The Role of PMOs in the AI Adoption Journey in the Energy Sector: An Exploratory Case Study

Dissertation Manuscript

Submitted to National University

School of Business and Economics

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

ANTONY PETER AMALRAJ

San Diego, California

September 2025

Abstract

Project management offices (PMOs) are increasingly central to driving strategic alignment and ensuring the successful execution of complex initiatives in the energy sector. As the industry transitions toward renewable energy, infrastructure modernization, and sustainability, PMOs play a vital role in addressing the risks linked to emerging technologies. The U.S. Department of Energy (DOE) identifies artificial intelligence (AI) as a catalyst for grid modernization and decarbonization, aligning with global perspectives that AI will transform project management. The problem this study addressed was the energy sector's challenges in adopting AI to meet decarbonization targets due to cybersecurity risks. Cybersecurity is critical because of the sector's role in national security, economic stability, and public safety. The purpose of this qualitative study was to explore how PMOs can help mitigate the cybersecurity risks associated with AI adoption during the transition to renewable energy. A qualitative methodology and exploratory case study design were utilized to examine the PMO's role in addressing these risks. Building on prior research, this study applied an integrated framework, TAI-Cybersecurity PRM, which embeds context-based cybersecurity risk management into the TAI-PRM process. This framework provides a systematic approach to strengthening security posture when implementing AI technologies. The analysis drew on DOE reports on AI and cybersecurity, along with insights from experienced U.S.-based energy professionals recruited through purposive sampling. The research question guiding the study was: How can PMOs assist in mitigating cybersecurity risks when adopting AI during the transition to renewable energy in the energy sector? The findings were organized into five themes: Trustworthy AI, Context Understanding, Cybersecurity Risks, Risk Management, and the Project Management Office. From these, five categories of practice recommendations emerged: building trustworthy AI, applying a risk-based approach, mitigating

cybersecurity threats, increasing awareness of AI-related risks, and strengthening PMO engagement in AI adoption. These recommendations, grounded in existing research and the TAI-Cybersecurity PRM framework, highlight PMOs' strategic role in balancing innovation with security. Finally, opportunities for future research were identified, including expanding generalizability, addressing ethical and privacy risks, evaluating the impact of evolving AI regulations, and conducting quantitative studies to complement the qualitative findings.

Acknowledgements

First and foremost, I am deeply grateful to my wife and best friend, Usha, whose unwavering patience, encouragement, and understanding enabled me to devote the time necessary for this research while balancing family and professional responsibilities. I also extend heartfelt thanks to my sister, Milani, and my children, Sharon, Christie, and Josh, for their constant love and support, which sustained me throughout this journey. The companionship of our puppy, Jagger, brought comfort and lightness during the many long hours of study and writing.

I hold deep gratitude for my late parents and my brother, whose memories continue to inspire me every day in both life and learning. Although they are no longer here, the love, values, and encouragement they gave me formed the foundation for this work. This dissertation reflects their lasting presence in my journey.

I am especially appreciative of my dissertation committee, Dr. Sharon Kimmel, Dr. Chloe Shay, and Dr. Robin Butler, for their expertise, constructive feedback, and mentorship. Their support has been instrumental in shaping the quality and direction of this dissertation. Finally, I offer my sincere thanks to the energy sector experts who participated in this study. Their willingness to share their insights and experiences was vital to the success of this research.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The concept of a project management office (PMO) is widely discussed in the literature. The Project Management Body of Knowledge defines a PMO as a management structure that standardizes project governance processes and facilitates sharing resources, knowledge, and tools (Project Management Institute, 2021). Many organizations in the energy sector increasingly rely on effective PMOs to drive reform, ensuring strategic alignment and successful project execution. PMOs play a crucial role in managing the complexity of large-scale projects, particularly as the sector shifts toward renewable energy sources, infrastructure modernization, and sustainability goals. Despite the widespread acceptance of the PMO concept, industry surveys reveal an average failure rate of 75% for PMOs, with 47% of practitioners viewing them as an overhead cost that adds bureaucracy while contributing little to the business value chain (Ershadi et al., 2021c).

Mahabir et al. (2022) highlighted that ineffective PMO processes can hinder successful project delivery and emphasized the need for a gradual and sustainable approach to maturity. Similarly, the Energy Information Administration (EIA) emphasized the importance of a PMO development model to ensure effective project delivery. Icshan et al.'s (2023) study explored the roles and responsibilities of PMO leaders in Indonesia, revealing that many PMOs were not operating as intended, leading to project failures. They emphasized the importance of clearly defining PMO functions and responsibilities to enhance project success, as these ambiguities often caused inconsistencies in governance, resource management, and oversight.

Ershadi et al. (2021a) examined the critical factors contributing to PMO success and recommended future research in PMO structuring and project management information systems. Almansoori et al. (2021) analyzed the characteristics influencing PMO practices in the

construction industry in the UAE. They called for future research to expand to other sectors to explore PMO's influence on organizational success. Miller (2021) assessed and grouped the success factors in managing AI projects. Due to the study's dependence on a constrained literature pool at a particular moment, Miller proposed additional research to identify shared characteristics capable of adjusting to the changing dynamics of AI initiatives.

Brandes et al. (2023) emphasized that, given the current climate crisis, leveraging AI to manage projects in the energy sector is essential, as the industry is adopting renewable energy technologies. The Department of Energy (DOE) envisions AI's role in modernizing the grid and achieving the decarbonization goal through renewable energy transformation projects. According to a survey of 2314 professionals from 129 countries conducted by Müller et al. (2024), 76% believe that AI will transform the management of projects. Renshaw (2023) testified to the House Energy Subcommittee about the role of AI in the energy sector while highlighting the concerns with data privacy and security and the lack of explainability.

Artificial Intelligence (AI), the Internet of Things (IoT), and cloud computing are key enablers of Industry 4.0. However, since 2021, Industry 5.0 has gradually gained momentum, representing the next stage of industrial evolution (Vyhmeister & Castane, 2024). While leveraging the digital innovations and automation introduced by Industry 4.0, Industry 5.0 focuses on a human-centric model, prioritizing resilience and sustainability. Vyhmeister and Castane (2024) analyzed project risk management concerning trustworthy AI requirements in the manufacturing sector and proposed further research for other industrial sectors. Therefore, there was a strong need for research on the role of PMOs in the AI adoption journey in the energy sector as the industry transitions to renewable energy technologies.

Statement of the Problem

The problem this study addressed was the energy sector's challenges in adopting AI to meet the decarbonization targets by 2030 due to cybersecurity issues. The United Nations' Intergovernmental Panel on Climate Change (IPCC) report highlighted the critical need for substantial carbon emission reductions by 2030 to prevent the severe consequences of climate change (U.S. Net Zero Plan, 2024). In his written testimony to the U.S. House Energy & Commerce Committee, Renshaw (2023) discussed the pressing challenges of cybersecurity and data leaks in adopting AI within the energy sector. Cybersecurity is critical for the energy sector due to its pivotal role in national security, economic stability, and public safety (CISA, 2024). Energy infrastructure is increasingly becoming more digital and interconnected, making it a prime target for cyberattacks. Disruptions in the energy sector caused by cyberattacks can lead to devastating consequences, including blackouts and economic instability, directly impacting public safety. Ershadi et al. (2021a) analyzed theoretical PMO success domains in the construction industry and suggested that "…future research can contextualize the topic by exploring the impact of different industry specifications". Ichsan et al. (2023) studied the role of PMO managers in Indonesian settings and recommended future research on the applicability of the role-based competency framework to other regions and sectors. Previous research on PMOs' influence on organizational success revealed the need for further study considering changing market conditions, more scrutinized regulatory requirements, the ongoing evolution of PMOs, and technological innovations. As the energy sector in the U.S. works to meet the National Grid's decarbonization targets, PMOs are expected to align strategically with organizational priorities. This research aimed to provide meaningful recommendations to organizational and PMO leaders in the energy sector to mitigate cybersecurity risks in adopting AI in renewable energy projects.

Purpose of the Study

The purpose of this qualitative study was to explore how PMOs in the energy sector might assist in mitigating cybersecurity risks associated with AI adoption during the transition to renewable energy, as the industry works to meet its decarbonization goals. By examining industry-specific regulatory requirements, secure design requirements, project management maturity, PMO leadership, organizational structure, and service delivery mechanisms, this study provided insights into how PMOs could align with strategic business objectives, ensure sustainable benefits, and overcome challenges specific to the energy sector in the United States. A qualitative study design was utilized, and narrative data were collected and analyzed to comprehend the nuanced perspectives and experiences of PMO leaders, project managers, program managers, cybersecurity professionals, AI experts, and organizational leaders within the energy sector as the population for sample data. These were intended to represent the multifaceted nature of PMO practices, including project management maturity, leadership dynamics, organizational structures, and value delivery. An estimated sample size of 15 experts, or until data saturation occurs, was considered for this study. By exploring subjective viewpoints and contextual nuances, this study aimed to generate insights into how the energy sector in the United States can benefit from PMO practices in achieving decarbonization targets.

Introduction to Conceptual Framework

Vyhmeister and Castane (2024) considered the trustworthy AI-project risk management (TAI-PRM) framework, which integrated trustworthy AI requirements with project risk management to address ethical risks in AI adoption within the manufacturing sector. As the industry transitioned from Industry 4.0 to 5.0, with a focus on human-centric and sustainable approaches, this framework aligned with that shift. The trustworthy AI principles included

maintaining human oversight, ensuring technical robustness and safety, safeguarding privacy through data governance, promoting transparency in decision-making, fostering diversity, ensuring societal and environmental well-being, and enforcing accountability. The framework was based on Failure Mode and Effects Analysis (FMEA) and the ISO 31000 Risk Management standard.

The FMEA method is a widely used risk assessment tool across industries, including technology, and is useful in managing trustworthy AI (TAI) risks. It offered a holistic view by evaluating potential failures across the system, aligning with TAI's focus on ethical and technical aspects. FMEA helped identify potential hazards by assessing their likelihood and impact, providing a structured approach to uncover hidden risks. It followed a systematic process, ranking risks by severity and developing strategies to address them consistently. Additionally, FMEA supported continuous improvement, allowing for ongoing monitoring and adaptation of risk strategies, which was crucial for maintaining ethical, transparent, and accountable AI systems over time (Vyhmeister & Castane, 2024). While the TAI-PRM framework effectively handled ethical risks, it did not address the cybersecurity risks of adopting AI systems.

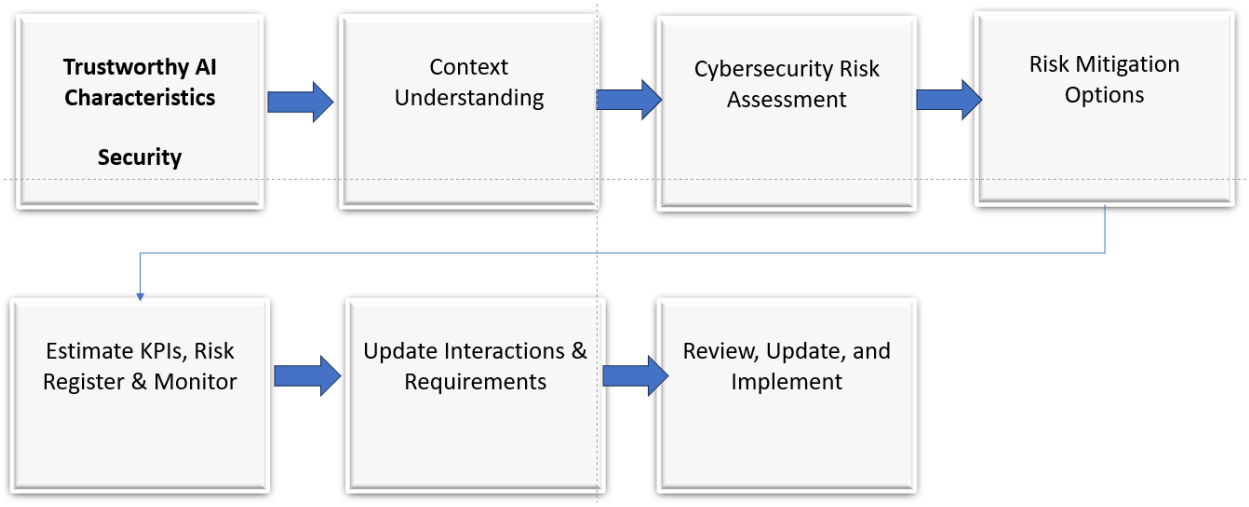
Melaku (2023) compared various cybersecurity frameworks, including NIST, COSO, COBIT 5, ITIL, and ISO 27005, noting their complexity. He considered a new context-based cybersecurity risk management framework that simplified the process by helping organizations identify vulnerabilities, assess potential impacts, and develop risk mitigation strategies to minimize those impacts. By understanding the organization's context, a company could effectively align its security risk management strategy with its overall risk appetite and tolerance, gaining a competitive advantage without impacting business continuity. This deeper understanding of the organizational context also provided insights into the critical IT systems

and business processes likely to be targeted, helping the company better prepare for potential threats (Melaku, 2023).

Building upon this prior research work, this study considered an integrated framework known as the TAI-Cybersecurity PRM. As shown in Figure 1, this framework incorporated context-based cybersecurity risk management into the established TAI-PRM process. By doing so, it aimed to provide a comprehensive approach that enhances the overall security posture when implementing AI technologies and ensures that specific risks are systematically identified, assessed, and mitigated. Security is one of the key characteristics of trustworthy AI. This framework included several key steps: understanding the context, assessing cybersecurity risks, selecting risk mitigation options, estimating KPIs, updating interactions and requirements, and reviewing and implementing the strategy. In the context understanding phase, the cybersecurity risk management strategy was aligned with the organization's risk appetite and tolerance. During the risk assessment phase, security risks were identified, analyzed, and prioritized (Melaku, 2023). Mitigation options were then chosen based on the organization’s risk appetite. In the KPI estimation, risk register, and monitoring phase, KPIs were tied to Trustworthy AI requirements. The update phase analyzed new interactions affecting system trustworthiness and adjusted risks accordingly. Finally, the risk mitigation strategy was implemented once all necessary updates had been made (Vyhmeister & Castane, 2024).

Figure 1

TAI-Cybersecurity PRM Framework



Note. This figure was independently developed by the researcher, Antony Amalraj, to represent the flow of the TAI-Cybersecurity PRM framework.

Introduction to Research Methodology and Design (Nature of the Study)

This research study used a qualitative methodology and an exploratory case study design. The choice of this design was informed by its suitability for examining specific cases within industries and geographic regions, as well as its capacity to address real-life challenges while operating under time constraints (Yin, 2015). Previous research studies in the PMO context have exemplified the significance of leveraging a case study design. For example, Gomo et al. (2020) leveraged a case study design to explore the PMO's role in knowledge transfer. Their research in South Africa, centered on a single large organization, explored how the PMO enabled knowledge transfer within the company. Similarly, Ichsan et al. (2023) utilized a case study design to understand the roles of PMO managers in an Indonesian setting. Almansoori et al. (2021) utilized a case study approach to investigate the role of PMOs within the UAE construction sector.

The participants were recruited through purposive sampling. An estimated sample size of 15 participants included PMO leaders, project managers, program managers, cybersecurity professionals, AI experts, and organizational leaders within the energy sector as the population for sample data. Recruitment involved contacting potential participants through Personal LinkedIn and the Project Management Institute (PMI) local chapter. These platforms were frequented by professionals in the project management field, making them suitable for targeting individuals with relevant experience and knowledge. Specific eligibility criteria were established to ensure the selection of participants who met the study criteria. This included requirements such as having a minimum of 5 years of experience in the energy sector, employment at a U.S.-based energy company, and holding a role as a PMO leader, Project Manager, Program Manager, Cybersecurity Professional, AI expert, or Organizational Leader. By targeting individuals with substantial experience and expertise in the field, the study aimed to capture insights from those well-versed in the challenges and dynamics of PMO operations within the energy sector.

Before data collection began, participants were provided with detailed information about the study objectives, procedures, and their rights as participants. Informed consent was obtained from each participant, ensuring that they understood the purpose of the research and voluntarily agreed to participate. Participants' confidentiality was maintained by assigning pseudonyms or codes to anonymize their identities in research reports and publications. Interviews and published reports from the U.S. Department of Energy on AI and cybersecurity were utilized as data collection methods to investigate the problem. The qualitative instrument of a semi-structured interview guide was prepared. Data saturation was assessed by systematically reviewing and analyzing the collected data, identifying recurring patterns, and determining when thematic saturation had occurred (Yin, 2015).

Research Questions

Research has shown that integrating TAI requirements into the risk management process enables the development and deployment of trustworthy AI systems in the manufacturing sector (Vyhmeister & Castane, 2024). This qualitative study aimed to explore how PMOs in the energy sector might assist in mitigating cybersecurity risks associated with AI adoption during the transition to renewable energy, as the industry works to meet its decarbonization goals.

RQ1

How can PMOs assist in mitigating cybersecurity risks when adopting AI in transitioning to renewable energy sources in the energy sector?

Significance of the Study

The ongoing climate crisis demands urgent and collective action from governments and organizations to achieve substantial carbon emission reductions by 2030. Transitioning to renewable energy and reducing carbon emissions is vital in the energy sector. However, progress is hindered by the sector's slow adoption of AI due to significant cybersecurity concerns (Renshaw, 2023). Given the energy sector's critical role in national security, economic stability, and public safety, it is increasingly becoming a prime target for cyberattacks (CISA, 2024). The integration of digital and interconnected infrastructure heightens vulnerability to these attacks, leading to potential risks such as blackouts, economic instability, and threats to public safety (Bailey et al., 2020). This study was significant as it addressed the intersection of cybersecurity, AI adoption, and project management in the energy sector. This domain was crucial to the global effort against climate change. By exploring how PMOs contributed to mitigating cybersecurity risks in the energy sector during its transition to renewable energy, this research offered insights into a strategic approach to ensure the sector's security and resilience. The findings of this study

could be beneficial for energy organizations and PMOs seeking to enhance project management frameworks, implement effective cybersecurity strategies, and accelerate the adoption of AI technologies while striving to meet decarbonization goals.

Definitions of Key Terms

Trustworthy AI

Trustworthy AI involves designing and implementing AI systems that are secure, reliable, ethical, transparent, and human-focused, and that protect privacy and data governance. It is grounded in seven fundamental principles: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability (Bedué & Fritzsche, 2021; Vyhmeister & Castane, 2024).

Project Management Office

A project management office (PMO) is a centralized body within an organization that governs, supports, and standardizes project management practices across multiple projects. The PMO plays a crucial role in ensuring that projects are aligned with organizational objectives, adhering to best practices, and are completed on time and within budget (Project Management Institute, 2021, p. 211).

Cybersecurity Risks

Cybersecurity risks involve the potential loss of confidentiality, integrity, or availability of information, data, or information systems. These risks can adversely affect organizational operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and even the nation (CSRC, n.d.).

Renewable Energy

Renewable energy refers to energy derived from natural resources, such as bioenergy, geothermal, solar, wind, ocean, and hydropower. This form of energy contributes to sustainable development, enhances energy access and security, and supports economic and social resilience, prosperity, and a climate-resilient future (Renewables, 2024).

Summary

This dissertation explored how PMOs in the energy sector might assist in mitigating cybersecurity risks, while the industry works toward achieving its decarbonization goals through renewable energy projects. As the energy sector sought to adopt AI to enhance operational efficiency and reduce carbon emissions, it faced challenges related to cybersecurity risks. The results of this study could offer valuable guidance to energy organizations and PMOs aiming to strengthen project management frameworks, implement effective cybersecurity strategies, and accelerate the adoption of AI technologies in support of decarbonization efforts. Chapter 2 will discuss the literature review, outlining key theories and concepts related to TAI, cybersecurity risks, and PMOs.

Chapter 2: Literature Review

The purpose of this qualitative study was to explore how PMOs in the energy sector might assist in mitigating cybersecurity risks associated with AI adoption during the transition to renewable energy, as the industry works to meet its decarbonization goals. The energy sector, responsible for 75% of global greenhouse gas emissions, is under immense pressure to reduce its carbon footprint (EIA, 2023). Key contributors included heavy reliance on fossil fuels, outdated infrastructure, and rising global energy demand (IPCC, 2023). To address this, the sector focused on transitioning to renewable energy sources such as wind and solar, enhancing energy efficiency through modernized infrastructure, and adopting decentralized systems and smart grids to optimize energy use (International Renewable Energy Agency (IRENA), 2023). According to 2023 energy usage data, 83% of the total energy consumption of 94 quadrillion BTU came from fossil sources, while 9% came from renewable energy sources (EIA, 2023). The U.S. DOE has launched an initiative to minimize greenhouse gas emissions through alternative sources. The IRENA estimates that an annual investment of $1.5 trillion is needed until 2030 to replace fossil fuels with renewable energy sources. This investment is critical for transitioning to a low-carbon energy system, which involves the large-scale deployment of renewable energy technologies, such as wind, solar, and hydroelectric power. Additionally, investments are required to enhance energy efficiency, develop advanced energy storage solutions, and upgrade grid infrastructure to accommodate the increasing share of renewable energy. These efforts, combined with innovative technologies like AI, are crucial for driving the shift toward decarbonization and achieving global climate goals. Renshaw (2023) highlighted the dual-edged nature of AI in cybersecurity, emphasizing the risk of AI-assisted cyberattacks and potential data leaks. Advanced AI systems could be exploited to develop sophisticated attacks, such as targeted

phishing campaigns, real-time deep-fake media manipulations, and enhanced hacking techniques. These threats highlighted the critical need for anticipatory governance and robust security protocols, especially as the proliferation of AI technologies increases their accessibility and misuse potential.

The literature review leveraged a search strategy for identifying and analyzing relevant literature on mitigating cybersecurity issues with the adoption of AI in the energy sector. It integrated perspectives from trustworthy AI, cybersecurity frameworks, and project risk management. The review also investigated the strategic role of PMOs in addressing cybersecurity risks while supporting decarbonization goals. This included leveraging project management strategies to manage risks and enhance security during AI adoption. The structured approach culminated in meaningful recommendations for the energy sector to effectively navigate the AI adoption journey and achieve sustainable transformation.

The current literature review explored the perspectives from Trustworthy AI, Cybersecurity Frameworks, and Project Risk Management. Peer-reviewed scholarly articles relevant to these constructs were identified using the National University's Roadrunner Library as the primary resource. The search strategy emphasized scholarly journals published between 2020 and 2024, utilizing Boolean and phrase search techniques with key terms such as "Trustworthy AI," "PMO," "risk management," "renewable energy," "decarbonization," and "cybersecurity." Databases like EBSCOhost, Web of Science, ScienceDirect, ProQuest Central, Business Source Complete, and Google Scholar were employed to ensure a comprehensive search. The relevant recent articles from 2021-2025 were retrieved from the following journals: PM World, Project Management Journal, and International Journal of Project Management. The current project management standards, trends, and practices were referenced from the following

sources: https://www.pmi.org and https://scaledagileframework.com. To identify the literature gap and future research, search strings “literature’ and ‘gap” were used, along with reviewing limitations and future research directions from peer-reviewed scholarly articles. Reverse author searches were performed to determine if any further study was conducted on the unanswered research questions, and no evidence of further follow-ups on this specific research topic was found. If resources were unavailable, interlibrary loan requests were submitted. This thorough and systematic approach ensured the depth and relevance of the literature review.

Conceptual Framework

Energy organizations face challenges building Trustworthy AI, such as a lack of explainability, security and privacy concerns, biased models, and insufficient or inaccurate data. Despite these challenges, AI has presented several viable use cases in the energy sector, including predictive maintenance, load forecasting, wildfire risk evaluation, grid management, and cybersecurity (Renshaw, 2023). The evolution from Industry 4.0's focus on digitization and automation to Industry 5.0's emphasis on human-centric AI underscored the importance of human-machine collaboration in building trustworthy AI systems that enhance decision-making. Building trust in AI differed fundamentally from traditional technologies due to AI’s transformative potential to revolutionize business processes and decision-making (Bedué & Fritzsche, 2021).

TAI-Cybersecurity PRM Framework

The conceptual framework of this study was built on Trustworthy AI (TAI) requirements and cybersecurity risk management. By incorporating TAI considerations into cybersecurity risk management, organizations could effectively identify risks, develop mitigation strategies, and mitigate cybersecurity threats associated with adopting AI technologies in renewable energy

projects (Melaku, 2023; NIST, 2023; Vyhmeister & Castane, 2024). By understanding an organization's strategic goals, security risk management priorities, and tactical and operational contexts, senior management could establish a comprehensive risk management strategy with an appropriate risk appetite while ensuring business continuity.

The cybersecurity risk assessment process involves identifying, evaluating, and prioritizing cybersecurity risks. These risks are assessed using Failure Mode and Effects Analysis (FMEA), a methodology that systematically identifies how a system or process can fail, evaluates the impact, and prioritizes and mitigates potential failures. Risk responses are selected based on the organization's risk appetite and include several options. Risk assumption involves agreeing to accept the assessed risks. Risk avoidance seeks to eliminate the sources of risk. Risk reduction focuses on implementing security controls to minimize risks, while risk planning involves managing risks through detailed mitigation plans. Risk transfer shifts responsibility for the risks to a third party (Melaku, 2023). The KPI estimation step connects TAI security considerations with monitoring strategies and potential failure modes. The subsequent Update Interactions and Requirements step identifies the potential risks of integrating AI assets. Lastly, the Review, Update, and Implementation step ensures that risk response strategies were adequately reviewed and refined. When no additional updates are needed, risk treatment options are applied to effectively address risks and maintain system integrity. (Vyhmeister & Castane, 2024).

Trustworthy AI. Trustworthy AI refers to artificial intelligence systems designed and operated in ways that uphold ethical principles, ensure safety and security, and maintain reliability throughout their lifecycle (Vyhmeister & Castane, 2024). The concept is critical to

maximizing societal benefits while minimizing risks. The foundational components of Trustworthy AI include:

- Validation and reliability.
- Safety.
- Security.
- Privacy.
- Explainability and Interpretability.
- Fairness with bias mitigation.
- Transparency and Accountability.

Validation and reliability form the basis for trustworthiness and apply to all other characteristics. Validation ensures that AI applications fulfill their intended use, while reliability ensures that functional requirements are consistently met without failure throughout the lifecycle of AI applications. Transparency and accountability are overarching principles that apply to all other characteristics (NIST, 2023). The increasing adoption of AI has brought attention to its potential issues, including security and data leaks. These concerns have driven efforts to develop "trustworthy AI," as advocated by the EU High-Level Expert Group on AI and the EU Artificial Intelligence Act. However, critics like Ryan (2020) argued that framing AI in terms of trust humanizes it unnecessarily and misuses the concept. Expanding on this critique, Dorsch and Deroy (2024) contended that while AI systems trained on appropriate datasets may exhibit reliability and appear trustworthy, true trust requires moral reasoning, a characteristic beyond the capability of AI systems. Thus, they emphasize distinguishing between technical reliability and the moral dimensions inherent in trust.

Each trustworthy AI requirement aims to reduce AI's risks and potential negative impacts. As a result, it is crucial to implement mechanisms that can identify and address these risks at every stage of the AI lifecycle. Vyhmeister and Castane (2024) examined strategies for incorporating TAI requirements within the manufacturing sector. They proposed a comprehensive framework that integrates TAI considerations with existing risk management practices, drawing on the ISO 31000 standard. This integration aims to ensure that AI applications in manufacturing are managed responsibly and in alignment with regulatory standards, while also addressing potential risks and ethical concerns. House (2023) outlines principles for the responsible development and use of trustworthy AI. These principles include promoting inclusive growth, respecting human rights and democratic values, ensuring transparency, safeguarding robustness and security, and establishing accountability across the AI lifecycle. It also provides guidance for national policies, advocating for investment in AI research, fostering inclusive ecosystems, and preparing for AI's impact on the labor market. Revisions reflect emerging challenges like generative AI, misinformation, and environmental sustainability while stressing the importance of international cooperation and interoperable governance.

The application of AI is critical to achieving energy transition and has been widely utilized in areas such as cybersecurity, power system protection analysis, and simulation-based studies on smart grid protection (Meiser & Zinnikus, 2024). As the energy sector increasingly relies on AI to meet decarbonization goals, ensuring the trustworthiness of AI technologies becomes essential. To enhance trustworthiness, a model-centric approach aims to eliminate or minimize biases, while a data-centric approach focuses on analyzing the data used to train machine learning algorithms (Bhatt et al., 2024). The availability of large datasets is vital for

models to perform effectively, as even a well-designed model will produce suboptimal results when trained on insufficient data. Meiser and Zinnikus (2024) highlighted using synthetic data to improve the trustworthiness of AI by incorporating real-time scenarios, particularly in the energy domain, where replicating such scenarios is challenging or unethical.

While AI systems can support and accelerate the energy transition, the sector faces significant barriers to adoption, including complexity, high costs, a lack of skilled resources, and rapid technological advancements (Jimenez & Gonzalez, 2022). Jimenez and Gonzalez (2022) also discussed using AI maturity measures across six domains in energy transition—AI readiness, forecasting, smart grids, asset management, planning and operation, and decision support systems—to evaluate the current state and identify gaps. Additionally, the president's executive order underscores the importance of developing standards and guidelines for safe, secure, and trustworthy AI, calling for a plan to implement the DOE's AI model and establish AI testbeds (House, 2023).

Cybersecurity Risk Management. The energy sector is a primary target for cybersecurity attacks due to its critical role in supporting daily life, ensuring national security, and its extensive interconnectedness with other industries (CISA, 2024). As the energy sector relies on smart grid technologies to provide reliable, safe, and affordable energy, vulnerabilities in these interconnected systems make the smart grid prone to cybersecurity attacks (Bouramdane, 2023). The energy companies may operate smart grids in stand-alone or grid-tied mode, depending on the available infrastructure, operation goals, and regulatory requirements. In stand-alone mode, energy generation and distribution occur locally using renewable energy sources like solar and wind. In grid-tied mode, the smart grid is connected to the main power grid, which can use both fossil-based traditional and renewable energy sources. Cybersecurity challenges in energy

systems arise from the interconnected nature of devices, exposure to external networks, and the risk of malicious attacks on critical infrastructure. According to the International Energy Agency (IEA, 2024), cyberattacks on the energy sector have been escalating rapidly since 2018, peaking in 2022 amidst the Russia-Ukraine war. The average data breach cost in the sector during this period was estimated at $4.72 million USD.

The common types of cyberattacks on smart grids are Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, Malware attacks, Phishing attacks, Insider threats, Man-in-the-middle attacks, Advanced Persistent Threats, Data Manipulation Attacks, Supply Chain attacks, SQL injection attacks, and Zero-day exploits (Bouramdane, 2023). DDoS attacks make the targeted systems inaccessible to legitimate users by stressing the smart grid's resources with a high volume of traffic, potentially causing service outages for end users (Roy, 2021). Distributed DDoS attacks are similar to DDoS but involve forming a botnet using multiple compromised devices. Malware attacks refer to infecting smart grid systems with viruses—self-replicating programs attached to the smart grid's software, which can cause the system to malfunction and provide unauthorized access to threat actors; worms—stand-alone software programs that can impact smart grid devices, leading to system crashes and unauthorized usage; and ransomware, which encrypts and locks out the smart grid systems, demanding a ransom payment to restore access, disrupting business operations, causing reputational damage, and leading to financial loss. Trojan horses impersonate legitimate software and create backdoor access for threat actors, allowing malicious activities to occur. Botnets are created using a network of multiple compromised devices to perform coordinated attacks (Pepin et al., 2022). Keyloggers capture the keystrokes from infected devices, including login credentials and highly sensitive information. Spyware monitors and tracks smart grid operations without the knowledge

of legitimate users and uses the information to perform illegitimate and unethical activities (Li et al., 2024). Phishing attacks use deceptive techniques to trick users into believing messages are coming from trusted sources and asking for sensitive information, including login credentials, passwords, financial details, etc. Insider threats arise from internal authorized users, who knowingly or unknowingly compromise the grid's security. Man-in-the-middle attacks exploit vulnerable wireless networks, acting as a middleman without the knowledge of both parties and eavesdropping on and manipulating data. Advanced Persistent Threats aim to obtain critical information from targeted organizations using sophisticated technologies and disrupt energy operations (Akuffo-Badoo, 2023; Tharzeen et al., 2023). Data Manipulation Attacks alter data within the smart grid system, affecting grid security. Supply chain attacks leverage vulnerabilities in third-party software used in the smart grid to create backdoor access for malicious activities. SQL injection attacks exploit vulnerabilities in web-based applications within the smart grid to gain access to the database (Gowtham & B, 2021). Zero-day exploits target vulnerabilities in the components of smart grid systems before the vendor can release a patch for the affected software (Akello, 2024).

AI-driven cyberattacks are a growing and sophisticated threat, transforming the landscape of cybercrime and warfare. These attacks enhance traditional methods like phishing, malware, and data manipulation attacks while also introducing new challenges, such as adversarial AI and the manipulation of AI models (Necula, 2023). AI-powered malware, such as polymorphic and metamorphic variants, can adapt and evolve to evade detection mechanisms, posing significant challenges to cybersecurity defenses. Phishing attacks are becoming more targeted and effective, leveraging AI to analyze data and create highly convincing messages. Additionally, AI enables more sophisticated botnets that are capable of launching coordinated, evasive, and evolving

attacks. These advancements amplify the risks to privacy, security, and societal stability. AI-driven threats could lead to prolonged systemic failures, economic losses, disruption of emergency services, and even political instability through social media manipulation. The evolving nature of these threats highlights the urgency for enhanced cybersecurity mechanisms to address AI as both a tool for attackers and a force multiplier for defenders.

Vulpe et al. (2024) categorized the impacts of AI into macro-level impacts—globalization, pervasiveness, and transformation of the public sphere—and micro-level impacts—individualization and distribution of risks. Globalization of risks highlights how AI eliminates language barriers, enabling non-English-speaking threat actors from underdeveloped countries to target global victims. Pervasiveness refers to AI's ability to amplify threats, while the transformation of the public sphere addresses the social impacts of AI, including its influence on public opinion. The use of AI systems can undermine trust by generating misinformation and automating cybersecurity breaches. At the micro level, the individualization of risks shifts responsibility to individuals to manage AI-related risks despite the complexity of technology. Meanwhile, inequality in the distribution of risks emphasizes that cyberattacks often disproportionately target marginalized communities. Puthal and Mohanty (2021) analyzed the underlying model of AI and categorized cyberattacks into input and poisoning attacks. Input attacks are described as attacks that alter the system output, whereas poisoning attacks are tampering with the training model. They articulate the use of software assurance processes in mitigating cyber risks.

To combat cybersecurity threats within the energy sector, the Energy Information Sharing and Analysis Centre (E-ISAC) was established in 1999, which supported the organizations with incident analysis, tools, and sharing of critical security information to address evolving

cybersecurity threats to the grid. The E-ISAC portal serves as the hub, enabling partner organizations to voluntarily and securely share and exchange information on security incidents (E-ISAC, 2024). Similarly, the European Energy Information Sharing and Analysis Centre (EE-ISAC) was established to foster collaboration among organizations within the EU to enhance cybersecurity in the energy sector (Wallis & Leszczyna, 2022). This trust-based network provides a platform for ongoing support, identifying and assessing opportunities to strengthen technical leadership and improve actionable threat intelligence.

Cybersecurity Risk Management (CRM) is a systematic approach to identifying, analyzing, and addressing cybersecurity threats and vulnerabilities within an organization to safeguard its assets and maintain resilience against cyberattacks (Lee, 2021). An effective CRM framework aligns with the organization's security objectives, policies, budgets, and resources while requiring strong commitment from top management. It incorporates processes like reporting, communication, and accountability into the overall risk management strategy. The NIST Cybersecurity Framework, NIST Cybersecurity Risk Management Framework, ISO/IEC 27005:2018 Risk Management Framework, OCTAVE, IEC 62443, and NIST AI Risk Management Framework are available to support the energy sector in the cybersecurity risk management process (Melaku, 2023). All these frameworks use both security and compliance measures.

NIST Special Publication 800-37 provides guidelines for managing security and privacy risks through technology-neutral process steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor (Melaku, 2023). Organizations can adapt these steps flexibly to align with their specific objectives and security needs, such as executing the steps in a different order, combining tasks, or tailoring them as necessary (NIST, 2023). The Prepare step involves

conducting or updating organization-wide risk assessments, establishing a baseline for controls, prioritizing critical assets, developing a risk management strategy, creating a strategy for monitoring control effectiveness, and identifying and assigning key roles for executing the risk management framework. This framework emphasizes risk-based decisions based on an understanding of the security and privacy posture of information systems and the provision of common controls. The posture reflects the status of systems and resources based on available information assurance resources and the capabilities to manage security, comply with privacy requirements, and adapt to evolving risks. The Categorize step involves documenting system characteristics and categorizing the systems based on the potential impact of loss. In the Select step, controls are identified, control baselines are established, and a continuous monitoring strategy that aligns with the enterprise-wide risk management strategy is developed. During the Implement step, the selected controls are put into action. The Assess step validates the effectiveness of the controls in protecting the organization's assets. The Authorize step ensures accountability for the security and privacy management plan by a senior management team member. Finally, the Monitoring step involves continuously monitoring and updating the security and privacy plan.

ISO/IEC 27005 is part of the ISO 27000 series and serves as a standard offering guidance for managing information security risks. The 2018 version of ISO 27005 complements the principles defined in ISO 27001, providing a structured approach to implementing information security through risk management. It outlines key stages, including establishing the context, performing risk assessments, treating risks, accepting risks, communicating and consulting about risks, and conducting continuous monitoring and review.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk management framework for managing information security risks (Melaku, 2023). It was developed by Carnegie Mellon University's Software Engineering Institute (SEI) and is designed to help organizations identify, assess, and manage risks associated with their information assets. The methodology focuses on aligning security strategies with organizational objectives and ensuring that risk management is integrated into business processes. OCTAVE differs from traditional technology-focused assessments by emphasizing organizational risk and strategic, practice-based issues instead of technological and tactical concerns (SEI, 2023). OCTAVE enables organizations to make informed decisions about protecting critical information assets by evaluating their confidentiality, integrity, and availability risks. It incorporates all dimensions of risk—assets, threats, vulnerabilities, and organizational impact—into its decision-making process. This comprehensive view allows organizations to align their protection strategies with specific security risks.

The NIST AI RMF is a risk management framework designed to address AI risks by minimizing negative impacts and maximizing potential benefits. It includes four main functions: map, measure, manage, and govern. The Map function establishes the context by outlining AI systems' purpose, applications, and positive and negative impacts. It categorizes AI systems by identifying the specific tasks supported by AI, comparing potential benefits and costs, and assessing the risks and benefits of each underlying component, including third-party software. Additionally, it considers the impacts on organizations, individuals, and society. The Measure function uses quantitative and qualitative methods to evaluate and monitor an AI system’s adherence to trustworthy characteristics. The Manage function prioritizes risks and identifies appropriate risk treatments, including strategies to maximize benefits and minimize negative

impacts. The Govern function establishes governing policies and procedures that align with legal and regulatory requirements for assessing and mitigating AI risks. Swaminathan and Banks (2023) highlighted accountability gaps in the NIST AI RMF and recommended leveraging joint accountability agreements to ensure clear ownership and responsibility in achieving trustworthy characteristics. Danks and Trusilo (2023) argued that the lack of AI standards may introduce risks associated with underlying AI components.

In comparing these frameworks, ISO/IEC 27005 focuses on a holistic approach, while the NIST framework operates at a tactical level, and OCTAVE functions at a strategic level. ISO and NIST frameworks are suitable for organizations of any size, whereas OCTAVE is more appropriate for large organizations. Melaku et al. (2023) identified research gaps in existing risk management frameworks, noting that they are often too complex to implement, narrowly focused on specific applications or functions, and lack integration with NIST or ISO frameworks. The TAI-Cybersecurity PRM framework is proposed to address the research gap, integrating TAI requirements with a context-based cybersecurity risk management approach.

Overview of Decarbonization

Decarbonization is the reduction of carbon emissions per unit of GDP linked to greenhouse gas (GHG) emissions and carbon intensity (Magyari, 2023). Several countries have committed to reducing carbon emissions by employing various strategies. Triani (2023) discussed the decarbonization approaches utilized by different countries, including Mexico, Russia, China, Sweden, and Bolivia. These countries are implementing diverse strategies to combat climate change and reduce carbon emissions. Mexico focuses on replacing fossil fuels with renewable energy, promoting electric vehicles, and reducing fertilizer use. Russia aims to expand renewable energy in the power sector, establish supportive policies, and develop

hydrogen production. China emphasizes transitioning to solar, wind, hydro, biomass, and nuclear power plants, advancing electric vehicles, and implementing an emissions trading system. Sweden invests in renewable energy and adopts carbon capture and storage technologies. Bolivia is working on a carbon tax mechanism, enhancing renewable energy capacities, and formulating policies for greenhouse gas mitigation.

Magyari (2023) conducted an explorative study analyzing the decarbonization strategies employed by the V4 countries: the Czech Republic, Hungary, Poland, and Slovakia. These nations have outlined long-term energy goals centered on renewable and nuclear energy development. Their strategies include integrating solar, wind, and biomass into the energy mix, modernizing energy systems, enhancing energy efficiency, and increasing the share of nuclear energy in electricity generation. They also emphasize transitioning coal regions, implementing smart grids, diversifying energy supplies, and developing infrastructure. Additionally, their plans focus on decarbonizing energy systems to make them clean, secure, decentralized, and interconnected while leveraging existing gas infrastructure for renewables and advancing district heating and cogeneration initiatives.

In the U.S., the DOE has published a roadmap outlining four key technological pillars for significantly reducing emissions across industrial subsectors: energy efficiency, industrial electrification, low-carbon fuels and feedstocks, and carbon capture, utilization, and storage (DOE, 2024a). Energy efficiency focuses on optimizing industrial processes. Industrial electrification emphasizes leveraging low-carbon electricity. Low-carbon fuels and feedstocks prioritize using hydrogen and biofuels: carbon capture, utilization, and storage aim to capture CO2 and repurpose it to create new products. The DOE (2024b) report highlighted the potential of AI in effective grid management, including planning, permitting, operations, reliability, and

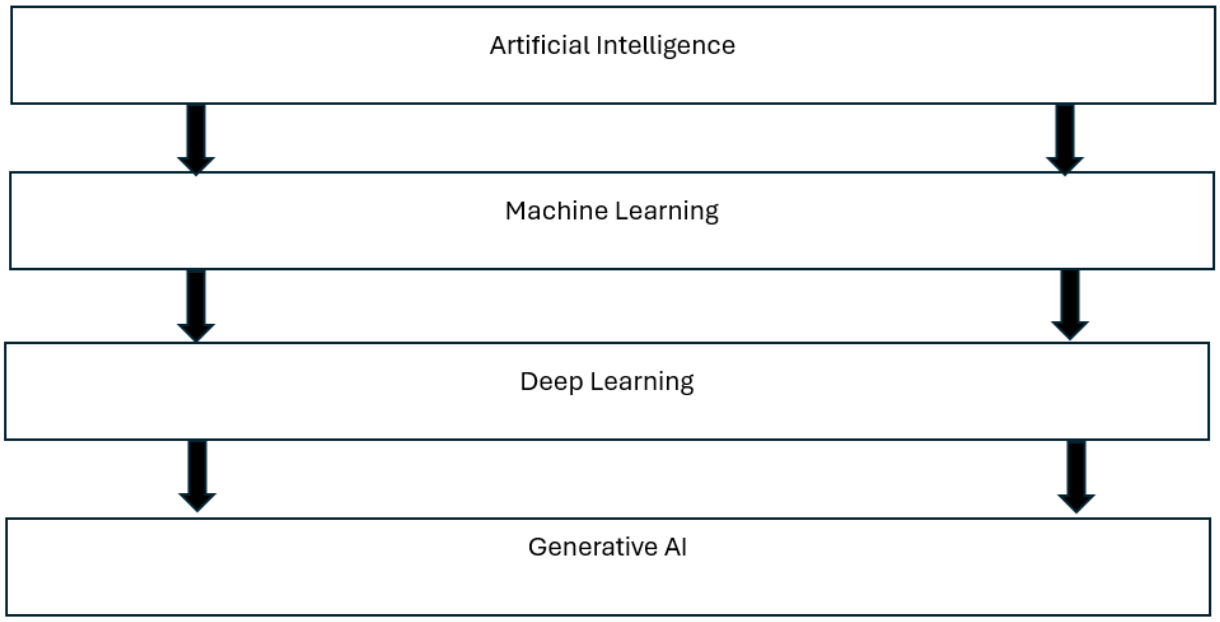
resilience. However, it underscored the need to mitigate risks associated with these new AI use cases.

Overview of AI

Artificial Intelligence refers to creating machines capable of performing tasks that typically require human intelligence (McKinsey & Company, 2024). Over time, as shown in Figure 2, the field of AI has evolved from developing systems that replicate human behaviors to more advanced methodologies, including Machine Learning (ML), Deep Learning (DL), and Generative AI. ML uses algorithms to learn patterns from large datasets and make predictions. ML algorithms are categorized as supervised learning, where data is pre-cataloged; unsupervised learning, where data is not cataloged, and the system identifies patterns independently; semi-supervised learning, which combines both pre-cataloged and uncatalogued data; and reinforcement learning, where algorithms are trained to learn from successes and failures. DL employs artificial neural networks modeled after neurons in the human brain to generate sophisticated insights. A recent innovation is Generative AI, which utilizes large neural networks, known as large language models, to create content such as text, videos, and images. These advancements highlight AI's growing capabilities and applications across various domains (Bellini et al., 2022).

Figure 2

Evolution of AI



Note. This figure was independently developed by the researcher, Antony Amalraj, to illustrate the evolution of AI.

Generative AI transforms the energy sector by enhancing operational efficiency and decision-making through innovative applications. Rueda et al. (2021) studied the application of the WaveNet AI model to predict renewable energy production, while Alsayegh and Masood (2024) investigated leveraging AI for knowledge management using advanced agent architecture (AAA). Zhang et al. (2023) also discussed utilizing AI to optimize energy harvesting processes for sustainable energy solutions. While AI models present promising opportunities to enhance business value, they pose significant risks, including cybersecurity threats, ethical dilemmas, privacy concerns, and intellectual property challenges. Shakeri et al. (2020) highlighted AI's ability to generate malicious code in cloud environments and create sophisticated phishing emails. Gupta et al. (2024) emphasized that threat actors can exploit generative AI vulnerabilities

to carry out social engineering and phishing attacks and deploy harmful payloads. Similarly, Humphreys et al. (2024) highlighted the potential risks of data poisoning, leaks, and manipulation linked to generative AI systems.

Challenges in AI Adoption

Siaterlis et al. (2022) analyzed 20 research projects in the manufacturing sector and identified key challenges in adopting AI. A lack of skilled resources in AI creates significant difficulties for organizations in maintaining and supporting complex AI applications. The absence of documented standards for developing, testing, and deploying AI-driven applications also introduces operational and security risks. Immature IoT technologies further hinder AI adoption, as many AI-driven applications rely on cloud technologies that are neither fully mature nor seamlessly integrated with existing systems like ERP and SCADA, raising additional security concerns. Moreover, poor data quality remains a critical barrier, as it directly impacts the performance and reliability of AI systems.

Regona et al. (2022) reviewed 72 articles and identified key challenges in adopting AI within the construction industry. AI applications in this sector require constant algorithm training to identify patterns; however, the fragmented nature of the industry often results in data scarcity. High development, training, and maintenance costs make AI implementation expensive. Additionally, AI adoption requires a shift from traditional practices, which faces significant resistance from industry bodies. The non-standardization of construction projects further complicates AI integration. Other barriers include the need for costly AI expertise, concerns about data security, and unresolved ethical, moral, and legal issues. Lastly, AI's impact on traditional skills raises fears of job displacement, which hinders broader acceptance within the industry. Badi et al. (2022) conducted a research study involving 27 executives from the

healthcare sector in the UAE, utilizing both quantitative and qualitative methods. The study identified and prioritized five main categories as key challenges in adopting AI: accuracy, privacy and security, ethical barriers, interoperability, and control.

Mobayo et al. (2021) conducted a quantitative research study in the energy sector in Nigeria involving 384 respondents. The study identified and ranked key challenges in AI adoption, including outdated power system infrastructure, limited cellular technologies, a lack of skilled resources, threats from cyberattacks, data quality issues, the absence of AI policies and regulations, security and privacy concerns, the complexity of AI models, and challenges in integrating AI with existing systems. Danish (2023) conducted a research study using a multidisciplinary approach to assess challenges in adopting AI in the energy sector. It categorized them into four dimensions: performance and cost challenges, security and privacy challenges, technical challenges, and social and ethical challenges. Ensuring data availability and quality is crucial, as AI systems require high-quality, well-structured data for accurate predictions. Privacy and security concerns arise from handling sensitive energy data, necessitating robust measures like encryption. The explainability of AI decisions remains challenging, especially for critical tasks requiring stakeholder understanding. Reliability issues emerge when training data or system testing is inadequate. Integrating AI systems with existing infrastructure demands significant changes, and high costs pose barriers for organizations. The lack of regulations and standards complicates compliance, while scalability is essential for large-scale energy operations. Additionally, challenges such as real-time decision-making, performance evaluation, interoperability, adaptability to dynamic energy markets, and evolving regulations further complicate adoption. Ethical concerns, including bias, job displacement, and the need for transparency and human-in-the-loop mechanisms, underscore the multifaceted

complexities of implementing AI in energy systems. Challenges such as real-time decision-making, performance evaluation, interoperability, adaptability to dynamic energy markets, and evolving regulations further complicate adoption. Ethical concerns, including bias, job displacement, and the need for transparency and human-in-the-loop mechanisms, underscore the multifaceted complexities of implementing AI in energy systems (Brandas et al., 2023; Ukoba et al., 2024)

Risk Management Methodologies

Risks are an inevitable aspect of any initiative and managing them effectively at every stage of the project lifecycle is essential to ensure the successful delivery of projects. A proactive approach to risk management minimizes potential threats and helps organizations capitalize on opportunities, enhancing overall project outcomes. Several industry-recognized methodologies have been developed to address the complexities of risk management, including IPMA, PRINCE2, TenStep, and PMI. Each of these methodologies provides a structured and systematic approach, equipping project managers with tools and techniques to identify, assess, and mitigate risks while maintaining alignment with organizational objectives and priorities. Jedrusik (2024) explored risk management based on established methodologies such as IPMA, PRINCE2, and TenStep in a qualitative research study involving 25 project managers. The study concluded that 72% of respondents favored the IPMA methodology over others. The IPMA methodology incorporates quantitative and qualitative risk analysis and considers various risk response strategies, including avoidance, minimization, and passive and active acceptance. Additionally, the IPMA Competence Baseline organizes competencies into three domains: people, practice, and perspective. PRINCE2 proposes a five-step risk management process: identify, evaluate, plan, deploy, and communicate. In the identification step, risks and early warning indicators are

identified, while the evaluation step assesses overall risk weights in alignment with the risk tolerance levels established by organizational leadership. The planning step focuses on devising risk responses to mitigate or eliminate threats and maximize opportunities. The deployment step defines clear roles and responsibilities for risk management and implements the planned responses. Finally, the communication step ensures that progress on risk management is effectively shared with relevant stakeholders. Project Management Institute (2021), on the other hand, outlines seven risk management principles. These include achieving excellence in risk management by balancing the benefits and costs of risks, tailoring the risk management process to align with organizational priorities, aligning risk management with evolving strategies and governance, focusing on risks that directly impact organizational objectives, optimizing risk responses by effectively balancing exposures, costs, and benefits, fostering a proactive risk management culture, and continuously improving competencies to identify and manage both positive and negative risks influencing project success.

The complexity of large-scale public projects, influenced by uncertain factors like climate, geology, technical challenges, and resource availability, significantly affects schedule management. For instance, Ethiopia's infrastructure projects face an average schedule delay of 110%, while Norway’s large-scale government projects average a 10-month delay. Defense and communication projects have completion rates as low as 12–20%, with delays averaging 30–40 months. Larger projects, such as hydropower developments, are particularly vulnerable, with delays averaging 32% (~18 months), as larger-scale projects pose more significant risks (Chen et al., 2024). These delays impact stakeholders by postponing anticipated benefits, disrupting plans, increasing costs, reducing productivity, and eroding profit margins and competitive advantages.

To assess and control risks, a variety of techniques and models, such as Program Evaluation and Review Technique (PERT), Analytic Hierarchy Process (AHP), System Dynamics, Structural Equation Modeling (SEM), network analysis, artificial intelligence, and Integrated Structured Modeling (ISM), have been developed and are currently in use. PERT, integrated with fuzzy set theory, is used to evaluate schedules and predict the probability of project completion based on various scenarios (R. Zhang et al., 2020). However, as this method relies on logical relationships between project nodes, it is challenging to evaluate complex systems. System Dynamics is a qualitative model that utilizes causal loop diagrams to estimate overall cost overrun risk. The AHP model focuses on factors that can be observed and quantified, whereas the SEM model is used for factors that cannot be directly observed (Kim et al., 2021; Taha et al., 2022). Bashir et al. (2023) leveraged weighted social network analysis to analyze the influence of risk factors. Cheng and Darsa (2021) employed artificial neural networks to rank risk factors and predict schedule delays. Egwim et al. (2021) integrated a random forest classifier with machine learning algorithms to predict schedule delays. Shoar et al. (2023) utilized the ISM model, which focuses on hierarchical structures, direct relationships, and correlations between variables, to identify key risk factors. Li et al. (2024) combined the ISM model with the Monte Carlo simulation model to analyze investment risks in clean energy projects.

The complex nature of energy projects requires effective management of risks, including environmental, technological, regulatory, and economic risks. Salami (2025) proposed a multi-criteria decision-making methodology (MCDM) for assessing risks in energy projects. The FMEA method is widely used to prioritize failure modes and develop preventive actions in manufacturing, engineering, and healthcare. Fault Tree Analysis (FTA) uses tree diagrams to deduce failure modes and identify associated root causes, particularly in the energy and chemical

industries. The Bowtie Risk Assessment method, commonly applied in healthcare and aviation, is designed to analyze the causes and effects of high-level hazardous events. Hubbard and Seiersen (2023) highlighted the importance of quantitative assessments in improving decision-making processes to enhance security. Despite the availability of traditional risk assessment models, they often fail to adapt to the unique operational constraints of Industrial Control Systems (ICS). Integrating AI and machine learning is increasingly necessary to address this gap and strengthen ICS cybersecurity.

The modern trend in the energy sector utilizes innovative technologies such as ICS, Digital Twins, and the Internet of Things (IoT). ICS plays a critical role in the energy sector and is key to its critical infrastructure. The increasing integration of ICS with other energy systems, combined with the convergence of Information Technology (IT) and Operational Technology (OT) systems, exposes the energy sector to significant cybersecurity risks due to vulnerabilities in ICS systems (Shikhaliyev, 2024). Digital Twins represent a transformative technology in the energy sector, enabling the optimization of grid operations, anomaly detection, asset life evaluation, and failure prediction (Ismail et al., 2024). However, manipulating Digital Twins in renewable energy sources can result in production inefficiencies or even system outages (Saeed et al., 2024). The Internet of Things (IoT) devices are widely used in the energy sector to interconnect sensors, IT, and OT systems. These devices collect vast amounts of data, enabling real-time monitoring, predictive analytics, and automated control, which improve efficiency, reduce costs, and enhance sustainability in energy systems (Jiang et al., 2022). However, vulnerabilities in IoT devices, such as weak authentication, insecure communication protocols, and outdated firmware, can be exploited by hackers, potentially causing operational disruptions (Bakshi et al., 2024).

Bello and Hassan (2024) examined the impact of geopolitical risks on renewable energy consumption in 20 OECD countries over the period 1970 to 2022. Their findings emphasized the need for strategic actions to enhance renewable energy adoption and decarbonization efforts. They recommended promoting peaceful coexistence among countries and regions to facilitate the transition to clean energy, implementing policies to reduce pollution and CO2 emissions to support renewable energy deployment, and encouraging economic development and globalization. According to the study, open and growth-oriented economies play a crucial role in driving the shift toward renewable energy, highlighting the importance of global cooperation, effective environmental policies, and economic reforms in addressing climate change. The growing complexity of large-scale projects, particularly in the energy sector, underscores the need for continuous adaptation to emerging technologies and market dynamics. Integrating advanced systems such as ICS, Digital Twins, and IoT highlights both the opportunities and vulnerabilities introduced by technological advancements, emphasizing the importance of cybersecurity in modern project management.

Role of Project Management Offices

Several research studies in the PM literature have discussed the role of PMO in project success. Silvius (2021) articulated that the role of the PMO as the custodian of project management standards and practices within organizations ensures that project planning, prioritization, and execution align with organizations' strategic priorities. Ershadi et al. (2021b) discussed the role of PMO in sustaining procurement management through strategic analysis and goal-setting processes. Sandhu et al. (2019) proposed these new PMO roles: strategic management and organizational learning. They argued that these PMO roles could improve the project-delivering capability of PBOs and develop effective business ecosystems. Wu and Zhu

(2020) articulated the need for having an executive role as Chief Project Officer (CPO), as PMOs lack the authority to carry out the projects end-to-end. They cite the growing popularity of project management, increasing project complexity, and the number of project management practitioners as the rationale for the need for executive-level presence.

Sandhu et al. (2019) compiled a list of the following PMO functions for the different types of PMOs: defining core processes, supporting project selection, prioritization, and project management systems, maintaining knowledge artifacts, tracking, and monitoring end-to-end project delivery, and sharing organizational information. Khafri et al. (2022) studied the cause and effect of PMO functions and reported that establishing PMO structure and functions is the most effective function. In their study, Ershadi et al. (2021c) reported that risk management, tracking project benefits, status reporting, governance, and introducing project management tools are the top functions. Ichsan et al. (2023) reported that knowledge management, strategic alignment, governance, supporting role, innovation, and organizational and project performance enablers are the PMO functions. De Brito and De Medeiros Júnior (2021) argued that integrating projects, business units, and project personnel, establishing communication channels to communicate project status to the stakeholders, and standardizing tools and techniques are the key PMO functions.

Barbalho and Da Silva (2021) analyzed the effect of the following critical success factors on PMO's success: project management maturity, stakeholder support, adoption of project management best practices, PMO leadership, and technical expertise. Their study found that stakeholders' support and adopting project management best practices success factors significantly affected PMO's success. However, the study could not confirm the effect of other success factors, such as project management maturity and PMO leadership and technical

expertise, on PMO's success. Paton and Andrew (2019) categorized the factors affecting PMO success into three groups. They are resource management, project management, and organizational culture. In the resource management category, inconsistent PMO resources, inexperienced PMO and project leadership, poor strategies, and lack of training are listed as the top-ranked factors affecting PMO success. Simultaneously, in the project management category, project ownership conflict, ineffective communication strategy, lack of senior management support, and administrative overhead are the most important factors affecting PMO success. In the organizational culture, resistance to change, ineffective change management, and lack of working organizational culture are the high-ranked factors. Ntshwene et al. (2022) examined the following factors as the driving forces for organizations to invest in establishing a PMO. They are project failures, lack of documentation on project transactions, unmanaged and repetitive project tasks, ineffective communication, lack of defined business objectives, inadequate processes and templates, and insufficient resource optimization.

Khafri et al. (2022) discussed the different levels of PMO maturity and their effect on the PMO status. Project control is the first level of PMO maturity, where the project management maturity is at the initial level, and the PMO is involved in developing the processes. The second level is process control, where the processes are defined and at the repeatable level. The third level is process development and support, where the PMO actively pursues process improvements. The fourth level is the managed level, and the fifth is strategy, where the project management maturity is at the optimization level. Fernandes et al. (2021) discussed three PMO maturity stages: basic, intermediate, and advanced for managing R&D projects. PMI & PWC (2021) developed a global PMO maturity index with five elements: governance, integration and alignment, processes, people, technology, and data. Domingues and Ribeiro (2023) compared

various project management maturity models: prado project management maturity model (PMMM), kerzner project management maturity model (KPMMM), organizational project management maturity model (OPM3), PM Solutions project management maturity model (PSPMM), and favored OPM3 as it measures maturity level across projects, programs, and portfolios.

Philbin and Kaur (2020) discussed the following four perspectives on measuring PMO performance: financial, customer, internal business processes, learning, and growth. They analyzed the key performance indicators (KPI) for each operational perspective. The financial perspective included the following KPIs: the financial value of projects awarded, the financial value of proposals submitted, and the financial value of PMO-managed projects. The customer perspective included these KPIs: the number of resources involved in creating proposals, the number of resources involved in project delivery, and the number of new projects launched by the PMO. The internal process perspective focused on tracking process improvements and standard operating procedures. The learning and growth perspective focused on tracking the number of trainings and external presentations. Philbin and Kaur (2020) articulated that data collection concerning project management and social dimensions are important factors in designing and operationalizing scorecards to measure PMO performance. Almansoori et al. (2021) discussed leveraging the cost performance index, schedule variance index, cost variance index, project contribution margin, and complete performance index as the key performance indicators to measure PMO performance. Mahabir and Pun (2022) suggested the following performance metrics: enterprise reporting, project managers' adherence to processes, project managers' skills improvement, governance structure, and communications.

Summary

The main objective of this qualitative research study was to explore how PMOs in the energy sector could help mitigate cybersecurity risks associated with AI adoption during the transition to renewable energy, as the industry strives to meet its decarbonization goals. The literature review leveraged TAI-Cybersecurity PRM as the guiding framework, which integrated Trustworthy AI considerations and cybersecurity risk management, and explored scholarly literature related to barriers to AI adoption, risk management methodologies, and the role of project management offices in mitigating cybersecurity risks during the AI adoption journey. Chapter 3, Research Methods, discusses the study's research design, methodology, data collection procedures, and data analysis techniques.

Chapter 3: Research Method

The problem addressed in this study was that the energy sector had challenges adopting AI to meet the decarbonization targets by 2030 due to cybersecurity issues. In his written testimony to the U.S. House Energy & Commerce Committee, Renshaw (2023) discussed the pressing challenges of cybersecurity and data leaks in adopting AI within the energy sector. The energy sector, responsible for 75% of global greenhouse gas emissions, is under immense pressure to reduce its carbon footprint (EIA, 2023). The United Nation's IPCC report highlighted the critical need for substantial carbon emission reductions by 2030 to prevent the severe consequences of climate change (U.S. net zero plan, 2024). The purpose of this qualitative study was to explore how PMOs in the energy sector might assist in mitigating cybersecurity risks associated with AI adoption during the transition to renewable energy, as the industry works to meet its decarbonization goals.

The overarching intent of this study was to explore how PMOs in the energy sector might assist in the AI adoption journey, as the industry faces cybersecurity challenges while leveraging AI to accelerate its decarbonization goals through renewable energy projects. Given the energy sector's critical role in national security, economic stability, and public safety, it is increasingly becoming a prime target for cyberattacks (CISA, 2024). The PMO plays a key role in ensuring that projects align with organizational objectives, manage risks effectively, and are completed on time and within budget. Silvius (2021) highlighted the PMO's role as the custodian of project management standards and practices within organizations, ensuring that projects are planned and executed in alignment with the organization's strategic priorities. The qualitative methodology and exploratory case study design were selected for their suitability in examining the specific case of the PMO's role in mitigating cybersecurity risks during the adoption of AI to facilitate

the transition to renewable energy sources within the energy sector. This qualitative study addressed the research question: "How can PMOs assist in mitigating cybersecurity risks during the implementation of AI in the transition to renewable energy sources within the energy sector?".

Research Methodology and Design (Nature of the Study)

The qualitative research approach was selected over the quantitative approach for this study, as it explores the mitigation of cybersecurity challenges in the AI adoption journey within the energy sector by drawing on the real-life experiences and knowledge of experts. This method utilized open-ended questions to generate deeper understanding, whereas the quantitative approach focused on investigating cause-and-effect relationships and confirming or disproving assumptions through hypothesis testing (Bloomberg & Volpe, 2018).

The qualitative methodology and exploratory case study design were selected for this research study. The choice of this design was informed by its suitability for examining specific cases within industries and geographic regions, as well as its capacity to address real-life challenges while operating under time constraints (Yin, 2015). The case study design offered several strengths, including fostering a deep understanding of the topic, capturing diverse perspectives to gain a holistic view of the problem, and enhancing the validity and reliability of the findings. By collecting rich, detailed data from real-life contexts, this approach generated robust insights to address the research problem (Bloomberg & Volpe, 2018). The evidence-based nature enhanced the credibility of the research findings and their applicability to practical settings within the energy sector.

The significance of leveraging a case study design was underscored by Gomo et al. (2020) in their exploration of the PMO's role in knowledge transfer. In their study, conducted in

South Africa, the researchers focused on a single large organization, delving into how PMOs facilitate knowledge transfer within the organization. Similarly, Ichsan et al. (2023) leveraged a case study design to explore the role of PMO managers, restricting their study to PMO practitioners in Indonesia. Focusing on this context, the researchers examined the unique challenges and strategies PMO managers utilize in the Indonesian setting. Ichsan et al. gained a deeper understanding of PMO managers' multifaceted responsibilities and decision-making processes through qualitative data collection methods such as interviews and observations. Ershadi et al. (2021b) utilized a case study design to investigate the effects of PMOs in the construction industry. Their study, which focused on construction projects in Iran, sought to understand how PMOs contribute to project success and organizational performance. By conducting in-depth interviews with project managers, PMO staff, and other stakeholders, Ershadi et al. (2021a) explored the various roles and functions of PMOs in construction projects, shedding light on their impact on project outcomes.

A phenomenological research design is well-suited for exploring a group's subjective experiences and behaviors influenced by a discernible event (Bloomberg & Volpe, 2018). However, Bloomberg and Volpe (2018) highlighted that time plays a crucial role in phenomenological inquiry, requiring researchers to fully immerse themselves in the research environment to grasp the essence of participants' experiences. For instance, Watkins and Denney (2021) utilized a phenomenological approach in their study on stakeholder engagement, spanning multiple years, to capture the evolving dynamics. Similarly, Denney (2020) leveraged a phenomenological approach to investigating risk management practices in project management over a period of time. Although phenomenological research design provides valuable insights

into individual experiences and perceptions, it was unsuitable for addressing the research problem, which focuses on a specific case within the energy sector (Creswell & Poth, 2018).

Grounded theory focuses on generating a theory based on data derived from research participants' perspectives (Bloomberg & Volpe, 2018). Bloomberg and Volpe (2018) emphasized that this approach works backward from data to theory generation and is not suitable for studying a specific case. Sithambaram et al. (2021) utilized a grounded theory approach to capture key issues in agile projects across multiple industries. Therefore, a qualitative case study design methodology was selected for this research study.

Population and Sample

The study targeted PMO leaders, project managers, program managers, cybersecurity professionals, AI experts, and organizational leaders within the energy sector as the population for sample data. The following eligibility criteria must be met to participate in the study:

- Age 18 or older.
- At least 5 years of experience in the energy sector.
- Employment at a U.S.-based energy company.
- Hold a role as a PMO leader, Project Manager, Program Manager, Cybersecurity Professional, AI expert, or Organizational Leader.

Since the study focused on the role of PMOs in AI adoption within the energy sector, the targeted population was appropriate for the research.

The participants were recruited through purposive sampling. Since purposive sampling effectively selects participants with specialized expertise in the study area, this method was preferred. An estimated sample size of 15 experts, or until data saturation occurs, was considered for this study. Recruitment involved reaching out to potential participants through Personal

LinkedIn and the Project Management Institute (PMI) local chapter. By targeting individuals with substantial experience and expertise in the field, the study captured insights from those well-versed in the challenges and dynamics of PMO operations within the energy sector.

Materials and Instrumentation

The study employed materials and instrumentation to enhance the depth and accuracy of data collection. The inclusion of documentary materials along with other data collection methods improved the reliability and validity of the findings (Bloomberg & Volpe, 2018). Additionally, incorporating a triangulation mindset by utilizing publicly available U.S. DOE reports on AI and cybersecurity throughout the research process strengthened the study's credibility by ensuring that multiple perspectives and sources contribute to a comprehensive analysis (Yin, 2015).

Materials

The study considered both elicited and extant materials. Elicited materials involved both research participants and the researcher in producing data, whereas extant materials were pre-existing sources that the researcher could not influence (Bloomberg & Volpe, 2018). The study included the following elicited materials: journals, interview transcripts, and audio recordings. Additionally, the following extant materials, which were publicly available reports produced by the U.S. DOE, were considered:

- Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure (U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, 2024).
- Advanced Research Directions on AI for Science, Energy, and Security (Carter et al., 2023).
- Cybersecurity Baselines for Electric Distribution Systems and DER (NARUC, 2025).

Instruments

The study utilized a semi-structured interview guide as a qualitative instrument to gather information from the participants regarding their experiences, perspectives, and insights specific to PMO's role in the AI adoption journey in the energy sector. Interview protocols serve as tools to guide, customize, and standardize the interview process, ensuring that key areas of information are consistently gathered from each participant (Billups, 2021). Billups (2021) further articulated that these protocols facilitate the acquisition of detailed and precise insights from participants while allowing for flexibility and adaptability in data collection.

To develop this instrument, the tenets of the TAI-Cybersecurity PRM framework were utilized, along with insights from the literature review on trustworthy AI recommendations, challenges in AI adoption, the selection of risk management methodologies, and the role of project management offices. The interviews enabled the collection of rich data and in-depth insights to address the research question. The interview guide (see Appendix A) included warm-up questions and eight complex, open-ended questions designed to gain deep insights from experts. The interview lasted 30–45 minutes. Before beginning, after confirming the participant's eligibility, the consent letter was reviewed with the participants. Once the participants' consent was reviewed, agreed upon, and signed, the interview commenced. All study participants were asked the same questions.

Field testing was conducted to ensure the credibility and dependability of the data collected and to align with the Belmont principle of beneficence. The field test involved two experts from the energy sector who hold roles as PMO Leaders, Project Managers, Program Managers, Cybersecurity Professionals, AI Experts, or Organizational Leaders, each with at least 5 years of experience in a U.S.-based energy company. Additionally, a NU dissertation team

member reviewed the draft interview questions. Based on their feedback, the interview questions were revised accordingly. These experts did not participate in the actual interviews or provide answers to the interview questions. Therefore, a separate Institutional Review Board (IRB) review was not required for the field test. The interview questions were structured as follows:

- The first four questions focused on cybersecurity risk management in the AI adoption journey within the energy sector.
- The next three questions explored the PMO's role in mitigating cybersecurity risks during AI transformation.
- The final question sought expert recommendations on strengthening the PMO's role in mitigating cybersecurity risks in AI adoption within the energy sector.

These questions were carefully selected to provide rich data that addressed the research question regarding the role of PMOs in mitigating cybersecurity risks in AI adoption within the energy sector. Member checking was utilized to ensure the interview transcripts' trustworthiness.

Study Procedures

Recruitment of participants who met the eligibility criteria was conducted through the National University's IRB-approved posts on the PMI local chapter and the researcher's personal LinkedIn sites. Purposive sampling was used to recruit eligible participants. The steps for participant recruitment were as follows:

1. Obtained National University's IRB approval for the newsletter and LinkedIn posts.
2. Once approval was secured, posts were published on the researcher's personal LinkedIn and the PMI local chapter's newsletter. The posts contained information for interested participants to contact the researcher.

3. Interested participants who met the eligibility criteria received an informed consent agreement.
4. Eligible participants read, completed, and signed the informed consent agreement.
5. Participants' information and the signed informed consent agreement were stored securely on a password-protected researcher's computer.

The interview guide served as the primary data collection instrument for this study. Semi-structured interviews with open-ended questions were developed to encourage detailed responses. By asking open-ended questions and probing for deeper insights, the study aimed to uncover valuable perspectives on the research topic (Creswell & Poth, 2018). The data collection process followed these steps:

1. Obtained National University's IRB approval for the proposed research study.
2. Once approval was secured, the researcher conducted a field test with two experts and refined the interview questions as needed.
3. With participants' permission, audio recordings of the interviews were conducted.
4. Automated transcription was performed using Microsoft Teams.
5. Conducted interviews with the eligible participants using the revised interview guide.
6. Securely stored the audio recordings and transcriptions on the researcher's password-protected computer.

Data Analysis

The data analysis process began after collecting data from semi-structured interviews with a sample of 15 participants until data saturation occurred. Participants held roles as PMO leaders, project managers, program managers, cybersecurity professionals, AI experts, or organizational leaders and had at least 5 years of experience in a U.S.-based energy company.

NVivo qualitative analysis software is designed to help researchers organize, analyze, and interpret large volumes of unstructured data. The interview transcripts and the U.S. Department of Energy's reports on AI and Cybersecurity (see Appendix E) in the energy sector were uploaded into NVivo, where they were organized, categorized, coded, and queried. The data was then systematically analyzed to identify key patterns and emerging insights, ensuring alignment with the research question.

The study leveraged both deductive and inductive strategies. Deductive strategies were used to organize and align the research with the research question, while inductive strategies helped derive meaningful insights from the collected data (Admin, 2024). Influenced by the bracketing methods discussed by Thomas and Sohn (2023), the study employed reflexive journaling to eliminate researcher bias. Informed by Belotto's (2018) data analysis methods, the study used structural coding to label the interview transcripts related to the research question. Secondary labels included mitigated cybersecurity risks, unmitigated cybersecurity risks, AI adoption challenges, PMO services, and PMO maturity. Additionally, a descriptive coding method was used to capture the essence of the participants' responses.

To ensure trustworthiness, the study incorporated member checking and triangulation validation techniques, as informed by Bloomberg and Volpe (2018). Member checking involved sending the interview transcripts and themes to the participants within one week after the interview. Triangulation was performed by comparing audio recordings, interview transcripts, journals, and publicly available reports from the DOE. In this study, the researcher's role was to adopt an insider perspective, seek to discover and understand participants' experiences, bring their own perspective, and actively engage in the research process (Bloomberg & Volpe, 2018).

Assumptions

The study was based on four key assumptions. First, participants would provide truthful responses and avoid personal biases. For example, if participants hold biases against their organizational culture or PMO, they were assumed to still offer honest responses based on their own experiences. Second, participants were expected to be knowledgeable and capable of providing meaningful insights into the research topic. They were assumed to have relevant expertise and experience in PMO, AI, and cybersecurity risk management. Third, the data collection instrument designed for the study was expected to yield rich data and a deep understanding of the subject. The semi-structured interview guide was assumed to facilitate in-depth discussions, thereby enhancing the study's findings. Fourth, the TAI-Cybersecurity PRM framework was assumed to be appropriate for addressing cybersecurity risks in AI adoption within the energy sector.

Limitations

The study aimed to explore the role of PMOs in mitigating cybersecurity risks during the AI adoption journey in the energy sector. Its focus was limited to a single case, and participants were restricted to professionals working in U.S.-based energy organizations, which limited generalizability. The research was confined to cybersecurity risks and did not address other risks associated with trustworthy AI. Future research could expand into other industries and explore broader risks beyond cybersecurity. Additionally, the researcher's senior leadership roles in energy companies, personal interest in the research topic, and participants' preconceptions or emotional connections to the research problem could have introduced research bias. To mitigate this research bias, memo writing, a bracketing method, was leveraged during data collection to maintain objectivity.

Delimitations

The study utilized purposive sampling to target eligible participants from a specific population. While this technique effectively recruited participants with specialized expertise who met the eligibility criteria, it could have introduced selection bias since the researcher was responsible for recruitment (Bloomberg & Volpe, 2018). A small sample size was selected, which was suitable for an exploratory study, but limited the representation of the broader population and reduced generalizability. Additionally, eligible participants were interviewed only once, which could have resulted in responses that did not fully capture their experiences. Additionally, participants could modify their responses if they knew they were being studied or observed, a phenomenon known as the Hawthorne Effect (James & Vo, 2010). The study utilized pseudonyms or codes to anonymize their identities to minimize this.

Ethical Assurances

Before data collection began, participants received detailed information about the study's objectives, procedures, and rights. Informed consent was obtained from each participant, ensuring they understood the purpose of the research and voluntarily agreed to participate (Hu & Chang, 2017). To maintain confidentiality, pseudonyms or codes were assigned to anonymize participants' identities. Additionally, audio recordings and transcripts were securely stored and accessible only to authorized research personnel (Yin, 2015). Breaks were provided during interviews to minimize potential discomfort during data collection (Hu & Chang, 2017).

Summary

The study explored the role of PMO in mitigating cybersecurity risks during the adoption of AI in the energy sector. This exploratory research utilized a qualitative case study design, chosen for its suitability in examining specific cases within industries and geographic regions

and its ability to address real-life challenges under time constraints (Yin, 2015). Purposive sampling was selected for its effectiveness in generating deep insights from eligible participants with specialized knowledge in the study area. The population sample for the study included PMO leaders, project managers, program managers, cybersecurity professionals, AI experts, and organizational leaders within the energy sector. A semi-structured interview guide was used as a qualitative instrument to gather participants' experiences, perspectives, and insights regarding the PMO's role in AI adoption in the energy sector.

Before data collection began, informed consent was obtained from interested participants. National University's IRB approval was secured for the study. The memo writing bracketing method was used to mitigate researcher and participant bias. Member checking was used to validate participants' responses, enhancing the trustworthiness of the study. Audio recordings and interview transcriptions were securely stored and restricted to authorized research personnel. NVivo software was used for qualitative analysis. Chapter 4 will present the study's findings, including data analysis and interpretations of the collected data.

Chapter 4: Findings

The Project Management Body of Knowledge defines a Project Management Office (PMO) as a management structure that standardizes project governance processes and facilitates sharing resources, knowledge, and tools (Project Management Institute, 2021). Many organizations in the energy sector increasingly rely on effective PMOs to drive reform, ensuring strategic alignment and successful project execution. PMOs play a crucial role in managing the complexity of large-scale projects, particularly as the sector shifts towards renewable energy sources, infrastructure modernization, and sustainability goals. Brandes et al. (2023) emphasized that, given the current climate crisis, leveraging AI to manage projects in the energy sector is essential as the industry is adopting renewable energy technologies. According to a survey of 2314 professionals from 129 countries conducted by Müller et al. (2024), 76% believe that AI will transform the management of projects. Renshaw (2023) testified to the House Energy Subcommittee about the role of AI in the energy sector while highlighting the concerns with data privacy and security and the lack of explainability.

The problem this study addressed in this study is that the energy sector had challenges adopting AI to meet the decarbonization targets by 2030 due to cybersecurity issues. The United Nations' IPCC report highlighted the critical need for substantial carbon emission reductions by 2030 to prevent the severe consequences of climate change (U.S. net zero plan, 2024). In his written testimony to the U.S. House Energy & Commerce Committee, Renshaw (2023) discussed the pressing challenges of cybersecurity and data leaks in adopting AI within the energy sector. Cybersecurity is critical for the energy sector due to its pivotal role in national security, economic stability, and public safety (CISA, 2024). Energy infrastructure is increasingly becoming more digital and interconnected, making it a prime target for

cyberattacks. Disruptions in the energy sector caused by cyberattacks can lead to devastating consequences, including blackouts and economic instability, directly impacting public safety. Ershadi et al. (2021a) analyzed theoretical PMO success domains in the construction industry and suggested that "…future research can contextualize the topic by exploring the impact of different industry specifications". Ichsan et al. (2023) studied the role of PMO managers in Indonesian settings and recommended future research on the applicability of the role-based competency framework to other regions and sectors. Previous research on PMOs' influence on organizational success revealed the need for further study considering changing market conditions, more scrutinized regulatory requirements, the ongoing evolution of PMOs, and technological innovations. As the energy sector in the U.S. works to meet the National Grid's decarbonization targets, PMOs are expected to align strategically with organizational priorities. This research aimed to provide meaningful recommendations to organizational and PMO leaders in the energy sector to mitigate cybersecurity risks in adopting AI in renewable energy projects.

The purpose of this qualitative study was to explore how PMOs in the energy sector might assist in mitigating cybersecurity risks associated with AI adoption during the transition to renewable energy as the industry works to meet its decarbonization goals. By examining industry-specific regulatory requirements, secure design requirements, project management maturity, PMO leadership, organizational structure, and service delivery mechanisms, this study provided insights into how PMOs could align with strategic business objectives, ensure sustainable benefits, and overcome challenges specific to the energy sector in the United States. The qualitative methodology and exploratory case study design were selected for their suitability in examining the specific case of the PMO's role in mitigating cybersecurity risks during the adoption of AI to facilitate the transition to renewable energy sources within the energy sector.

The research analysis focused on publicly available DOE reports on AI and cybersecurity, as well as responses from qualified research participants with at least 5 years of experience in U.S.-based energy companies. These participants held roles such as PMO leaders, project managers, program managers, cybersecurity professionals, AI experts, and organizational leaders. The goal was to explore the role of PMOs in the AI adoption journey within the energy sector. Chapter 4 represents the overall findings of this research study. It is organized by the following research question addressed, the trustworthiness of the data, the results, the evaluation of findings, and a summary.

Trustworthiness of the Data

To establish trustworthiness, the principles of credibility, transferability, dependability, and confirmability were utilized in the research process. Credibility was ensured through prolonged engagement with the data, member checking, and triangulation to validate interpretations and findings. Transferability was addressed by providing detailed descriptions of the research context, methods, and data analysis procedures, and purposive sampling of experienced professionals from the energy sector. Dependability was ensured through transparent documentation of the research process and the data analysis methods. Confirmability was achieved through triangulation, audit trail, and maintaining transparency in the research process.

Credibility

To ensure the credibility of data collection and findings, the study utilized prolonged engagement with the research topic and data, member checks, field testing, triangulation, and purposive sampling to select study participants. Eligibility criteria were established, which included a minimum of 5 years of experience in the energy sector, employment at a U.S.-based

energy company, and holding a role as a PMO Leader, Project Manager, Program Manager, Cybersecurity Professional, AI Expert, or Organizational Leader. These participants had extensive experience in the energy sector, cybersecurity, AI, and project management. Their knowledge and experiences provided valuable insights into the research topic.

Field testing was conducted to enhance the credibility of the data collection process and to align with the Belmont principle of beneficence. The field test involved two senior leaders from the energy sector, with 30 and 14 years of experience, respectively. These individuals held roles as Chief Information Security Officer (CISO) and Director of Enterprise Security PMO, and possessed expertise in AI, cybersecurity, PMO, and project management. Additionally, a member of the NU dissertation team reviewed the semi-structured interview questions to ensure alignment with the research objectives. Member checks were utilized to validate the interpretation of findings, and triangulation was achieved by incorporating published Department of Energy (DOE) reports on AI and cybersecurity in the energy sector.

Dependability

Dependability was achieved through a clearly documented and transparent research process, along with systematic data analysis methods. Field notes and interview transcripts were securely preserved for a planned retention period of three years. A semi-structured interview guide was used to ensure that all 12 participants were presented with the same set of questions, and their responses were analyzed and compared for similarities and differences among participants. Field Testing and Triangulation were utilized to enhance the dependability of the data collected and analyzed. To protect participants' confidentiality, all responses were anonymized.

Transferability

In qualitative research, transferability refers to the development of context-specific findings that can be meaningfully applied to broader settings, while preserving the richness of the original context (Bloomberg & Volpe, 2018). In this qualitative study, transferability was supported through purposive sampling, thick description, and the provision of detailed information about the research topic and process. Purposive sampling included participants from the U.S. energy sector who had 5 or more years of relevant experience. These experts possessed substantial knowledge of the research topic. Participants were provided with comprehensive descriptions of the study's purpose, scope, and methodology to ensure informed and meaningful engagement. Field testing was conducted with two industry experts and a member of the dissertation team to validate the relevance and clarity of the research instrument. As a result, the findings may be applicable not only within the U.S. energy sector but also in other geographic regions and industries pursuing AI adoption.

Confirmability

Confirmability refers to the extent to which the findings and interpretations are clearly grounded in the collected data and analysis, rather than being influenced by the researcher's personal biases or perspectives (Bloomberg & Volpe, 2018). Confirmability was achieved through triangulation, audit trail, and maintaining transparency in the research process. A secure Microsoft Teams environment was provided to allow participants to share their responses directly and freely. All 12 participants were presented with the same set of field-tested interview questions, and the resulting transcripts were reviewed and validated to ensure accuracy and consistency. Interview transcripts and the U.S. DOE reports on AI and Cybersecurity (see Appendix E) in the energy sector were archived to enhance the transparency of the research

process. Additionally, audit trail and triangulation strategies were utilized to further ensure confirmability.

Data Saturation

Data saturation in qualitative research is the point at which newly collected data adds little or no additional insight to the research context. Data saturation was assessed by systematically reviewing and analyzing the collected data, identifying recurring patterns, and determining when thematic saturation occurred. Since all participants were from the same energy industry in the United States, saturation was reached after interviewing 12 participants.

Results

The results of this qualitative exploratory case study were derived from semi-structured interviews conducted with 12 participants, as well as an analysis of the U.S. Department of Energy's (DOE) reports on AI and cybersecurity (see Appendix E). To ensure a relevant and robust sample, participants were selected from the energy sector based on their knowledge and experience related to the research topic. Eligibility criteria were established, requiring participants to have a minimum of 5 years of experience in the energy sector, current employment at a U.S.-based energy company, and a professional role as a PMO Leader, Project Manager, Program Manager, Cybersecurity Professional, AI Expert, or Organizational Leader. The participants were categorized by their roles and areas of expertise (see Table 1). The participants' responses, along with the analysis of the U.S. Department of Energy's reports on AI and Cybersecurity (see Appendix E), were synthesized into five key themes (see Table 2).

Table 1

Participants Categorized by Role and Area of Expertise

Participant code	Role	Years of experience	Area of expertise
P1	Cybersecurity Leader	>5 Years	Cybersecurity, Program Management, Project Management
P2	Organizational Leader	>5 Years	Cybersecurity, AI, Project and Program Management
P3	Cybersecurity Leader	>5 Years	Cybersecurity, AI, Project and Program Management, PMO
P4	Organizational Leader	>5 Years	Cybersecurity, AI, Project and Program Management, and PMO
P5	Cybersecurity and Project Mgmt. Professional	>5 years	Cybersecurity, Project and Program Management, and PMO
P6	Organizational Leader	>5 Years	Cybersecurity, AI, Project and Program Management
P7	PMO Leader	>5 Years	Cybersecurity, PMO, Project and Program Management
P8	Organizational Leader	>5 Years	Cybersecurity, AI, PMO, Project and Program Management
P9	Organizational Leader	>5 Years	Cybersecurity, AI, PMO, Project and Program Management
P10	Organizational Leader	>5 Years	Cybersecurity, AI, Project Management
P11	Organizational Leader	>5 Years	Cybersecurity, AI, PMO, Project and Program Management
P12	Organizational Leader	>5 Years	Cybersecurity, AI, Project Management

Table 2

Participants' Responses Organized by Themes

Theme	Definition
Trustworthy AI	Trustworthy AI refers to artificial intelligence systems designed and operated in ways that uphold ethical principles, ensure safety and security, and maintain reliability throughout their lifecycle.
Context Understanding	Context understanding refers to the process of identifying an organization's critical systems and business processes and aligning its security risk management strategy without compromising business continuity.
Cybersecurity Risks	Cybersecurity risks are defined as the effect of uncertainty on or within information and technology. They refer to the loss of confidentiality, integrity, or availability of information, data, or information systems, and reflect potential adverse impacts to the organization.
Risk Management	Risk management is the systematic process of identifying, analyzing, and responding to risk factors throughout the lifecycle of a project, with the goal of minimizing negative impacts and maximizing potential benefits.
Project Management Office (PMO)	The Project Management Office (PMO) is a management structure that standardizes project-related governance processes and facilitates the sharing of resources, tools, techniques, and methodologies across the organization.

RQ1

How can PMOs assist in mitigating cybersecurity risks when adopting AI in transitioning to renewable energy sources in the energy sector?

Theme 1: Trustworthy AI. In defining and implementing Trustworthy AI requirements, participants reported that their organizations were setting up AI governance bodies with representation from legal, IT, cybersecurity, enterprise risk management, and other key stakeholders to oversee the use of AI technologies within the organization, updating existing

policies to account for the responsible use of AI, and training end users on the responsible use of AI technologies. P2 said, “Similar to our existing cybersecurity training and acceptable use policies for internet and data usage, we now also include AI standards and acceptable use guidelines related to AI technologies.” P8’s responses aligned with the establishment of an AI governance body, AI policies, an AI Risk Management Framework (AI RMF), and AI controls, but sharply pointed out that the adoption of AI is ad hoc and operates in the shadow of IT. P8 also emphasized that, “…NIST AI RMF may help [organizations] implement trustworthy AI and OWASP's Top 10 List for managing non-human identities (NHI) that come when implementing agent-based AI and Agentic AI-driven tools.”

P6 stated that the organization is using third-party AI tools and services that were designed and tested using Trustworthy AI principles. P10 remarked, “We’re shifting toward enabling innovation while managing risk, rather than just saying no and hoping people comply.” The Department of Energy (DOE) report R1 noted that, due to the highly impactful consequences of energy system failures, AI methods and systems must be validated and verified throughout the lifecycle of data and model development. Report R1 also highlighted that “AI must account for and characterize the uncertainties in measurement data and forecasts when making decisions and certify that it is resilient to interference.”

Theme 2: Context Understanding. Participants clearly noted that while AI technologies offer significant benefits, they also expand the organizational risk surface, necessitating a risk-based approach to manage these risks effectively. P8 stated, “It [AI-driven Information and Communication Technology (ICT) systems] also introduces cybersecurity, regulatory, and compliance risks, making the need for strong governance paramount.” P6 told, “Unlike

traditional technologies that are often centrally controlled, AI tools can be accessed and used more widely across an organization, which increases the risk surface."

P9 emphasized that tasks such as threat management, threat monitoring, and endpoint monitoring, which typically require significant human effort, can be enhanced by AI to deliver faster, deeper, and more accurate results. However, the use of AI could inadvertently increase the attack surface that must be actively monitored. The Department of Energy (DOE) Report R2 highlighted that while AI adoption in the energy sector can support the modernization of integrated energy delivery systems, improve reliability, and reduce energy costs, it also introduces challenges such as scalable computing due to system complexity, data privacy risks, and the need to manage uncertainties inherent in energy systems. Report R2 recommended that "distribution system owners and oversight bodies should use a risk-based approach to determine which assets are most critical to adopt the cybersecurity baselines."

Theme 3: Cybersecurity Risks. Participants emphasized that AI technologies differ significantly from traditional technology stacks, introducing new risks such as model poisoning, data leakage, data sensitivity, and data privacy concerns. These risks require a robust risk management framework to effectively manage and govern AI use. Additionally, respondents highlighted the ongoing need for human oversight and interaction when integrating AI into transformation projects. P3 noted, "Trusting AI systems too deeply, without appropriate checks and balances, can pose serious risks [in the energy sector's context, as it affects daily operations and the lives of millions]." P8 stated, "Organizations must contend with cybersecurity risks [such as model poisoning, model bias, data sensitivity, data leakage, etc.] and the rogue use of AI tools, which may have a negative impact within [organizations] due to poor governance".

The U.S. Department of Energy (DOE) Report R3 grouped AI-related risks in the energy sector into four major areas. Unintentional failure modes of AI refer to issues such as skewed model outputs caused by limited or poor-quality sensor data, inaccurate predictions during unforeseen events, misalignment between AI system design and organizational goals due to insufficient human oversight, and increased energy consumption driven by the use of large AI models. Adversarial attacks against AI are distinct from traditional cybersecurity threats, as they exploit the data-driven nature of AI systems. These include poisoning attacks that tamper with training data to induce faulty behavior, evasion attacks in which adversarial inputs closely resemble valid data to manipulate outputs, such as producing incorrect energy pricing, and data extraction attacks where sensitive information about energy infrastructure is retrieved. Hostile AI applications involve malicious use of AI, such as leveraging model inference to strengthen cyberattacks on energy infrastructure or deploying AI techniques to evade cybersecurity defenses. Finally, the compromise of the AI software supply chain occurs when adversaries exploit vulnerabilities in AI development and deployment processes, using compromised components as entry points to infiltrate and disrupt energy systems.

Theme 4: Risk Management. Participants outlined that their organizations are leveraging cybersecurity risk management frameworks such as NIST and MITRE ATT&CK, tailoring them to meet their specific organizational needs to effectively manage and govern cybersecurity risks. There was broad agreement among participants on using NIST as a strong foundational framework for developing risk management processes. P11 noted, “Looking ahead, we may incorporate the NIST AI Risk Management Framework into future assessments, especially when involving third-party vendors or when AI becomes more integrated into our operational landscape.” P10 stated, “It is important to remember, NIST is a framework, not a

rulebook. You use it to assess what applies to your organization and where your priorities lie." P8 added, "I'd recommend the use of the NIST AI RMF to apply tailored best-practice cybersecurity controls for AI implementation projects."

The U.S. Department of Energy (DOE) Report R2 highlighted that, "While current defense techniques are not mature enough to guarantee security against sophisticated attacks, potential risks can be mitigated through a range of best practices including training, data curation, access controls, and human supervision." Additionally, the DOE report R2 recommended 21 priority cybersecurity baselines for the secure management of assets, accounts, networks, and suppliers, measures that could significantly reduce risks and mature an organization's cybersecurity program.

Theme 5: Project Management Office. Participants believed that the PMO could play a vital role in the AI adoption journey within the energy sector. P4 and P12 expressed that the PMO should serve as a strategic enabler by leading the establishment of an AI governance structure closely aligned with the cybersecurity risk management framework, embedding AI best practices into projects, and implementing AI policies, standards, and methods to minimize AI-related risks. P9, P11, and P12 emphasized that the PMO needs to engage early by aligning with the AI Governance Group, integrating AI oversight, and applying its deep expertise in managing AI adoption risks. P10 highlighted that the PMO's experience in navigating complex environments would be a value-add in mitigating cybersecurity risks when collaborating with cybersecurity professionals. P7 articulated, "I strongly believe that the PMO is essential for project success. It also plays a key role in minimizing risk, especially when it comes to vendors working on our projects. We ensure they are compliant with our cybersecurity standards and that their work is performed safely and securely." Additionally, participants P7 and P9 noted that

organizations in the energy sector are generally open to supporting peer organizations, unlike in many other industries, and could benefit from sharing insights during the AI adoption journey.

Evaluation of the Findings

This study aimed to address the challenges faced by the energy sector in adopting AI in the transformation journey due to cybersecurity issues. The evaluation of the findings aligned with the existing research and the conceptual framework discussed in chapters 1 and 2. All 12 participants included in the study were from the energy sector, with at least 5 years of experience, and possessed relevant expertise and knowledge. The findings are consistent with existing research that underscores the importance of Trustworthy AI requirements and context-driven risk management in AI adoption, as reflected in the works of Vyhmeister & Castane (2024) and Melaku (2023). Notably, the findings align with the TAI-Cybersecurity PRM, which integrates Trustworthy AI principles into the risk management process. The study's findings align with the Industry 5.0 paradigm, which shifts the emphasis away from the digital-automation model of Industry 4.0 toward a human-centric AI framework.

The findings align with Bedué and Fritzsche's (2021) conceptualization that building trust in AI differs fundamentally from building trust in traditional technologies, due to AI's transformative potential to revolutionize business processes and decision-making. The emphasis on understanding organizational context is particularly significant, as it enables the alignment of security risk strategies with the broader enterprise risk appetite and tolerance. Participants highlighted that the PMO plays a pivotal role in integrating and ensuring Trustworthy AI within the risk management process, thereby strengthening the organization's security posture through the systematic identification, assessment, and mitigation of AI-specific risks.

RQ1

How can PMOs assist in mitigating cybersecurity risks when adopting AI in transitioning to renewable energy sources in the energy sector?

RQ1 explored how PMOs might assist in mitigating cybersecurity risks in the AI adoption journey in the energy sector. All participants highlighted the importance of establishing Trustworthy AI practices through a formal governance structure with representation from cross-functional teams, including legal, IT, cybersecurity, enterprise risk management, and other key stakeholders. They also emphasized updating existing cybersecurity policies and programs to include responsible AI use. This aligned with the TAI-Cybersecurity PRM framework's Trustworthy AI step, which highlighted the use of TAI principles to build trustworthy AI systems. Consistent with Mobayo et al. (2021) and Danks and Trusilo (2023), this study found that the absence of AI policies and regulations poses a significant barrier to adoption. Additionally, the respondents underscored the need for robust validation, verification, and resilience of AI systems due to the high-stakes nature of energy infrastructure, highlighting the importance of addressing data uncertainty and model robustness throughout the AI lifecycle. This is consistent with Danish's (2023) findings on the need for high-quality data in AI systems, which must be validated through robust measures, such as encryption, to ensure availability and support accurate predictions.

The findings indicated that, while the adoption of AI offers significant benefits, such as supporting the modernization of energy delivery systems, improving reliability, and reducing energy costs, it also expands the attack surface. This necessitates a risk-based approach to identify which systems and business processes are critical for maintaining business continuity. This is aligned with the TAI-Cybersecurity PRM framework's Context Understanding step,

which suggests that understanding an organization's context is crucial for effectively aligning the security risk management strategy to improve its security posture. Participants said that the data-driven nature of AI introduces new risks that differ from traditional cybersecurity threats, requiring a robust risk management framework to manage and govern these risks. This is consistent with Necula's (2023) findings, which highlighted that AI-driven cyberattacks pose new challenges, including adversarial AI and the manipulation of AI models, while also amplifying traditional methods such as phishing, malware, and data manipulation.

The findings also revealed that the PMO could play a vital role in the AI adoption journey within the energy sector by serving as a strategic enabler, leading the establishment of an AI governance structure aligned with the cybersecurity risk management framework, embedding AI best practices into projects, and implementing AI policies, standards, and methods to minimize AI-related risks. This is consistent with the findings of Silvius (2021) and Ichsan et al. (2023), who suggested that PMOs serve as strategic enablers by establishing standards and improving organizational and project performance. Most participants responded that the PMO should engage early by aligning with the AI Governance Group, integrating AI oversight, and leveraging its expertise in managing AI adoption risks. They also mentioned that PMOs' experience in navigating complex environments can add significant value in mitigating cybersecurity risks, particularly when working collaboratively with cybersecurity professionals. This is supported by the TAI-Cybersecurity PRM framework, which emphasizes the use of risk management steps, including conducting risk assessments, selecting risk mitigation options based on the organization's risk appetite, and establishing KPIs specific to TAI requirements to effectively mitigate cybersecurity risks.

Summary

This chapter provided an in-depth exploration of mitigating cybersecurity risks in the AI adoption journey in the energy sector by interviewing experts in the energy sector in the United States who held expertise in cybersecurity, AI, project management, and PMO, and the reports published by the Department of Energy on AI & Cybersecurity in the energy sector. The results were organized into five themes that contributed to the mitigation of cybersecurity risks in the AI adoption journey in the energy sector, which included Trustworthy AI, Context Understanding, Cybersecurity Risks, Risk Management, and Project Management Office.

The AI adoption in the energy sector faces high challenges due to the high consequences of energy systems failures, as it affects daily lives and national security. The chapter offered valuable insights into how the risks associated with AI technology are different from traditional cybersecurity risks and provided insights into how these new AI-related risks can be mitigated and the role of PMO in helping with mitigation efforts. Building on the findings from the analysis of the expert insights, it sets the stage for the next chapter. Chapter 5 will synthesize findings, highlight practical implications, propose recommendations for the energy sector to mitigate cybersecurity risks in the AI adoption journey, and outline avenues for future research.

Chapter 5: Implications, Recommendations, and Conclusions

Many organizations in the energy sector increasingly rely on effective project management offices (PMOs) to drive reform, ensure strategic alignment, and achieve successful project execution. PMOs play a crucial role in managing the complexity of large-scale projects, particularly as the sector shifts toward renewable energy sources, infrastructure modernization, and sustainability goals. Brandes et al. (2023) emphasized that, given the current climate crisis, leveraging AI to manage projects in the energy sector is essential as the industry adopts renewable energy technologies. Similarly, the U.S. Department of Energy (DOE) envisions AI as a critical enabler for grid modernization and achieving decarbonization goals through renewable energy transformation projects.

The problem addressed in this study was the energy sector's challenges in adopting AI to meet decarbonization targets by 2030 due to cybersecurity concerns. The IPCC stressed the urgency of substantial carbon emission reductions by 2030 to prevent the most severe consequences of climate change (U.S. Net Zero Plan, 2024). Reinforcing this urgency, Renshaw (2023), in written testimony to the U.S. House Energy & Commerce Committee, discussed pressing challenges of cybersecurity and data breaches in adopting AI within the energy sector. Cybersecurity is particularly critical because of the sector's pivotal role in national security, economic stability, and public safety (CISA, 2024). With energy infrastructure becoming increasingly digital and interconnected, the sector has become a prime target for cyberattacks. Disruptions caused by such attacks can lead to devastating outcomes, including blackouts, economic instability, and risks to public safety.

The purpose of this qualitative study was to explore how PMOs in the energy sector might assist in mitigating cybersecurity risks associated with AI adoption during the transition to

renewable energy as the industry works to meet its decarbonization goals. By examining industry-specific regulatory requirements, secure design requirements, project management maturity, PMO leadership, organizational structure, and service delivery mechanisms, this study provided insights into how PMOs could align with strategic business objectives, ensure sustainable benefits, and overcome challenges specific to the energy sector in the United States. A qualitative methodology and exploratory case study design were selected for their suitability in examining the specific case of the PMO's role in mitigating cybersecurity risks during AI adoption to facilitate the renewable energy transition within the energy sector. The results of this qualitative exploratory case study were derived from semi-structured interviews with 12 participants and an analysis of U.S. Department of Energy (DOE) reports on AI and cybersecurity. Participants were selected for their relevant expertise, with eligibility requiring at least 5 years of experience in the U.S. energy sector and current roles as PMO leaders, project or program managers, cybersecurity professionals, AI experts, or organizational leaders.

The study was guided by four key assumptions. First, participants were expected to provide truthful responses, even if they held biases against their organizational culture or PMO. Second, they were assumed to have relevant expertise in PMO, AI, cybersecurity, and project and program management to offer meaningful insights. Third, the semi-structured interview guide was expected to generate rich data and support in-depth discussions that would strengthen the findings. Finally, the TAI-Cybersecurity PRM framework was assumed to be suitable for addressing cybersecurity risks in AI adoption within the energy sector.

The study utilized purposive sampling to recruit participants from the energy sector with expertise in AI, PMO, cybersecurity, and project and program management. Data saturation was achieved after 12 interviews. Although the small sample size was appropriate for an exploratory

study, it limited broader representation and reduced generalizability. To minimize the Hawthorne effect, participants' responses were anonymized.

The study had several limitations. Because its focus was restricted to a single case, the energy sector in the United States, it lacked generalizability. Future research could expand to other industries and geographic contexts to enhance generalizability. In addition, the study examined only cybersecurity risks in AI adoption, excluding other types of risks. To address potential researcher bias stemming from the researcher's senior leadership role in the energy sector, memo writing was leveraged to maintain objectivity.

This chapter brings together the exploration of the role of PMOs in the AI adoption journey within the energy sector. In Chapter 4, the analysis of the data collected was grounded in existing research and the TAI-Cybersecurity PRM conceptual framework, which integrates trustworthy AI principles into the risk management process. The findings were organized into five themes: trustworthy AI, context understanding, cybersecurity risks, risk management, and the project management office (PMO). Building on the evaluation of these findings, this chapter discusses their implications and provides recommendations for practice. It also identifies directions for future research based on the study's limitations. In conclusion, this chapter synthesizes the research process, from the initial problem statement through the analysis of the findings' implications, underscoring the significance of the study and its contributions to practice.

Implications

The PMO plays a crucial role in ensuring that projects are aligned with organizational objectives, adhering to best practices, and are completed on time and within budget (Project Management Institute, 2021, p. 211). Through the evaluation of the findings, valuable insights

were generated regarding the role of PMOs in AI adoption within the energy sector. These findings were organized into five themes, addressing the research question while being grounded in existing research and the TAI-Cybersecurity conceptual framework. The TAI-Cybersecurity PRM framework integrates TAI requirements into cybersecurity risk management practices to effectively mitigate risks associated with AI adoption. This framework incorporates context-based cybersecurity risk management into the established TAI-PRM process, providing a comprehensive approach that enhances the overall security posture when implementing AI technologies and ensures that specific risks are systematically identified, assessed, and mitigated. The findings of this study supported the work of Vyhmeister and Castane (2024) on integrating TAI requirements into risk management practices through a TAI-PRM framework based on failure mode and effect analysis and the ISO 31000 standard. While their study focused solely on the manufacturing sector, this research extended the applicability to the energy sector.

Research Question 1

How can PMOs assist in mitigating cybersecurity risks when adopting AI in transitioning to renewable energy sources in the energy sector?

Theme 1: Trustworthy AI. This theme underscored the need to build trustworthy AI systems by defining and implementing trustworthy AI requirements. Participants shared several approaches to building trustworthy AI systems, including: (a) establishing an AI governance body with representation from relevant stakeholders; (b) creating AI policies, standards, and guidelines; (c) providing end-user training on responsible AI use; (d) validating third-party AI tools; and (e) validating and verifying AI methods throughout the AI life cycle. Participants further highlighted that building trustworthy AI systems requires continuous oversight and adherence to these practices.

Participants emphasized the importance of establishing AI governance bodies that include representatives from multiple departments, such as legal, IT, enterprise risk management, cybersecurity, and other key stakeholders, to define acceptable AI use policies and monitor adherence. They noted that, similar to existing acceptable use policies for internet and data usage, their organizations apply acceptable use guidelines for AI technologies. Participants also stated that the National Institute of Standards and Technology (NIST) AI Risk Management Framework and the Open Worldwide Application Security Project's (OWASP) Top 10 Non-Human Identities (NHI) may assist organizations in implementing trustworthy AI systems. Furthermore, they reported that their organizations use third-party AI tools designed and tested in alignment with trustworthy AI principles. The U.S. Department of Energy report emphasized that, given the highly consequential nature of energy infrastructure, AI methods must be validated and verified throughout the AI life cycle. The report also underscored the importance of characterizing uncertainties in measurement data and forecasts when making decisions and ensuring that AI systems remain resilient to interference.

Theme 2: Context Understanding. This theme revealed that while AI technologies offer significant benefits, they also expand the organizational risk surface, necessitating a risk-based approach for effective management. Participants discussed how AI technologies broaden the attack surface for threat actors and emphasized the need for risk-based strategies when implementing AI systems. They noted that AI-driven information and communication technology (ICT) systems introduce cybersecurity, regulatory, and compliance risks that require strong governance. Unlike traditional technologies that are centrally controlled, AI tools can be accessed and used more broadly across the organization, further increasing the risk surface. Participants highlighted that tasks such as threat management, threat monitoring, and endpoint

monitoring, typically requiring significant human effort, can be enhanced by AI to deliver faster, deeper, and more accurate results. However, they cautioned that AI use may also inadvertently expand the attack surface, requiring continuous monitoring. The U.S. Department of Energy report reinforced this perspective, recommending that distribution system owners and oversight bodies adopt a risk-based approach to identify critical assets and establish appropriate cybersecurity baselines.

Theme 3: Cybersecurity Risks. This theme highlighted that AI technologies diverge from traditional technology stacks and bring novel cybersecurity risks that necessitate a comprehensive risk management framework. Participants, along with reports from the U.S. Department of Energy, identified AI-related risks arising from (a) lack of checks and balances, (b) poor governance, (c) rogue use of AI tools, (d) unintentional failure modes of AI, (e) adversarial attacks, and (f) compromise of the AI supply chain. Participants cautioned that trusting AI technologies without appropriate safeguards could result in serious consequences, particularly in the energy sector, where operations directly affect the daily lives of millions. They further warned that poor governance and the unauthorized or rogue use of AI tools may exacerbate cybersecurity vulnerabilities.

Recognizing the severity of these risks, the U.S. Department of Energy categorized AI-related risks into four major areas. The first involves unintentional failure modes of AI, such as skewed outputs from poor-quality or limited sensor data, inaccurate predictions during unforeseen events, misalignment between AI system design and organizational objectives due to insufficient human oversight, and the increased energy consumption associated with large-scale AI models. The second area concerns adversarial attacks that exploit the data-driven nature of AI systems, including poisoning attacks that manipulate training data to induce faulty behaviors,

evasion attacks where adversarial inputs mimic valid data to alter outputs (e.g., generating incorrect energy pricing), and data extraction attacks that expose sensitive energy infrastructure information. The third area addresses hostile AI applications, including the unauthorized or malicious use of AI tools that undermine organizational security and governance. Finally, the fourth area highlights risks associated with the compromise of the AI software supply chain, wherein adversaries exploit vulnerabilities in AI development and deployment processes, using compromised components as entry points to infiltrate and disrupt energy systems.

Theme 4: Risk Management. This theme revealed that organizations are leveraging risk management frameworks to manage and govern cybersecurity risks. Participants, supported by reports from the U.S. Department of Energy (DOE), highlighted approaches to mitigating AI-related risks, including (a) foundational risk management frameworks, (b) cybersecurity best practices, and (c) cybersecurity priority baselines. Participants widely agreed on using the NIST framework as the foundation for risk management and indicated potential future use of the NIST AI Risk Management Framework when engaging with third-party suppliers.

Participants recommended implementing tailored cybersecurity controls based on the NIST AI Risk Management Framework in AI implementation projects. Acknowledging the immaturity of current defense techniques to address evolving AI risks, the DOE report emphasized the importance of cybersecurity best practices such as end-user training, data curation, access controls, and human oversight. Additionally, the DOE report recommended establishing cybersecurity priority baselines to securely manage assets, accounts, networks, and suppliers.

Theme 5: Project Management Office (PMO). This theme provided valuable insights into the role of project management offices (PMOs) in the energy sector. Participants strongly

emphasized that PMOs play a critical role in the AI adoption journey. Specifically, they highlighted that PMOs can (a) support the establishment of AI governance structures, (b) embed cybersecurity best practices into AI projects, (c) implement AI policies and standards, (d) engage early and remain involved throughout the AI lifecycle, (e) leverage their expertise in navigating complex environments, and (f) foster knowledge sharing among peer organizations.

Participants underscored that PMOs should act as strategic partners by leading governance initiatives, embedding best practices, and enforcing policies to mitigate AI-related risks. They emphasized the importance of early engagement and the application of PMO expertise throughout AI implementation. Participants also noted that the PMO's experience in managing complex environments is crucial for successful AI adoption and effective risk management, particularly when working with third-party suppliers while adhering to cybersecurity standards. Finally, they highlighted that collaboration among peer organizations in the energy sector offers valuable opportunities for knowledge sharing.

Recommendations for Practice

Based on the findings, several practice recommendations emerged. These are organized into five categories: building trustworthy AI, utilizing a risk-based approach, mitigating cybersecurity risks, enhancing awareness of AI-related risks, and engaging the PMO in the AI adoption process. The recommendations are grounded in existing research and the TAI-Cybersecurity PRM framework.

Build Trustworthy AI. The findings indicate the importance of defining and implementing trustworthy AI in mitigating cybersecurity risks. This is supported by the integration of TAI into risk management practices, as suggested by Vyhmeister and Castane (2024), and is aligned with the TAI-Cybersecurity PRM framework's Trustworthy AI step,

which highlights the use of TAI principles to build trustworthy AI systems. Based on the findings, it is recommended to establish a robust governance structure to oversee and monitor the responsible use of AI within organizations. An AI governance body should be established with representation from key stakeholders, including Information Technology, Legal, Enterprise Risk Management, Cybersecurity, and other relevant functions. This body would be responsible for creating policies, standards, and guidelines related to the responsible use of AI. In addition, based on the findings, it is recommended to validate third-party AI tools before their widespread adoption across the organization. Organizational users are also required to be trained in the responsible use of AI. Given the potentially severe consequences of energy system failures, it is recommended that AI methods and systems be validated and verified throughout the lifecycle of data and model development.

Utilize a Risk-Based Approach. While the adoption of AI brings significant benefits to the energy sector, such as modernizing energy delivery systems, improving reliability, and reducing energy costs, it also expands the attack surface. Based on the findings, it is recommended to adopt a risk-based approach to managing these risks effectively. In addition, it is suggested that distribution system owners and oversight bodies identify the most critical assets and ensure that appropriate cybersecurity baselines are implemented. This aligns with the analyses of risk influences proposed by Bashir et al. (2023) and Cheng and Darsa (2021) and with the TAI-Cybersecurity PRM framework's Context Understanding step, which emphasizes that understanding an organization's context is crucial for effectively aligning the security risk management strategy to improve its security posture.

Enhance the Awareness of AI Risk Factors. The findings indicate the importance of increasing awareness of AI risk factors to ensure that appropriate mitigation strategies are

applied. They also indicate that AI-related risks may stem from insufficient checks and balances, weak governance, unauthorized use of AI tools, unintentional failure modes, adversarial attacks, and vulnerabilities in the AI supply chain. Based on the findings, it is recommended to maintain ongoing human oversight and interaction when integrating AI into transformation projects. It also cautions against risks such as skewed model outputs caused by limited or poor-quality sensor data, inaccurate predictions during unforeseen events, misalignment between AI system design and organizational goals due to inadequate human oversight, and increased energy consumption associated with large AI models. These concerns are supported by Necula (2023) and Vulpe et al. (2024), who highlighted the macro- and micro-level impacts of AI systems that require proactive risk awareness and align with the TAI-Cybersecurity PRM framework's Risk Assessment step.

Mitigate Cybersecurity Risks. Based on the findings, it is recommended to adopt a robust risk management framework as a foundation while tailoring appropriate cybersecurity and AI controls to mitigate risks. This is supported by Melaku's (2023) work on leveraging a context-based cybersecurity framework to mitigate risks and align with the TAI-Cybersecurity PRM framework's Risk Management steps. Cybersecurity risk management (CRM) is a systematic approach to identifying, analyzing, and addressing cybersecurity threats and vulnerabilities within an organization to safeguard assets and maintain resilience against cyberattacks (Lee, 2021). Because defense techniques for addressing AI-related risks are still immature, organizations are encouraged to adopt cybersecurity best practices, including end-user training, access controls, data curation, and human oversight. Additionally, it is recommended to establish cybersecurity priority baselines to securely manage assets, accounts, networks, and suppliers.

Engage PMO Early in the AI Adoption Journey. The evaluation of findings indicates that project management offices (PMOs) may play an important role in the AI adoption journey within the energy sector, aligning with the research of Sandhu et al. (2019) and Khafri et al. (2022) on defining PMO functions and with the TAI-Cybersecurity PRM framework's Risk Management steps. Based on the findings, it is recommended that, as strategic enablers, PMOs support the establishment of AI governance structures and implement policies and standards to promote trustworthy AI systems. PMOs are encouraged to engage early and remain involved throughout the AI lifecycle, leverage their expertise to navigate complex environments and mitigate risks, embed cybersecurity best practices into AI projects, and foster knowledge sharing among peer organizations in the energy sector.

Recommendations for Future Research

Drawing on the study's limitations, several potential research opportunities are identified. These included expanding the scope to enhance the generalizability of the findings, examining additional risks such as ethical, privacy, and safety concerns, investigating the impact of evolving AI regulations, and conducting quantitative studies. Building on this study's findings, future researchers could pursue these directions to advance knowledge and strengthen contributions to theory and practice.

Enhance the Generalizability of The Findings. While this study focused on the role of PMOs in the AI adoption journey within the energy sector in the United States, future research could be expanded geographically and across industries. Future studies could also examine the role of PMOs in AI adoption in both developed and developing countries and within organizations of varying sizes. As Müller et al. (2024) noted, 76% of 2,314 professionals from 129 countries strongly believed that AI would transform project management. Such expansion

would provide deeper insights into how PMOs might support AI adoption under different organizational, cultural, economic, and political contexts, thereby enhancing the generalizability of the findings.

Broaden the Scope to Include Other Risks. This study focused on building trustworthy AI to mitigate cybersecurity risks in the AI adoption journey; however, future research could expand to include other risks, such as ethical, privacy, and safety risks. As suggested by Vyhmeister & Castane (2024), the concept of trustworthy AI, built on foundational principles of validation and reliability, safety, security, privacy, explainability and interpretability, fairness with bias mitigation, transparency, and accountability, is crucial to maximizing societal benefits while minimizing risks. Building on this study's findings and expanding the scope to include additional risks would provide organizations with a more comprehensive view of how to develop risk-conscious, trustworthy AI.

Investigate the Effect of Changing AI Laws. Future research could examine the effect of changing AI laws on adoption and how PMOs might assist organizations in navigating evolving regulatory requirements while ensuring both compliance and value delivery. As outlined by House (2023), challenges related to AI misinformation, environmental sustainability, and the labor market require international cooperation and interoperable governance. Building on this study's findings by expanding the scope to include regulatory requirements would enable organizations to strengthen compliance efforts while also supporting national security.

Quantitative Study. This research utilized a qualitative methodology and an exploratory case study design to draw on the real-life experiences and knowledge of experts. Future research could utilize quantitative methodologies to investigate cause-and-effect relationships and confirm or disprove assumptions through hypothesis testing (Bloomberg & Volpe, 2018).

Building on this study's findings and analyzing them quantitatively would provide organizations with both qualitative and quantitative data to inform AI adoption decisions.

Conclusions

This study examined the role of Project Management Offices (PMOs) in the AI adoption journey within the energy sector and their contribution to mitigating cybersecurity risks. The results indicated the importance of defining and implementing trustworthy AI requirements, consistent with existing research and the TAI-Cybersecurity PRM framework, to support the development of trustworthy AI systems. Given the potentially severe consequences of energy system failures, it is recommended that AI methods and systems be validated and verified throughout the entire lifecycle of data and model development. Based on the results, it is further recommended that organizations establish a robust governance structure to oversee and monitor the responsible use of AI.

Although AI adoption offers significant benefits to the energy sector, such as modernizing energy delivery systems, improving reliability, and reducing costs, it has also expanded the attack surface. To manage these risks effectively, a risk-based approach is recommended, along with raising awareness of AI-specific risk factors to ensure appropriate mitigation strategies. These risks may arise from poor governance, inadequate checks and balances, unauthorized use of AI tools, unintentional system failures, adversarial attacks, or vulnerabilities in the AI supply chain. The results indicated the ongoing need for human oversight and intervention when integrating AI into transformation projects, as well as the importance of adopting a comprehensive risk management framework as a foundation while tailoring cybersecurity and AI controls to specific organizational contexts. Because defense techniques for addressing AI-related risks remain immature, organizations are encouraged to

implement proven cybersecurity practices, such as end-user training, access controls, data curation, and human oversight. Based on the findings, it is recommended that, as strategic enablers, PMOs support the establishment of AI governance structures and implement policies and standards to promote trustworthy AI systems.

While this study focused on the role of PMOs in AI adoption in the U.S. energy sector, future research could extend to other industries and geographic regions. Broader categories of risk, including ethical, privacy, and safety concerns, should also be examined. In addition, future studies might investigate the impact of evolving AI regulations on adoption and assess how PMOs could support organizations in maintaining compliance while ensuring value delivery. Finally, quantitative research could complement these findings by testing cause-and-effect relationships and validating assumptions through hypothesis-driven analysis.

References

Admin, M. (2024, January 25). *Qualitative research design and data analysis: Deductive and inductive approaches — SAGE Research Methods Community*. Sage Research Methods Community. https://researchmethodscommunity.sagepub.com/blog/qualitative-research-design-and-data-analysis-deductive-and-inductive-approaches

Akello, N. B. O. (2024). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences*, *11*(1), 148–162. https://doi.org/10.30574/wjaets.2024.11.1.0152

Akuffo-Badoo, E. B. (2022). Understanding advanced persistent threats. *Advances in Multidisciplinary & Scientific Research Journal Publication*, *1*(1), 15–22. https://doi.org/10.22624/aims/crp-bk3-p3

Almansoori, S., Rahman, I. A., & Memon, A. H. (2021, June 28). *Common attributes influencing PMO practices in UAE Construction Industry*. https://www.tojqi.net/index.php/journal/article/view/1151

Alsayegh, A., & Masood, T. (2024). Leveraging generative AI for knowledge-driven information retrieval in the energy sector. *MATEC Web of Conferences*, *401*, 10008. https://doi.org/10.1051/matecconf/202440110008

Badi, F. K. A., Alhosani, K. A., Jabeen, F., Stachowicz-Stanusch, A., Shehzad, N., & Amann, W. (2021b). Challenges of AI adoption in the UAE healthcare. *Vision the Journal of Business Perspective*, *26*(2), 193–207. https://doi.org/10.1177/0972262920988398

Bailey, T., Maruyama, A., & Wallance, D. (2020, November 3). *The energy-sector threat: How to address cybersecurity vulnerabilities*. McKinsey & Company.

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Barbalho, S. C. M., & Silva, G. L. (2021). Control of project data and team satisfaction as results of PMO effort in new product development projects. *International Journal of Managing Projects in Business*, *15*(1), 121–149. https://doi.org/10.1108/ijmpb-02-2021-0045

Bashir, H., Hamdan, S., Ojiako, U., Haridy, S., Shamsuzzaman, M., & Zarooni, H. a. A. (2023). A weighted fuzzy social network analysis-based approach for modeling and analyzing relationships among risk factors affecting project delays. *Engineering Management Journal*, *36*(1), 3–13. https://doi.org/10.1080/10429247.2022.2162305

Bedué, P., & Fritzsche, A. (2021). Can we trust AI? An empirical investigation of trust requirements and guide to successful AI adoption. *Journal of Enterprise Information Management*, *35*(2), 530–549. https://doi.org/10.1108/jeim-06-2020-0233

Bellini, V., Cascella, M., Cutugno, F., Russo, M., Lanza, R., Compagnone, C., & Bignami, E. G. (2022). Understanding basic principles of Artificial Intelligence: a practical guide for intensivists. *PubMed*, *93*(5), e2022297. https://doi.org/10.23750/abm.v93i5.13626

Bello, S., & Hassan, Y. A. (2024). Examining the effect of geopolitical risks on renewable energy consumption in OECD countries. *Environmental Economics*, *15*(2), 108–117. https://doi.org/10.21511/ee.15(2).2024.08

Belotto, M. (2018). Data analysis methods for qualitative research: Managing the challenges of coding, interrater reliability, and thematic analysis. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2018.3492

Bhatt, N., Bhatt, N., Prajapati, P., Sorathiya, V., Alshathri, S., & El-Shafai, W. (2024). A Data-Centric Approach to improve performance of deep learning models. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-73643-x

Billups, F. D. (2021). *Qualitative data collection tools: Design, development, and applications*. https://doi.org/10.4135/9781071878699

Bloomberg, L., & Volpe, M. (2018). *Completing your qualitative dissertation: A roadmap from beginning to end*. https://doi.org/10.4135/9781452226613

Bouramdane, A. (2023). Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705. https://doi.org/10.3390/jcp3040031

Brandas, C., Didraga, O., & Albu, A. (2023). A SWOT analysis of the role of artificial intelligence in project management. *Informatica Economica*, *27*(4/2023), 5–15. https://doi.org/10.24818/issn14531305/27.4.2023.01

Carter, J., Feddema, J., Kothe, D., Neely, R., Pruet, J., Stevens, R., Balaprakash, P., Beckman, P., Foster, I., Iskra, K., Ramanathan, A., Taylor, V., Thakur, R., Agarwal, D., Crivelli, S., De Jong, B., Rouson, D., Sohn, M., Wetter, M., . . . Dietrich, E. (2023). *Advanced research directions on AI for science, energy, and security: Report on Summer 2022 workshops*. https://doi.org/10.2172/1986455

Chen, Y., Li, Y., & Zha, Y. (2024). ISM-BN-Based Schedule Risk Analysis in Large-Scale Public Projects. *Advances in Civil Engineering*, *2024*(1). https://doi.org/10.1155/adce/5517481

Cheng, M., & Darsa, M. H. (2021). Construction schedule risk assessment and management strategy for foreign general contractors working in the Ethiopian construction industry. *Sustainability*, *13*(14), 7830. https://doi.org/10.3390/su13147830

CISA. (2024). *Energy sector*. Retrieved September 29, 2024, from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches*. SAGE Publications.

CSRC. (n.d.). *Cybersecurity Risk - Glossary | CSRC*. Retrieved October 2, 2024, from https://csrc.nist.gov/glossary/term/cybersecurity_risk

Danish, M. S. S. (2023). AI in energy: Overcoming unforeseen obstacles. *AI*, *4*(2), 406–425. https://doi.org/10.3390/ai4020022

Danks, D., & Trusilo, D. (2023). Artificial intelligence and humanitarian obligations. *Ethics and Information Technology*, *25*(1). https://doi.org/10.1007/s10676-023-09681-2

Denney, V. P. (2020). Exploring the upside of risk in project Management: A phenomenological inquiry. *JMPM*, *8*(1). https://doi.org/10.19255/jmpm02312

DOE. (2024a). *DOE Industrial Decarbonization Roadmap*. Energy.gov. https://www.energy.gov/industrial-technologies/doe-industrial-decarbonization-roadmap

DOE. (2024b). *How AI can help clean energy meet growing electricity demand*. Energy.gov. https://www.energy.gov/policy/articles/how-ai-can-help-clean-energy-meet-growing-electricity-demand

Domingues, L., & Ribeiro, P. (2023). Project management maturity models: Proposal of a framework for models comparison. *Procedia Computer Science*, *219*, 2011–2018. https://doi.org/10.1016/j.procs.2023.01.502

Egwim, C. N., Alaka, H., Toriola-Coker, L. O., Balogun, H., & Sunmola, F. (2021). Applied artificial intelligence for predicting construction projects delay. *Machine Learning With Applications*, *6*, 100166. https://doi.org/10.1016/j.mlwa.2021.100166

EIA. (2023). *Energy Facts*. https://www.eia.gov/energyexplained/us-energy-facts/. Retrieved November 17, 2024, from https://www.eia.gov/energyexplained/us-energy-facts/

Ershadi, M., Jefferies, M., Davis, P., & Mojtahedi, M. (2021a). Achieving sustainable procurement in construction projects: The pivotal role of a project management office. *Construction Economics and Building*, *21*(1). https://doi.org/10.5130/ajceb.v21i1.7170

Ershadi, M., Jefferies, M., Davis, P., & Mojtahedi, M. (2021b). Project management offices in the construction industry: a literature review and qualitative synthesis of success variables. *Construction Management and Economics*, *39*(6), 493–512. https://doi.org/10.1080/01446193.2021.1916052

Ershadi, M., Jefferies, M., Davis, P., & Mojtahedi, M. (2021c). Comparative analysis of PMO functions between the public and private sectors: Survey of high-performing construction organizations. *Journal of Construction Engineering and Management*, *147*(11). https://doi.org/10.1061/(asce)co.1943-7862.0002181

Fernandes, G., Sousa, H., Tereso, A., & O'Sullivan, D. (2021). Role of the Project Management Office in university research Centers. *Sustainability*, *13*(21), 12284. https://doi.org/10.3390/su132112284

Gowtham, M., & B, P. H. (2021). Semantic Query-Featured Ensemble Learning Model for SQL-Injection attack detection in IoT-Ecosystems. *IEEE Transactions on Reliability*, *71*(2), 1057–1074. https://doi.org/10.1109/tr.2021.3124331

Gupta, R., Nair, K., Mishra, M., Ibrahim, B., & Bhardwaj, S. (2024). Adoption and impacts of generative artificial intelligence: Theoretical underpinnings and research agenda. *International Journal of Information Management Data Insights*, *4*(1), 100232. https://doi.org/10.1016/j.jjimei.2024.100232

House, W. (2023, October 30). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Howatt, J. (2024, May 22). *AI is Already Impacting the Energy sector - EPRI Journal*. EPRI Journal. https://eprijournal.com/ai-is-already-impacting-the-energy-industry/

Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk*. John Wiley & Sons.

Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business. *AI And Ethics*, *4*(3), 791–804. https://doi.org/10.1007/s43681-024-00443-4

Ichsan, M., Sadeli, J., Jerahmeel, G., & Yesica, Y. (2023). The role of project management office (PMO) manager: A qualitative case study in Indonesia. *Cogent Business & Management*, *10*(2). https://doi.org/10.1080/23311975.2023.2210359

IEA. (2024, January 24). *Renewables*. International Energy Agency. https://www.iea.org/news/clean-sources-of-generation-are-set-to-cover-all-of-the-world-s-additional-electricity-demand-over-the-next-three-years

IRENA. (2023). *Energy Outlook*. Retrieved January 12, 2025, from https://www.irena.org/Energy-Transition/Outlook

Ismail, F. B., Al-Faiz, H., Hasini, H., Al-Bazi, A., & Kazem, H. A. (2024). A comprehensive review of the dynamic applications of the digital twin technology across diverse energy sectors. *Energy Strategy Reviews*, *52*, 101334. https://doi.org/10.1016/j.esr.2024.101334

James, L., & Vo, H. (2010). Hawthorne Effect. In *Encyclopedia of research design* (Vol. 0, pp. 561–563). SAGE Publications, Inc.,. https://doi.org/10.4135/9781412961288

Jedrusik, A. (2024). Project risk management based on known project management methodologies. *EUROPEAN RESEARCH STUDIES JOURNAL*, *XXVII*(Issue 4), 14–24. https://doi.org/10.35808/ersj/3503

Jiang, C., Xu, H., Huang, C., & Huang, Q. (2022). An adaptive information security system for 5G-Enabled smart grid based on artificial neural network and Case-Based learning algorithms. *Frontiers in Computational Neuroscience*, *16*. https://doi.org/10.3389/fncom.2022.872978

Jimenez, V. M. M., & Gonzalez, E. P. (2022). The role of artificial intelligence in Latin Americas energy transition. *IEEE Latin America Transactions*, *20*(11), 2404–2412. https://doi.org/10.1109/tla.2022.9904766

Khafri, A. Z., Aboumasoudi, A. S., & Khademolqorani, S. (2022). Prioritizing Multi-Interwoven factors in the Project Management Office using Delphi and Fuzzy DEMATEL. *Journal of Mathematics*, *2022*(1). https://doi.org/10.1155/2022/6482419

Kim, J., Kim, C., Kim, G., Kim, I., Abbas, Q., & Lee, J. (2021). Probabilistic tunnel collapse risk evaluation model using analytical hierarchy process (AHP) and Delphi survey technique. *Tunnelling and Underground Space Technology*, *120*, 104262. https://doi.org/10.1016/j.tust.2021.104262

Li, S., Xiang, J., Li, R., & Wang, D. (2024). Risk-return analysis of clean energy grid project investment based on integrated ISM and Monte Carlo model. *EAI Endorsed Transactions on Energy Web*, *11*. https://doi.org/10.4108/ew.7243

Magyari, J. (2023). Decarbonization challenges and opportunities in the Central European energy sector: Implications for management. *Society and Economy*, *45*(4), 451–471. https://doi.org/10.1556/204.2023.00007

Mahabir, R. J., & Pun, K. F. (2022). Revitalizing project management office operations in an engineering-service contractor organization: A key performance indicator based performance management approach. *Business Process Management Journal*, *28*(4), 936–959. https://doi.org/10.1108/bpmj-10-2021-0655

McKinsey & Company. (2024, April 3). *What is AI (artificial intelligence)?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai

Meiser, M., & Zinnikus, I. (2024). A survey on the use of synthetic data for enhancing key aspects of trustworthy AI in the energy domain: Challenges and opportunities. *Energies*, *17*(9), 1992. https://doi.org/10.3390/en17091992

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6), 101. https://doi.org/10.3390/risks11060101

Mobayo, J. O., Aribisala, A. F., Yusuf, S. O., & Belgore, U. (2021). The awareness and adoption of artificial intelligence for effective facilities management in the energy sector. *Journal*

of Digital Food Energy & Water Systems, *2*(2). https://doi.org/10.36615/digitalfoodenergywatersystems.v2i2.718

NARUC. (2025). *Cybersecurity Baselines for electric Distribution Systems and DER: Interim Implementation Guidance.* https://pubs.naruc.org/pub/96999449-C80D-6780-A3B6-273988121062

Necula, S. (2023). Assessing the Potential of Artificial intelligence in advancing clean energy technologies in Europe: A Systematic review. *Energies*, *16*(22), 7633. https://doi.org/10.3390/en16227633

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

Ntshwene, K., Ssegawa, J., & Rwelamila, P. (2022). Key Performance Indicators (KPIs) for measuring PMOs Services in selected Organizations in Botswana. *Procedia Computer Science*, *196*, 964–972. https://doi.org/10.1016/j.procs.2021.12.098

Paton, S., & Andrew, B. (2019). The role of the Project Management Office (PMO) in product lifecycle management: A case study in the defence industry. *International Journal of Production Economics*, *208*, 43–52. https://doi.org/10.1016/j.ijpe.2018.11.002

Pepin, L., Wang, L., Wang, J., Han, S., Pishawikar, P., Herzberg, A., Zhang, P., & Miao, F. (2022). Botnets Breaking Transformers: Localization of power botnet attacks against the distribution grid. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2203.10158

Philbin, S. P., & Kaur, R. (2020). Measuring PMO Performance – Application of the Balanced Scorecard in a collaborative research context. *Journal of Modern Project Management*, *7*(4). https://doi.org/10.19255/jmpm02213

Project Management Institute. (2021). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management (ENGLISH)* (7th ed.).

Puthal, D., & Mohanty, S. (2021). Cybersecurity issues in AI. *IEEE Consumer Electronics Magazine*, *10*(4), 33–35. https://doi.org/10.1109/mce.2021.3066828

Regona, M., Yigitcanlar, T., Xia, B., & Li, R. Y. M. (2022). Opportunities and adoption Challenges of AI in the construction industry: A PRISMA review. *Journal of Open Innovation Technology Market and Complexity*, *8*(1), 45. https://doi.org/10.3390/joitmc8010045

Renshaw, J. (2023). *The role of artificial intelligence in powering America's energy future*. Hearing of the House Energy and Commerce Committee, Subcommittee on Energy, Climate, and Grid Security, United States House of Representatives. https://publicdownload.epri.com/PublicAttachmentDownload.svc/AttachmentId=86002

Roy, S. (2021). Denial of service attack on protocols for smart grid communications. In *IGI Global eBooks* (pp. 560–578). https://doi.org/10.4018/978-1-7998-5348-0.ch029

Rueda, F. D., Suárez, J. D., & Del Real Torres, A. (2021). Short-Term load forecasting using Encoder-Decoder WaveNet: application to the French grid. *Energies*, *14*(9), 2524. https://doi.org/10.3390/en14092524

Saeed, S., Gull, H., Aldossary, M. M., Altamimi, A. F., Alshahrani, M. S., Saqib, M., Iqbal, S. Z., & Almuhaideb, A. M. (2024). Digital transformation in energy sector: cybersecurity challenges and implications. *Information*, *15*(12), 764. https://doi.org/10.3390/info15120764

Salamai, A. (2025). A SuperHyperSoft framework for comprehensive risk assessment in energy projects. *Neutrosophic Sets and Systems*, *77*, 614–624.

Sandhu, M. A., Ameri, T. Z. A., & Wikström, K. (2019). Benchmarking the strategic roles of the project management office (PMO) when developing business ecosystems. *Benchmarking an International Journal*, *26*(2), 452–469. https://doi.org/10.1108/bij-03-2018-0058

Shakeri, M., Pasupuleti, J., Amin, N., Rokonuzzaman, M., Low, F. W., Yaw, C. T., Asim, N., Samsudin, N. A., Tiong, S. K., Hen, C. K., & Lai, C. W. (2020). An overview of the building energy management system considering the demand response programs, smart strategies and smart grid. *Energies*, *13*(13), 3299. https://doi.org/10.3390/en13133299

Shikhaliyev, R. H. (2024). Cybersecurity Risks Management of Industrial Control Systems: A Review. *Problems of Information Technology*, *15*(1), 37–43. https://doi.org/10.25045/jpit.v15.i1.05

Shoar, S., Yiu, T. W., Payan, S., & Parchamijalal, M. (2023). Modeling cost overrun in building construction projects using the interpretive structural modeling approach: a developing country perspective. *Engineering Construction & Architectural Management*, *30*(2), 365–392. https://doi.org/10.1108/ecam-08-2021-0732

Siaterlis, G., Nikolakis, N., Alexopoulos, K., & Makris, S. (2022). Adoption of AI in EU manufacturing. Gaps and challenges. In *Annals of DAAAM for . . . & proceedings of the . . . International DAAAM Symposium* (pp. 0547–0550). https://doi.org/10.2507/33rd.daaam.proceedings.077

Silvius, G. (2021). The role of the Project Management Office in Sustainable Project Management. *Procedia Computer Science*, *181*, 1066–1076. https://doi.org/10.1016/j.procs.2021.01.302

Sithambaram, J., Nasir, M. H. N. B. M., & Ahmad, R. (2021). Issues and challenges impacting the successful management of agile-hybrid projects: A grounded theory approach. *International Journal of Project Management*, *39*(5), 474–495. https://doi.org/10.1016/j.ijproman.2021.03.002

Swaminathan, N., & Danks, D. (2024). Governing ethical gaps in distributed AI development. *Deleted Journal*, *3*(1). https://doi.org/10.1007/s44206-024-00088-0

Taha, G., Sherif, A., & Badawy, M. (2022). Dynamic modeling for analyzing cost overrun risks in residential projects. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems Part a Civil Engineering*, *8*(3). https://doi.org/10.1061/ajrua6.0001262

Tharzeen, A., Natarajan, B., & Srinivasan, B. (2023). *Phasor Data Correction and Transmission System State estimation under Man-in-the-Middle attack* (pp. 1–5). 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). https://doi.org/10.1109/isgt51731.2023.10066426

Thomas, S. P., & Sohn, B. K. (2023). From Uncomfortable Squirm to Self-Discovery: A phenomenological analysis of the bracketing experience. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231191635

Triani, M. (2023). Overview of the decarbonization options for the electricity sector: opportunities and challenges. *IOP Conference Series Earth and Environmental Science*, *1248*(1), 012004. https://doi.org/10.1088/1755-1315/1248/1/012004

Ukoba, K., Olatunji, K. O., Adeoye, E., Jen, T., & Madyira, D. M. (2024). Optimizing renewable energy systems through artificial intelligence: Review and future prospects. *Energy & Environment*, *35*(7), 3833–3879. https://doi.org/10.1177/0958305x241256293

U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. (2024). *Potential benefits and risks of artificial intelligence for critical energy infrastructure*. https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

Vulpe, S., Rughiniș, R., Țurcanu, D., & Rosner, D. (2024). AI and cybersecurity: a risk society perspective. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1462250

Vyhmeister, E., & Castane, G. G. (2024). TAI-PRM: trustworthy AI—project risk management framework towards Industry 5.0. *AI And Ethics*. https://doi.org/10.1007/s43681-023-00417-y

Wallis, T., & Leszczyna, R. (2022). EE-ISAC—Practical Cybersecurity Solution for the energy sector. *Energies*, *15*(6), 2170. https://doi.org/10.3390/en15062170

Watkins, D. V., & Denney, V. P. (2023). Understanding Project stakeholder Planning, identification and Engagement: a Phenomenological approach. *Journal of Leadership Accountability and Ethics*, *20*(5). https://doi.org/10.33423/jlae.v20i5.6602

Wu, T., & Zhu, Z. (2020). The chief project officer: a new executive role for turbulent times. *Journal of Business Strategy*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/jbs-02-2020-0038

Yin, R. K. (2015). *Qualitative Research from Start to Finish, Second Edition*. Guilford Press.

Zhang, R., Zhu, Y., & Xu, S. (2020). Scheduling risk Evaluation for the Integrated Design of Blanket System Project for CFETR based on Fuzzy PRET method. *Journal of Fusion Energy*, *39*(4), 156–162. https://doi.org/10.1007/s10894-020-00246-5

Zhang, W., Pan, C., Liu, T., Zhang, J., Sookhak, M., & Xie, M. (2023). Intelligent networking for energy harvesting powered IoT systems. *ACM Transactions on Sensor Networks*, *20*(2), 1–31. https://doi.org/10.1145/3638765

Appendix A

Interview Protocol

Introduction: Hello, and thank you for agreeing to participate in this interview today. My name is Antony Amalraj, and I am a doctoral student at National University conducting my dissertation research.

This interview is expected to last 30-45 minutes. I will be recording our discussion and taking notes to make sure I have complete information. Your responses will be held in confidence.

Consent: I would like to review the consent letter with you before we begin the interview.

Do you agree to participate in the study?

Participant: Yes _____ or No_____

Lead into the Interview: Thank you. I am interested in exploring the role of PMOs in the AI adoption journey within the energy sector, and your individual answers will not be shared with anyone. Your perspectives and experiences are important to understanding the role of PMOs in mitigating cybersecurity risks in the AI adoption journey within the energy sector.

Do you have any questions before we get started?

Warm-up questions:

- Do you have any questions about this research?
- What do you enjoy most about working in the energy sector?

Complex questions:

1. How do AI-driven transformation projects impact your organization's cybersecurity risk landscape?
2. How does your organization define and implement Trustworthy AI principles, specifically focusing on security in AI adoption?

3. What cybersecurity risks have been identified in AI-driven transformation projects?
4. What risk management frameworks are used to mitigate cybersecurity risks?
5. How does your PMO ensure cybersecurity risk management is integrated into AI adoption projects?
6. How does your PMO collaborate with cybersecurity and AI teams to ensure effective integration and risk management?
7. How do you see the role of PMOs evolving as AI adoption in the energy sector continues to grow?
8. What recommendations would you give to organizations looking to strengthen PMO involvement in AI adoption and cybersecurity risk management?

Conclusion: Thank you for taking the time to meet with me today and to share your perspectives/experiences on the role of PMOs in the AI adoption journey within the energy sector.

Debriefing questions:

1. Do you have any questions or concerns?
2. Is there anything you would like to add or clarify about the role of PMOs in mitigating cybersecurity risks in the AI adoption journey?

Appendix B

Consent Form

My name is Antony Amalraj, and I am a doctoral student at National University (NU).

I'm asking you to take part in a research study about mitigating cybersecurity risks in the AI adoption journey within the energy sector. The name of this research is "The Role of PMOs in the AI Adoption Journey in the Energy Sector."

You may participate in this research if you meet all of the following criteria:

- Age 18 or older
- At least 5 years of experience in the energy sector
- Employment at a U.S.-based energy company
- Holding a role as a PMO leader, Project Manager, Program Manager, Cybersecurity Professional, AI expert, or Organizational Leader

I hope to include 15 people in this research.

Please read this form carefully and ask any questions you may have before agreeing to take part in the study.

What you will be asked to do: If you agree to be in this study, you will be asked to do the following activities:

1. Participate in a 1:1 online interview over Zoom or Microsoft Teams for 30-45 minutes.
2. Review your interview transcript via email for 10-15 minutes.

During these activities, you will be asked questions about:

- Your experience with adopting AI in transformation projects within the energy sector, including any challenges faced, cybersecurity risks encountered, and the mitigation strategies implemented.
- Role of Project Management Offices (PMO) in planning and executing transformation projects.

Risks: There are no foreseeable risks or discomforts associated with this research.

If you participate, there are no direct benefits to you. This research may increase the body of knowledge in the subject area of this research.

Recording:

I would like to audio record your responses with Zoom or Microsoft Teams during the interview. You can disable the video function of the online meeting platform at any time.

Confidentiality: I will keep the records of this study private and take reasonable measures to protect the security of all your personal information. In any report I make public, I will not include any information that will make it possible to identify you. I will securely store your data for 3 years. Then, I will delete electronic data and destroy paper data.

Taking part is voluntary: Participation in this study is completely voluntary. You may quit at any time.

If you have questions: Please ask any questions you have now. If you have questions later, you may contact me at A.Amalraj8996@o365.ncu.edu or at 248.798.3777.

If you have any questions or concerns regarding your rights as a subject in this study, you may contact the Institutional Review Board (IRB) via email at irb@nu.edu

Appendix C

Social Media Post

My name is Antony Amalraj, and I am a doctoral student at National University. I am conducting a research study to explore the role of PMOs in the AI Adoption Journey in the Energy Sector.

I am recruiting individuals who meet all of these criteria:

- Age 18 or older
- At least 5 years of experience in the energy sector
- Employment at a U.S.-based energy company
- Holding a role as a PMO leader, Project Manager, Program Manager, Cybersecurity Professional, AI expert, or Organizational Leader

If you decide to participate in this study, you will be asked to do the following activities:

3. Participate in a 1:1 online interview over Zoom or Microsoft Teams for 30-45 minutes.
4. Review your interview transcript via email for 10-15 minutes.

During these activities, you will be asked questions about:

- Your experience with adopting AI in transformation projects within the energy sector, including any challenges faced, cybersecurity risks encountered, and the mitigation strategies implemented.
- Role of Project Management Offices (PMO) in planning and executing transformation projects.

If you are interested in participating in this study, or have questions, please contact me at A.Amalraj8996@o365.ncu.edu or at 248.798.3777.

Thank you for considering participating in this voluntary research!

Antony Amalraj

RESEARCH VOLUNTEERS NEEDED

STUDY PURPOSE: THE ROLE OF PMOS IN THE AI ADOPTION JOURNEY IN THE ENERGY SECTOR

You can participate in this study if you meet all of thie following criteria:

- Age 18 or older
- Atleast five years of experience in the energy industry
- Employment at a U.S.-based energy company.
- Holding a role as a PMO leader, Project Manager, Program Manager, Cybersecurity Professional, AI expert, or Organizational Leader

In this study, participants will:

- Participate in a 1:1 online interview over Zoom or Microsoft Teams for 30-45 minutes.
- Review your interview transcript via email for 10-15 minutes.

Participants will be asked questions about:

• Your experience with adopting AI in transformation projects within the energy sector, including any challenges faced, cybersecurity risks encountered, and the mitigation strategies implemented.

• Role of Project Management Offices (PMO) in planning and executing transformation projects.

Contact Antony Amalraj, Doctoral Student at National University
248.798.3777
A.Amalraj8996@o365.ncu.edu

Appendix D

Field Test Findings and Summary

Field Test Findings and Summary Form

Researcher's Name: Antony Amalraj

Title of the Study: The Role of PMOs in the AI Adoption Journey in the Energy Sector: An Exploratory Case Study

Dissertation Chair's Name: Dr. Sharon Kimmel

Date: 5/9/2025

Instructions: Please answer all the questions below.

1a. How many experts participated in the field test?

Two experts participated in the field test.

1b. Identify each participants expertise relevant to the proposed research study topic and/or methodology.

Expert#1: This expert participant had over 30 years of experience in the energy sector, held senior roles such as Chief Information Security Officer (CISO) and Area Vice President, and possessed expertise in cybersecurity, AI, PMO, and project management.

Expert#2: This expert participant had 14 years of experience in the energy sector, held a senior role as Director of Enterprise Security PMO, and possessed expertise in PMO, cybersecurity, AI and project management.

2. Please summarize the field test findings and, if applicable, changes to the data collection instrument. If no changes were made, then indicate 'no changes.'

No changes. The experts provided feedback that the interview protocol was concise and included reasonable questions. They strongly believed that the interview guide would capture sufficient information to address the concepts being studied, and they agreed that the terminology used throughout the guide was familiar to the participants of interest.

3. For the actual dissertation study, are you revising any of the sampling/recruitment procedures and research procedures that you wrote in the Dissertation Proposal?

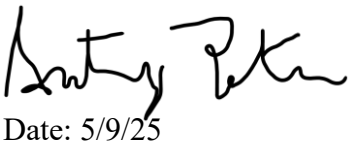
___ Yes __X__ No

(***Please answer yes or no. If you answer yes, please summarize what procedures you are changing and the rationale.***

4. What other changes (from the Dissertation Proposal proposed study plan) for the actual dissertation research study are you proposing to implement based on what you learned in the field test?

No changes.

Signature of Student Researcher:



Date: 5/9/25

Signature of the Dissertation Chair: Sharon R. Kimmel, Ph.D., ASCE

Date: 16 May 2025.

Appendix E

U.S. Department of Energy's Reports on AI and Cybersecurity

Report ID	Source	Report Name	Link
DOE-R1	U.S. Department of Energy	Advanced Research Directions on AI For Science, Energy, and Security	https://www.anl.gov/sites/www/files/2024-05/AI4SESReport-2023-v7.pdf
DOE-R2	U.S. Department of Energy	Cybersecurity Baselines for Electric Distribution Systems and DER	https://www.energy.gov/sites/default/files/2025-01/Cybersecurity%20Baselines%20for%20Electric%20Distribution%20System%20Interim%20Implementation%20Guidance.pdf
DOE-R3	U.S. Department of Energy	Potential Benefits and Risks of Artificial Intelligence for Critical Infrastructure	https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

Appendix F

National University IRB Approval Letter

Date: 5-2-2025

IRB #: IRB-FY24-25-808
Title: The Role of PMOs in the AI Adoption Journey in the Energy Sector: An Exploratory Case Study
Creation Date: 3-31-2025
End Date:
Status: Approved
Principal Investigator: Antony Amalraj
Review Board: NU IRB
Sponsor:

Study History

Submission Type Initial	Review Type Exempt	Decision Exempt

Key Study Contacts

Member Antony Amalraj	Role Principal Investigator	Contact a.amalraj8996@o365.ncu.edu
Member Antony Amalraj	Role Primary Contact	Contact a.amalraj8996@o365.ncu.edu
Member Sharon Kimmel	Role Co-Principal Investigator	Contact skimmel@nu.edu