors from governance and mapping to measurement and management. The *Figure 5* graph illustrates intersections where each cell in the matrix represents whether a specific ATLAS Tactic (column) correlates with a NIST AI RMF Function (row). A filled blue cell indicates a correlation, making it clear how each function aligns with specific tactics:

Govern GV: This function correlates with "Reconnaissance" and "Resource Development" tactics, focusing on understanding adversarial threats and managing resources for GRC AI.

Map MP: This involves "Discovery" and "ML Model Access," which are crucial for understanding the AI system's environment and access vulnerabilities.

Measure MS: Associated with "Credential Access," "Defense Evasion," and "ML Attack Staging," this function emphasizes the importance of measuring security controls and system vulnerabilities.

Manage MG: The most extensive function, it covers "Initial Access," "Execution," "Persistence," "Privilege Escalation," "Impact," "Exfiltration," and "Collection," focusing on managing various aspects of ERM and CSRM risk through mitigation strategies and response.

This visual representation mirrors the style of business intelligence dashboards such as “heatmaps” used in executive decision-making. It provides a clear overview of the comprehensive strategy required to manage AI business risks and adversarial threats, comprising detail in financials to harms, encompassing everything from governance to technical response.

This format is crucial for executive leaders, policy-makers, and legislators, as it helps them grasp how GRC-based AI cybersecurity frameworks align with their strategic goals.

Key Risk Indicators (KRIs) to Key Performance Indicators (KPIs)

Govern GV - Involves establishing and maintaining a governance structure that effectively manages AI risks.

- ***Reconnaissance:*** This tactic correlates with "Govern" as it involves understanding the adversarial threats' motivations and interests leading to prioritized targeting the AI system, which is essential for formulating governance policies. ***KRI:*** Frequency of identified external or internal adversarial threats. ***KPI:*** Effectiveness of implemented governance policies in mitigating identified threats.
- ***Resource Development:*** Aligns with "Govern" as it encompasses the management of resources, both internal and external, crucial for AI risk governance. ***KRI:*** Adequacy of resources for AI risk management. ***KPI:*** Efficiency in resource allocation and utilization for risk governance activities.

Map MP - Focuses on understanding the context and environment in which AI systems operate.

- ***Discovery:*** Aligns with "Map" as it involves discovering details about the AI system and its environment, which is crucial for mapping the risk landscape. ***KRI:*** Completeness of environmental and system data collected. ***KPI:*** Accuracy of risk landscape mapping based on collected data.
- ***ML Model Access:*** This tactic is related to "Map" as it involves understanding how access to the ML model can be obtained, which is essential for mapping the system's vulnerabilities. ***KRI:*** Number of unauthorized access attempts to ML

models. ***KPI:*** Effectiveness of controls in restricting ML model access to authorized personnel only.

Measure MS - Involves the application of metrics and measurements to evaluate the effectiveness of AI risk management.

- ***Credential Access:*** Correlates with "Measure" as it requires measuring the security of credentials and access control mechanisms. ***KRI:*** Incidents of compromised credentials. ***KPI:*** Success rate of detecting and responding to credential compromises.
- ***Defense Evasion:*** Aligns with "Measure" as it involves tactics to evade detection, necessitating the measurement of the system's ability to detect and respond to such tactics. ***KRI:*** Frequency of undetected malicious activities. ***KPI:*** Improvement in detection rates of evasion tactics.
- ***ML Attack Staging:*** Related to "Measure" as it involves preparing attacks against AI systems, which requires the measurement of system vulnerabilities and response capabilities. ***KRI:*** Number of vulnerabilities identified during attack simulations. ***KPI:*** Reduction in exploitable vulnerabilities post-simulation.

Manage MG - Entails the ongoing management of AI risks through response and mitigation strategies.

- ***Initial Access:*** Correlates with "Manage" as it involves gaining initial entry into the system, requiring access points and vulnerability management. ***KRI:*** Number of successful unauthorized access incidents. ***KPI:*** Effectiveness of access control measures in preventing unauthorized entries.

- ***Execution:*** Aligns with "Manage" as it involves executing a cyber attack, necessitating the management of system defenses and response strategies. ***KRI:*** Number of successful attacks. ***KPI:*** Reduction in successful attacks due to improved defense strategies.
- ***Persistence:*** Correlates with "Manage" as it involves maintaining a presence in the AI system, requiring ongoing risk management to detect and eradicate such threats. ***KRI:*** Duration of undetected malicious presence in systems. ***KPI:*** Reduction in time taken to detect and eradicate threats.
- ***Privilege Escalation:*** Aligns with "Manage" as it entails managing system privileges to prevent unauthorized escalation. ***KRI:*** Incidents of unauthorized privilege escalation. ***KPI:*** Effectiveness of privilege management controls.
- ***Impact:*** This tactic correlates with "Manage" as it involves dealing with the impacts of an attack, which is central to risk management and response strategies. ***KRI:*** Extent of damage caused by attacks. ***KPI:*** Efficiency of response and recovery strategies in minimizing attack impacts.
- ***Exfiltration:*** Relates to "Manage" as it involves managing how data is protected to prevent unauthorized exfiltration. ***KRI:*** Amount of data exfiltrated during breaches. ***KPI:*** Effectiveness of data loss prevention measures.
- ***Collection:*** Aligns with "Manage" as it involves collecting data from compromised systems, necessitating data security management and leakage prevention. ***KRI:*** Incidents of data leakage from compromised systems. ***KPI:*** Success in securing data and preventing unauthorized data collection.

References

Abdullah, H. (2019). Analyzing the technological challenges of governance, risk and compliance (GRC). *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*. https://doi.org/10.1109/iceeccot46775.2019.9114642

Addeo, F., Delli Paoli, A., Esposito, M., & Ylenia Bolcato, M. (2019). Doing Social Research on online communities: the benefits of Netnography. *ATHENS JOURNAL OF SOCIAL SCIENCES*, *7*(1), 9–38. https://doi.org/10.30958/ajss.7-1-1

Allen, J., An, H., Bose, R., de Beaumont, W., & Teng, C. M. (2022). Collie: A broad-coverage ontology and lexicon of verbs in English. *Language Resources and Evaluation*, *57*(1), 57–86. https://doi.org/10.1007/s10579-022-09600-9

Allison, J. (2023). Devising a cyber security management module through Integrated Course Design. *Journal of Further and Higher Education*, 1–15. https://doi.org/10.1080/0309877x.2023.2250729

Alwaheidi, M. K., Islam, S., & Papastergiou, S. (2022). A conceptual model for data-driven threat analysis for enhancing cyber security. *Advances in Intelligent Systems and Computing*, 365–374. https://doi.org/10.1007/978-3-031-14054-9_34

Amazon. (2023a). *What are Large Language Models (LLM)?* https://aws.amazon.com/what-is/large-language-model/

Amazon. (2023b). *What is GPT?* Generative AI Machine Learning & AI. https://aws.amazon.com/what-is/gpt/

Ardil, C. (2021). A comparative analysis of multiple criteria decision making analysis methods for strategic, tactical, and operational decisions in military fighter aircraft selection. *International Journal of Aerospace and Mechanical Engineering*, *14*(7), 275-288.

Arnold, R., Carey, K., Abruzzo, B., & Korpela, C. (2019). What is a robot swarm: A definition for swarming robotics. *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. https://doi.org/10.1109/uemcon47517.2019.8993024

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946. https://doi.org/10.1016/j.comnet.2019.106946

Barreto, F., Moharkar, L., Shirodkar, M., Sarode, V., Gonsalves, S., & Johns, A. (2023). Generative Artificial Intelligence: Opportunities and challenges of large language models.

Intelligent Computing and Networking, 545–553. https://doi.org/10.1007/978-981-99-3177-4_41

Barry, E. S., Merkebu, J., & Varpio, L. (2022). Understanding state-of-the-art literature reviews. *Journal of Graduate Medical Education*, *14*(6), 659–662. https://doi.org/10.4300/jgme-d-22-00705.1

Bentil, W., Liew, C. L., & Chawner, B. (2021). The management and the usage of electronic resources in academic libraries: A bi-directional relationship. *Information Development*, *38*(1), 114–124. https://doi.org/10.1177/0266666920983600

Bento, F., Tagliabue, M., & Lorenzo, F. (2020). Organizational silos: A scoping review informed by a behavioral perspective on systems and Networks. *Societies*, *10*(3), 56. https://doi.org/10.3390/soc10030056

Bocken, N. M. P., & Geradts, T. H. J. (2020). Barriers and drivers to Sustainable Business Model Innovation: Organization Design and dynamic capabilities. *Long Range Planning*, *53*(4), 101950. https://doi.org/10.1016/j.lrp.2019.101950

Boddington, P. (2023). Towards the future with ai: Work and superintelligence. *Artificial Intelligence: Foundations, Theory, and Algorithms*, 409–456. https://doi.org/10.1007/978-981-19-9382-4_10

Bolton, D. (2020). Targeting ontological security: Information warfare in the modern age. *Political Psychology*, *42*(1), 127–142. https://doi.org/10.1111/pops.12691

Bruni, E., & Comacchio, A. (2023). Configuring a new business model through conceptual combination: The rise of the Huffington Post. *Long Range Planning*, *56*(1), 102249. https://doi.org/10.1016/j.lrp.2022.102249

Cambridge University. (2023a). *Acumen | Definition in the Cambridge English Dictionary*. Cambridge University Press & Assessment. https://dictionary.cambridge.org/us/dictionary/english/acumen

Cambridge University. (2023b). *Lexicon | Definition in the Cambridge English Dictionary*. Cambridge University Press & Assessment. https://dictionary.cambridge.org/us/dictionary/english/lexicon

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for Critical Infrastructure cyber-security: A systematic literature review. *Information & Computer Security*, *29*(5), 697–723. https://doi.org/10.1108/ics-07-2020-0121

CIO Council. (2023). *CISO Handbook*. Chief Information Security Officer. https://www.cio.gov/assets/resources/CISO_Handbook.pdf

Ciriello, R. F., Richter, A., & Mathiassen, L. (2024). Emergence of creativity in is development teams: A socio-technical systems perspective. *International Journal of Information Management, 74*, 102698. https://doi.org/10.1016/j.ijinfomgt.2023.102698

Clark, C. J., & Winegard, B. M. (2020). Tribalism in war and peace: The nature and evolution of ideological epistemology and its significance for modern social science. *Psychological Inquiry*, *31*(1), 1–22. https://doi.org/10.1080/1047840x.2020.1721233

Craig, A. (2020). *Capabilities and conflict in the cyber domain: An empirical study* (dissertation). Cardiff University, Cardiff CF10 3AT, UK. Retrieved from https://orca.cardiff.ac.uk/id/eprint/136860/1/2020CraigAPhD.pdf.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Crespo-Martinez, P. E. (2019). Selecting the business information security officer with ecu@risk and the Critical Role Model. *Advances in Intelligent Systems and Computing*, 368–377. https://doi.org/10.1007/978-3-030-20154-8_34

Cyber AI & Automation summit. (2023). *Cyber AI & Automation Summit*. Agenda. https://cyberai.securityweek.com/en/#agenda

Danos, N., Staab, K. L., & Whitenack, L. B. (2022). The Core Concepts, competencies, and grand challenges of comparative vertebrate anatomy and morphology. *Integrative Organismal Biology*, *4*(1). https://doi.org/10.1093/iob/obac019

De Waal, A., Weaver, M., Day, T., & Van der Heijden, B. (2019). Silo-Busting: Overcoming the Greatest Threat to Organizational Performance. *Sustainability*, *11*(23), 1–21. https://doi.org/10.3390/su11236860

Department of Defense. (2023). *DoD Cyber Workforce Roles*. DoD. https://public.cyber.mil/wid/dcwf/work-roles-2/

Dove, N. (2021). *The BISO Role: Where Business Meets Security*. IANS Faculty. https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/11/04/the-biso-role-where-business-meets-security

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Ehlers, R. S., & Blannin, P. (2020). Making Sense of the Information Environment. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/making-sense-information-environment

Elia, G., Margherita, A., & Passiante, G. (2020). Digital Entrepreneurship Ecosystem: How Digital Technologies and collective intelligence are reshaping the entrepreneurial process. *Technological Forecasting and Social Change*, *150*, 119791. https://doi.org/10.1016/j.techfore.2019.119791

Ettinger, J., Galyardt, A., Gupta, R., DeCapria, D., Kanal, E., Klinedinst, D. J., Shick, D., Perl, S. J., Dobson, G. B., Sanders, G., Costa, D. L., Rogers, L., Barmer, H., Kane, J., Evans, H., Brandon, E., Mellinger, A. O., & Institute, S. E. (2019). *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States (study report and implementation guides)*. SEI Digital Library. https://insights.sei.cmu.edu/library/cyber-intelligence-tradecraft-report-the-state-of-cyber-intelligence-practices-in-the-united-states-study-report-and-implementation-guides/

Fan, F.-L., Xiong, J., Li, M., & Wang, G. (2021). On interpretability of Artificial Neural Networks: A survey. *IEEE Transactions on Radiation and Plasma Medical Sciences*, *5*(6), 741–760. https://doi.org/10.1109/trpms.2021.3066428

Furnell, S. (2021). The cybersecurity workforce and Skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Garcia, P., Fernández, C., & Okonkwo, H. (2020). Leveraging Technology: How black girls enact critical digital literacies for Social Change. *Learning, Media and Technology*, *45*(4), 345–362. https://doi.org/10.1080/17439884.2020.1773851

Gomez, M. A., & Whyte, C. (2022). Unpacking strategic behavior in Cyberspace: A schema-driven approach. *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac005

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*. https://doi.org/10.3389/fdata.2021.583723

Hamad, F., Al-Aamr, R., Jabbar, S. A., & Fakhuri, H. (2020). Business intelligence in academic libraries in Jordan: Opportunities and challenges. *IFLA Journal*, *47*(1), 37–50. https://doi.org/10.1177/0340035220931882

HPE. (2023). *What is Swarm Intelligence?* Swarm Intelligence. https://www.hpe.com/us/en/what-is/swarm-intelligence.html

Huo, S., Mukherjee, K., Bandlamudi, J., Isahagian, V., Muthusamy, V., & Rizk, Y. (2023). Accelerating the support of conversational interfaces for rpas through apis. *Lecture Notes in Business Information Processing*, 165–180. https://doi.org/10.1007/978-3-031-43433-4_11

IBM. (2023a). *What is natural language processing (NLP)?* Think. https://www.ibm.com/topics/natural-language-processing

IBM. (2023b). *What is robotic process automation (RPA)?* Think. https://www.ibm.com/topics/rpa

ISC2. (2023). *CISSP - certified Information Systems Security professional*. CISSP. https://www.isc2.org/certifications/cissp

Ivančić, L., Vukšić, V., & Spremić, M. (2019). Mastering the digital transformation process: Business practices and lessons learned. *Technology Innovation Management Review*, *9*(2), 36–50. https://doi.org/10.22215/timreview/1217

Jandrić, P. (2020). A peer-reviewed scholarly article. *Postdigital Science and Education, 3*(1), 36–47. https://doi.org/10.1007/s42438-020-00202-8

Kaloudi, N., & Li, J. (2020). The AI-based Cyber Threat Landscape. *ACM Computing Surveys, 53*(1), 1–34. https://doi.org/10.1145/3372823

Kappers, W., & Harrell, M. (2020). From degree to chief information security officer (CISO): A Framework for consideration. *2020 ASEE Virtual Annual Conference Content Access Proceedings*. https://doi.org/10.18260/1-2--34694

Khalifa, A. S. (2021). Strategy and what it means to be strategic: Redefining strategic, operational, and Tactical Decisions. *Journal of Strategy and Management*, *14*(4), 381–396. https://doi.org/10.1108/jsma-12-2020-0357

Klemas, T., Atkins, S., Lively, R. K., & Choucri, N. (2021). Accelerating cyber acquisitions: Introducing a time-driven approach to manage risks with less delay. *ITEA Journal of Test and Evaluation*, *42*, 194–202. https://dspace.mit.edu/handle/1721.1/141745

Kollars, I., & Schechter, B. (2022). *Pathologies of Obfuscation: Nobody Understands Cyber Operations or Wargaming*. Scowcroft Center for Strategy and Security. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/pathologies-of-obfuscation-nobody-understands-cyber-operations-or-wargaming/

Kure, H. I., & Nwajana, A. O. (2022). Protection of critical infrastructure using an integrated cybersecurity risk management (I-CSRM) framework. *Advances in Computer and Electrical Engineering*, 94–133. https://doi.org/10.4018/978-1-6684-3855-8.ch004

Lawrence, I. (2021). Origins of the C-suite. *The 'C-Suite' Executive Leader in Sport: Contemporary Global Challenges for Elite Professionals*, 1–25. https://doi.org/10.1108/978-1-83909-698-320211001

Li, C., Gan, Z., Yang, Z., Yang, J., Li, L., Wang, L., & Gao, J. (2023). Multimodal Foundation Models: From Specialists to General-Purpose Assistants. Computer Science > Computer Vision and Pattern Recognition. *Arxiv*. https://doi.org/10.48550/arXiv.2309.10020

Li, L. (2022). Reskilling and upskilling the future-ready workforce for Industry 4.0 and Beyond. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10308-y

Lutz, B., & Paretti, M. C. (2021). Exploring the social and cultural dimensions of learning for recent engineering graduates during the school-to-work transition. *Engineering Studies*, *13*(2), 132–157. https://doi.org/10.1080/19378629.2021.1957901

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-Technical Systems Cybersecurity Framework. *Information & Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ics-03-2018-0031

McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, *134*, 103424. https://doi.org/10.1016/j.cose.2023.103424

McLean, S., Read, G. J., Thompson, J., Baber, C., Stanton, N. A., & Salmon, P. M. (2021). The risks associated with Artificial General Intelligence: A systematic review. *Journal of Experimental & Theoretical Artificial Intelligence*, *35*(5), 649–663. https://doi.org/10.1080/0952813x.2021.1964003

MITRE. 2023. Adversarial Threat Landscape for Artificial-Intelligence Systems, ATLAS. https://atlas.mitre.org/

Morrison-Smith, S., & Ruiz, J. (2020). Challenges and barriers in virtual teams: A literature review. *SN Applied Sciences*, *2*(6). https://doi.org/10.1007/s42452-020-2801-5

Musiani, F. (2022). Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, *25*(6), 785–800. https://doi.org/10.1080/1369118x.2022.2049850

Naseem, S., Alhudhaif, A., Anwar, M., Qureshi, K. N., & Jeon, G. (2022). Artificial general intelligence-based rational behavior detection using cognitive correlates for tracking online harms. *Personal and Ubiquitous Computing*, *27*(1), 119–137. https://doi.org/10.1007/s00779-022-01665-1

NIST. (2023). *AI RMF playbook*. NIST. https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook

Otgonpurev, M. (2021). *Effective application of Natural Language Processing techniques in Automated Cyber Threat Intelligence*. Graduate School of Informatics. https://nagoya.repo.nii.ac.jp/record/2000258/files/k13447_thesis.pdf

Ozuem, W., Willis, M., & Howell, K. (2022). Thematic analysis without paradox: Sensemaking and context. *Qualitative Market Research: An International Journal*, *25*(1), 143–157. https://doi.org/10.1108/qmr-07-2021-0092

Parker, A., & Brown, I. (2019). Skills Requirements for Cyber Security Professionals: A content analysis of job descriptions in South Africa. *Communications in Computer and Information Science*, 176–192. https://doi.org/10.1007/978-3-030-11407-7_13

Penning de Vries, B. B. L., van Smeden, M., Rosendaal, F. R., & Groenwold, R. H. H. (2020). Title, abstract, and keyword searching resulted in poor recovery of articles in systematic reviews of epidemiologic practice. *Journal of Clinical Epidemiology*, *121*, 55–61. https://doi.org/10.1016/j.jclinepi.2020.01.009

Peters, M. D. J., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., McInerney, P., Godfrey, C. M., & Khalil, H. (2021). Updated methodological guidance for the conduct of scoping reviews. *JBI Evidence Implementation*, *19*(1), 3–10. https://doi.org/10.1097/xeb.0000000000000277

Pierre, H. (2020). Business and corporate security: Contributing to a safer world. *International Security Management*, 277–289. https://doi.org/10.1007/978-3-030-42523-4_19

Pietruszka-Ortyl, A., Ćwiek, M., Ziębicki, B., & Wójcik-Karpacz, A. (2021). Organizational culture as a prerequisite for knowledge transfer among IT professionals: The case of energy companies. *Energies*, *14*(23), 8139. https://doi.org/10.3390/en14238139

Psaroulis, G. (2022). *Leadership in Organisational Cyber Security*. Digital Library. https://digital.library.adelaide.edu.au/dspace/bitstream/2440/136018/1/Psaroulis2022_PhD.pdf

Purohit, A. (2023). *AI, ML, DL, and Generative AI Face Off: A Comparative Analysis*. Data Insights. https://synoptek.com/insights/it-blogs/data-insights/ai-ml-dl-and-generative-ai-face-off-a-comparative-analysis/

Quinn, S., Ivy, N., Barrett, M., Witte, G., & Gardner, R. K. (2022). *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*. https://doi.org/10.6028/nist.ir.8286c

Ragas, M. (2019). Defining 'Business Acumen': A Delphi Study of Corporate Communications Leaders. *Public Relations Journal*, *13*(1), 2–3. https://prjournal.instituteforpr.org/wp-content/uploads/Business-Acumen-Ragas.pdf

Romanosky, S., & Petrun Sayers, E. L. (2023). Enterprise risk management: How Do Firms Integrate Cyber Risk? *Management Research Review*. https://doi.org/10.1108/mrr-10-2021-0774

Rosenberg, L., Willcox, G., & Schumann, H. (2023a). Towards Collective Superintelligence, a Pilot Study. *ARXIV*. https://doi.org/ https://doi.org/10.48550/arXiv.2311.00728

Rosenberg, L., Willcox, G., Schumann, H., & Mani, G. (2023b). Conversational Swarm Intelligence (CSI) Enhances Groupwise Deliberation. *ARXIV*. https://doi.org/10.48550/arXiv.2309.12366

Rosenbush, S. (2023). *CIOs Look Past the OpenAI Drama*. CIO Journal. https://www.wsj.com/articles/cios-look-past-the-openai-drama-8c3b976e?mod=tech_lead_story

Scrut Automation. (2023). *The impact of AI and ML on modern GRC Solutions V2*. ScrutIO. https://www.scrut.io/wp-content/uploads/2023/05/The-impact-of-AI-and-ML-on-modern-GRC-solutions-V2.pdf

Sharma, S., & Ahlawat, A. (2022). Architecture and types of intelligent agent and uses of various technologies. *2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. https://doi.org/10.1109/icict55121.2022.10064524

Sharma, P., & Goel, S. (2023). Front matter. *A Practical Guide on Security and Privacy in Cyber-Physical Systems*, i–xxii. https://doi.org/10.1142/9789811273551_fmatter

Solomon, M. (2022). *The Third Building Block for the SOC of the Future: Balanced Automation*. Incident Response. https://www.securityweek.com/third-building-block-soc-future-balanced-automation/

Solomon, M. (2023). *Burn and Churn: CISOs and the Role of Cybersecurity Automation*. CISO Strategy. https://www.securityweek.com/burn-and-churn-cisos-and-the-role-of-cybersecurity-automation/

Stancin, K., Poscic, P., & Jaksic, D. (2020). Ontologies in Education – State of the art. *Education and Information Technologies*, *25*(6), 5301–5320. https://doi.org/10.1007/s10639-020-10226-z

Stanford University. (2020). *Artificial Intelligence Definitions*. Human-Centered Artificial Intelligence (HAI). https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. https://doi.org/10.6028/nist.ir.8286

Sudharson, D., Bhuvaneshwaran, A., Kalaiarasan, T., Satheesh, D. K., Sushmita, S., & Jyothi, N. L. (2023). A multimodal AI framework for Hyper Automation in industry 5.0. *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*. https://doi.org/10.1109/icidca56705.2023.10099581

Sundler, A. J., Lindberg, E., Nilsson, C., & Palmér, L. (2019). Qualitative thematic analysis based on descriptive phenomenology. *Nursing Open*, *6*(3), 733–739. https://doi.org/10.1002/nop2.275

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). *NIST AI 100-1*. https://doi.org/10.6028/nist.ai.100-1

Thomas, O. O., & Lawal, O. R. (2020). Exploratory research design in management sciences: An X-ray of literature. *Annals of Dunarea de Jos University of Galati. Fascicle I. Economics and Applied Informatics*, *26*(2), 79–84. https://doi.org/10.35219/eai15840409109

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

United States Air Force. (2020). *Foreign Internal Defense*. Air Force Doctrine Publication (AFDP) 3-22. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-22/3-22-AFDP-FID.pdf

USG. (2024a). *NIST Request for Information (RFI) Executive Order (EO) 14110*. Federal Register. https://www.federalregister.gov/documents/2023/12/21/2023-28232/request-for-information-rfi-related-to-nists-assignments-under-sections-41-45-and-11-of-the

USG. (2024b). *EO 14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Federal Register. https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

Urso, G. (2020). Metropolisation and the challenge of rural-urban dichotomies. *Urban Geography*, *42*(1), 37–57. https://doi.org/10.1080/02723638.2020.1760536

Uszkoreit, J. (2017). *Transformer: A Novel Neural Network Architecture for Language Understanding*. Research Blog. https://blog.research.google/2017/08/transformer-novel-neural-network.html

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention Is All You Need. 31st Conference on Neural Information Processing Systems. *Arxiv*. https://doi.org/10.48550/arXiv.1706.037

Verganti, R., Dell'Era, C., & Swan, K. S. (2021). Design thinking: Critical analysis and future evolution. *Journal of Product Innovation Management*, *38*(6), 603–622. https://doi.org/10.1111/jpim.12610

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A systematic study and open challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/access.2020.3045514

Von Rosing, M., & Laurier, W. (2020). An introduction to the business ontology. *Sustainable Business*, 1–24. https://doi.org/10.4018/978-1-5225-9615-8.ch001

Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet of Things Journal*, *10*(16), 14671–14688. https://doi.org/10.1109/jiot.2023.3278329

Wehn, U., & Almomani, A. (2019). Incentives and barriers for participation in community-based environmental monitoring and information systems: A critical analysis and integration of the literature. *Environmental Science & Policy*, *101*, 341–357. https://doi.org/10.1016/j.envsci.2019.09.002

Werber, L., Ausink, J. A., Daugherty, L., Phillips, B., Knutson, F., & Haberman, R. (2019). *An Assessment of Gaps in Business Acumen and Knowledge of Industry Within the Defense Acquisition Workforce*. Research Reports. https://www.rand.org/pubs/research_reports/RR2825.html

White, S. P. (2019). *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine* (dissertation). Proquest, Ann Arbor, MI. Retrieved from https://www.proquest.com/openview/9b5581ccd254b08ca2c9dfe35c67b7de/1?pq-origsite=gscholar&cbl=44156.

Whyte, C. (2020). Problems of poison: New paradigms and "agreed" competition in the era of AI-enabled Cyber Operations. *2020 12th International Conference on Cyber Conflict (CyCon)*. https://doi.org/10.23919/cycon49761.2020.9131717

Wiedemann, A., Wiesche, M., & Krcmar, H. (2019). Integrating development and operations in cross-functional teams - toward a devops competency model. *Proceedings of the 2019 on Computers and People Research Conference*, 14–19. https://doi.org/10.1145/3322385.3322400

Wise, A. F., Knight, S., & Ochoa, X. (2021). What makes learning analytics research matter. *Journal of Learning Analytics*, *8*(3), 1–9. https://doi.org/10.18608/jla.2021.7647

Work, J. (2020). Evaluating commercial cyber intelligence activity. *International Journal of Intelligence and CounterIntelligence*, *33*(2), 278–308. https://doi.org/10.1080/08850607.2019.1690877

Wu, C., Zhang, R., Kotagiri, R., & Bouvry, P. (2023). Strategic decisions: Survey, taxonomy, and future directions from Artificial Intelligence Perspective. *ACM Computing Surveys*, *55*(12), 1–30. https://doi.org/10.1145/3571807

Xi, Z., Chen, W., Guo, X., He, W., Ding, Y., & Hong, B. (2023). The Rise and Potential of Large Language Model Based Agents: A Survey. *Arxiv*. https://doi.org/https://doi.org/10.48550/arXiv.2309.07864

Xie, Y., Sattari, K., Zhang, C., & Lin, J. (2023). Toward Autonomous Laboratories: Convergence of Artificial Intelligence and Experimental Automation. *Progress in Materials Science*, *132*, 101043. https://doi.org/10.1016/j.pmatsci.2022.101043

Zeng, F., Gan, W., Wang, Y., Liu, N., & Yu, P. S. (2023). Large Language Models for Robotics: A Survey. *Arxiv*. https://doi.org/https://doi.org/10.48550/arXiv.2311.07226

Zhang, C., Lu, J., & Zhao, Y. (2024). Generative pre-trained Transformers (gpt)-based automated data mining for building energy management: Advantages, limitations and the future. *Energy and Built Environment*, *5*(1), 143–169. https://doi.org/10.1016/j.enbenv.2023.06.005