Issues in Information Systems
Volume 26, Issue 3, pp. 484-493, 2025

DOI: https://doi.org/10.48009/3_iis_2025_139

Generative AI governance for cybersecurity: an integrated approach

John Casamassa, *Robert Morris University, jjcst32@mail.rmu.edu*
Wenli Wang, *Robert Morris University, wangw@rmu.edu*
Masialeti Masialeti, *Robert Morris University, masialetick@gmail.com*

Abstract

Generative Artificial Intelligence (GAI) is a transformative force that organizations in various industries may have to embrace to remain competitive and safe. As organizations navigate the complexities of this new digital landscape, organizations seek appropriate governance frameworks to help balance the dual imperatives of harnessing GAI-enabled innovations and safeguarding against GAI-enabled cybersecurity threats. This research discusses the benefits and risks of adaptive (Reuel and Undheim, 2024) and traditional GAI governance and recommends the traditional but integrated approach to practical GAI governance for cybersecurity, especially when the present GAI landscape is still developing. It identifies NIST AI RMF as the most suitable framework for managing risks unique to or exacerbated by GAI. It recommends COBIT 2019 for a large scope IT governance including GAI's goal alignment with organizational objectives and performance measurement for continuous improvement. It recommends NIST CSF 2.0 for its general process-based approach to address GAI-induced cybersecurity challenges.

Keywords: generative AI, artificial intelligence, IT governance, risk management, COBIT, CIST NSF, CIS AI RMF

Introduction

As artificial intelligence (AI) continues to transform various industries and sectors, its impact on productivity and safety has become increasingly significant, to the point where it is impossible for organizations to ignore this exciting and sometimes almost frightening technology. From automating tasks to enhancing medical diagnostics, AI offers unprecedented benefits, improving efficiency, accuracy, and decision-making. However, the adoption of AI technologies offers both promising benefits and formidable threats to cybersecurity, especially in information transparency and integrity. According to a 2024 study conducted by the TechTarget Enterprise Strategy Group, 70% of organizations said they prioritize data quality and integrity in their AI-driven initiatives (Gatanzano, 2024). While this heightened awareness is encouraging, a more sobering piece of insight resulting from this survey was that only 46% of organizations expressed only moderate confidence in the accuracy of data presented to end users for decision-making (Catanzano, 2024).

For the cybersecurity challenges in organizations and even the cybersecurity industry itself, AI poses a double-edged sword. On the one hand, AI can enhance cybersecurity measures by enabling more sophisticated threat detection, automating responses to incidents, and improving the overall efficiency of security operations. Machine learning algorithms can analyze vast amounts of data to identify anomalies and potential vulnerabilities, thus providing organizations with proactive defense mechanisms against

cyberattacks. However, on the other hand, AI can also be weaponized by malicious actors, resulting in heightened risks. According to a threat intelligence report published by Nokia in 2018 when AI was not as popular as present 2025, AI botnet activity was already responsible for 78% of malware detected in the networks (Sinha, 2018).

In 2018, OpenAI also issued the first version of its groundbreaking GPT (Generative Pre-trained Transformers); but then it was mostly used by professionals and researchers. In March 2023, OpenAI's GPT-4 was a much significantly improved release and it was put in the hands of laymen as well. Besides this text-based generative artificial intelligence (GAI) advancement, multimodal GAI that combines variety formats of information also improves drastically, exemplified by DALL-E in 2021, Midjourney in 2022, Vision Language Models (VLMs) such as CLIP, LLaVA in recent years and VILA-HD (Shi, et al. 2025) in 2025. Agentic AI has come to the commercial space in 2024 and 2025. For instance, autonomous customer service chatbots and even autonomous coder has been adopted by industries including banking and financial sectors. The wide applicability of these GAI tools not only enhance information diversity and multimodal insights but also enable malicious threat actors to produce highly convincing phishing emails, create deepfake content for misinformation, and develop new types of malware that evade traditional detection methods.

GAI's capabilities and speed make GAI an even sharper and swifter sword in the realm of cybersecurity. This necessitates an even more nuanced understanding of GAI's capabilities and limitations as well as their subsequent potential impacts. Organizations must navigate the complex landscape of GAI-driven threats while harnessing its potentials to strengthen their defenses.

Reuel and Undheim (2024) recommended adaptive governance for GAI. They focused on rules and regulations at society-level GAI governance and asked for an agile approach for adaptability, flexibility and fast responsiveness. They discussed the roles of government, industry, academics, civil society and citizens and recommend the activities each role can participate in. They also recognized the risks and limitations in adaptive GAI governance, such as insufficient oversight, insufficient depth, regulatory uncertainty and regulatory capture.

In comparison, our research studies the firm-level GAI governance. It not only recognizes the uniqueness of GAI such as its digital assets in datasets and AI models (parameters and metadata, etc.) and GAI's needs for cybersecurity in protecting these digital assets but also addresses how GAI enables new cybersecurity threats on traditional assets and new workflows and processes that challenge the traditional cybersecurity approaches.

To address the above issues, this research asks the following research questions (RQs):

RQ1: What are the risks and benefits of generative AI in cybersecurity?
RQ2: What IT governance framework(s) can be applied to govern generative AI in cybersecurity?

This paper is organized as follows. In the Background section, it discusses the impact of AI on information technology (IT) in general and its challenges in cybersecurity. In the Methodology section, it mentioned the design science approach for proposing integrating traditional governance frameworks at the firm level. In the Results section, it discusses GAI and cybersecurity in depth, and suggests how traditional IT governance frameworks can help assist GAI governance at the firm level. In the Discussions section, it shows the benefits of framework integration.

Background

Since the birth of AI in 1950s, "AI winters" in 1970s and 1980s, to AI's gaining traction in commercial applications in 1990s (Goff, 2023), AI has its ups and downs. The turn of the century marked a significant turning point as the advent of big data, enhanced computing power, and breakthroughs in neural networks led to a new wave of AI research, particularly in deep learning. This era witnessed the emergence of AI applications in various fields, from natural language processing to computer vision.

Today, AI is not just a tool but a transformative force across industries, influencing everything from healthcare and finance to entertainment and education. As researchers push the boundaries of what AI can achieve, the question of how to harness its potentials responsibly remains a critical focus. As AI continues to evolve, ethical considerations, such as bias, transparency, and the impact on employment, have come to the forefront of discussions about its integration into society. In addition, the continued development of AI has sparked debate about its growing impact on the world of cybersecurity, both as a tool and as a potential risk factor.

AI has had a profound effect on the modern information technology (IT) industry, reshaping how organizations operate, innovate, and deliver services. One of the most significant impacts of AI is automation, which streamlines processes and enhances efficiency. IT departments leverage AI to automate routine tasks such as software testing, system monitoring, and data management. The development of agentic AI in 2024 and 2025 even enables autonomous coding. This allows the rest of the IT departments to focus on strategic initiatives and complex problem-solving.

Additionally, AI-driven analytics tools enable businesses to extract valuable insights from vast amounts of data, enabling more informed decision-making and predictive analysis that can give companies competitive advantages they would otherwise not be able to gain. Machine learning algorithms, with supervised, unsupervised, and reinforced learning, can identify patterns and trends, facilitating anomaly detection both in internal IT operations and external hacking, which can result in enhanced operational security.

In software development, AI assists in code generation and debugging, accelerating the development lifecycle and improving code quality (Karl, 2024), which may also result in enhanced correctness and rigor in automated operations. This shift in AI-assisted software development not only reduces time-to-market but also fosters innovation, as teams can explore more creative solutions without being bogged down by mundane tasks.

Furthermore, AI enhances customer IT support through intelligent chatbots and virtual assistants, which provide immediate responses to user inquiries, improve service availability, and significantly reduce operational costs. These tools enhance customer satisfaction by delivering quick, accurate assistance, ultimately leading to increased loyalty. In cybersecurity, AI systems analyze network traffic and user behavior to detect anomalies and respond to potential threats in real-time, significantly improving an organization's defense against cyberattacks.

The integration of AI also brings challenges, such as the need for robust data governance and the ethical implications of automated decision-making. As organizations adopt AI technologies, they must address concerns related to data privacy, algorithmic bias, and the potential displacement of jobs. Despite these challenges, the benefits of AI in the IT industry are undeniable, driving transformation and paving the way for more intelligent, responsive, and efficient systems. As AI continues to evolve, it promises to further redefine the landscape of IT, fostering a culture of innovation and adaptability that will be essential for success in the digital age.

Methodology

This research takes a design science approach by examining the interactions among technology, management, controls and audits in the organizational settings. It is an interdisplinary research in technology, business and governance. It provides framework choices and examines the interoperable components.

Specifically, this research explores the cybersecurity threats posed specifically by GAI by examining specific attack vectors and tactics employed by cybercriminals, as well as the benefits that GAI brings to the cybersecurity domain. By analyzing both aspects, we aim to provide a comprehensive overview of the challenges and opportunities that GAI presents in the context of cybersecurity, highlighting the need for robust strategies and governance framework applications to mitigate risks while capitalizing on technological advancements.

Regarding governance frameworks, we will discuss the applications of COBIT (Control Objectives for Information and Related Technologies) framework from ISACA (Information Systems Audits and Control Association) as well as the cybersecurity framework (CSF) and AI risk management framework (AI RMF) from NIST (National Institute of Standards and Technology). Ultimately, a balanced approach with effective technology governance will be essential for organizations seeking to safeguard their digital assets in an era increasingly characterized by GAI-driven innovations.

Results

RQ1: What are the risks and benefits of generative AI in cybersecurity?

Generative AI (GAI) refers to a class of artificial intelligence models that can create new content based on patterns learned from existing data. This content can include text, images, music, and more. Generative AI poses significant threats to cybersecurity, primarily due to its capability to produce highly convincing and deceptive content at scale. One of the most alarming implications is the potential for creating sophisticated phishing attacks (PricewaterhouseCoopers, n.d.). Traditional phishing attempts often involve poorly crafted emails that are easily identifiable as fraudulent. However, with GAI, malicious actors can gather information from across the Internet that they can then use to generate personalized emails, pictures, and video that closely mimic the style and tone of legitimate communications, significantly increasing the likelihood of deceiving recipients (Forcepoint, 2024). These GAI-generated messages and media can incorporate specific details about the targets, making them appear authentic and tailored, which may lead individuals to divulge sensitive information or inadvertently install malware or perform other actions at the behest of the attacker. Moreover, GAI can be employed to produce counterfeit news articles or social media posts that can be used for a variety of nefarious ends including to sway political opinions or incite social unrest, thereby amplifying the risk of cyber conflicts (Miller & Eide, 2024).

In addition to all this, GAI can be used to create deepfakes—manipulated video or audio content that convincingly alters reality. Cybercriminals can utilize deepfakes to impersonate key individuals in organizations, such as executives or IT personnel, thereby facilitating unauthorized access to secure systems or sensitive data. The ability to generate realistic impersonations raises profound concerns for identity verification processes that rely on visual or auditory cues, making traditional security measures increasingly vulnerable.

Furthermore, GAI can automate and optimize cyberattacks by generating new types of malware or finding vulnerabilities in systems more efficiently than human hackers. This capability allows for rapid iterations on attack strategies, making it easier for cybercriminals and other malicious actors to discover and exploit weaknesses more quickly. GAI can also learn and adapt more rapidly to target specific endpoints or vulnerabilities (Shelton, 2023). The combination of AI's speed and creativity in generating novel attack vectors outpaces traditional cybersecurity defences, which often struggle to keep up with evolving threats. Additionally, the accessibility of GAI tools democratizes cybercrime; even individuals with limited technical skills can leverage these technologies to conduct sophisticated attacks, effectively lowering the barrier to entry for cybercriminals. This proliferation of accessible tools enhances the overall threat landscape, necessitating a re-evaluation of cybersecurity strategies.

Organizations must develop robust defence mechanisms that incorporate AI-driven analytics to detect unusual patterns and identify potential threats in real-time. Training and awareness programs for employees become crucial in combating AI-generated phishing attempts and misinformation, as human vigilance remains one of the most effective defences against cyber threats. Moreover, legal and regulatory frameworks must evolve to address the unique challenges posed by GAI, establishing accountability for misuse and creating standards for ethical AI development.

RQ2: What IT governance framework(s) can be applied to govern generative AI in cybersecurity?

Regardless of whether or not GAI is seen as a net positive in the IT world or not, the fact remains that it is a factor that must be addressed. Despite the very significant threat posed by GAI, there are methods that organizations can employ such as multi-factor authentication, regular software updates, and strict access controls that will help to mitigate the risks posed by GAI (F5, 2024). Security governance strategies and techniques are essential in providing a cohesive framework to an organization’s security system that help to maximize security without sacrificing efficiency in day-to-day operations.

Although the adaptive AI governance approach suggested by Reuel and Undheim (2024) is promising, organizations need to still work within their familiar territory and build upon their existing governance frameworks to address GAI related concerns. Pioneering in new IT governance framework or drastic change in framework adoption will provide additional risks and burdens to GAI adoption, which alone is already a daunting task. The lack of technical expertise and managerial understanding of AI in fast-changing GAI landscape and its advancements also challenges innovated governance. We recommend take the traditional approach with careful add-on discretions for the general medium- and big-sized firms, especially when GAI technology is still fledging and not fully-developed with maturity yet.

Applying COBIT framework for GAI

One popular governance framework currently in use is the COBIT (Control Objectives for Information and Related Technologies) governance framework. Developed by ISACA (Information Systems Audits and Control Association), COBIT provides a structured approach that helps organizations align their IT goals with business objectives while managing risks and optimizing resources. The framework encompasses a set of best practices, tools, and resources to help organizations achieve effective governance and control over their IT assets. COBIT is designed to assist companies in developing their own strategies that fit with an organization’s overall goals, by focusing on the components rather than a one-size-fits-all model (CyberTalents, n.d.). Olorunojowon (2017) demonstrated how COBIT 5 goals cascade, translating stakeholder needs into specific actionable goals at various levels and facilitating alignment and integration of business and IT strategy. Olorunojowon (2017) also discussed how COBIT 5 provided enabling

processes and activities required for goal attainment and how the balanced scorecards could be applied to ensure that metrics at all levels track the achievement of actionable goals.

COBIT is a governance system and a framework that includes components such as governance and management objectives, performance management, and capability assessments. Its flexibility allows organizations of all sizes and industries to tailor it to their specific needs. By focusing on stakeholder needs and establishing a clear decision-making structure, COBIT promotes a holistic approach to IT governance that includes risk management, compliance, and performance optimization. This makes it an invaluable tool for organizations looking to navigate the complexities of modern IT environments, including the challenges posed by emerging technologies like GAI. COBIT 2019 is the most recent iteration after COBIT 5, a version in 2012. COBIT 2019 was designed to address then contemporary IT practices like DevOps and agile systems analysis and design (Ergul, 2024).

In the context of securing organizations against the cybersecurity risks associated with GAI, COBIT offers several valuable mechanisms. First, COBIT emphasizes the importance of risk management, which is critical when addressing the potential threats posed by GAI technologies, such as sophisticated phishing attacks, deepfakes, and automated cyberattacks. By utilizing COBIT's risk management practices, organizations can systematically identify, assess, and mitigate risks related to the use of GAI, ensuring that appropriate safeguards are in place. Polat (2024) stated that COBIT's robust risk management processes can be adapted to AI, addressing potential risks like data privacy, security, and algorithmic bias, and ensuring these technologies are developed responsibly.

Additionally, COBIT's governance objectives encourage organizations to establish clear policies and procedures for the ethical use of GAI technologies. This includes implementing guidelines on GAI content generation, monitoring for misuse, and promoting awareness and training among employees to recognize GAI-generated threats.

Furthermore, COBIT's emphasis on performance measurement can help organizations monitor the effectiveness of governance in AI. Establishing metrics for AI, such as its accuracy and fairness, allows for the objective tracking of progress and areas for improvement. In the area of cybersecurity, COBIT's focus on performance measurement is vital for organizations aiming to secure their IT environments against GAI-related threats. By establishing key performance indicators (KPIs) and metrics related to cybersecurity, organizations can evaluate the effectiveness of their security measures and governance practices. This ongoing assessment enables organizations to identify areas for improvement and make data-driven decisions to enhance their defences. For instance, if an organization notices a rise in successful phishing attempts, it can analyse its training programs and modify them to better equip employees to recognize and respond to these threats. Another example is that an organization might track month over month how many IT processes were flagged as being AI generated from an illegitimate source. In doing so, management would be given a much clearer picture of which processes were most effective over time. By regularly assessing the performance of security controls and adjusting them based on metrics and outcomes, organizations can remain agile and responsive to evolving threats.

Continuous improvement is a cornerstone of effective cybersecurity, and COBIT's structured framework supports this process by encouraging regular reviews and updates to security policies and practices. Overall, by integrating COBIT's structured approach to governance and risk management with their cybersecurity strategies, organizations can better safeguard against the complex and dynamic risks associated with generative AI technologies, thereby enhancing their overall resilience in an increasingly digital landscape. Overall, COBIT 2019 is a general but robust governance framework applicable to GAI. COBIT's structured approach to IT governance and risk management equips organizations with the tools necessary to establish

clear policies, monitor performance, and implement effective controls tailored to the specific risks associated with GAI. By leveraging COBIT's governance objectives, organizations can foster an ethical environment for GAI usage, ensuring compliance with legal standards while promoting accountability and transparency. Additionally, COBIT's focus on continuous improvement encourages organizations to adapt their strategies as GAI technologies evolve. This proactive stance is essential for mitigating risks and enhancing overall cybersecurity posture. Ultimately, the integration of the COBIT framework into an organization's governance practices not only helps manage the inherent risks of GAI but also supports the responsible and innovative deployment of these emerging technologies.

Applying NIST frameworks for GAI

The National Institute of Standards and Technology (NIST)'s Cybersecurity Framework (CSF) is another governance toolset to help mitigate risks posed by AI. NIST CSF 2.0 is the most recent framework (NIST, 2024a). As AI is becoming increasingly integrated into business and societal functions, the NIST CSF framework offers its own structured approach to managing these risks, ensuring that AI technologies are developed and deployed responsibly.

The NIST CSF framework is built around five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2024a). These functions assist organizations in forming a very structured system for combatting the potential security threats posed by GAI, which include, but not limited to, misinformation, bias, data security breaches, adversarial attacks and so on. The following list provides some exemplary explanations of NIST CSF five core functions in their applications for AI/GAI:

NIST's "Identify" function helps organizations understand their AI assets (e.g., datasets, AI models, intellectual property, model parameters and metadata, etc.) and how these assets integrate with organizational processes and interact with organizational stakeholders like human resources and clients. Risks related to these AI assets are also identified and prioritized. potential biases in datasets and implement fairness measures.

NIST's "Protect" function secures AI assets and proactively reduces risks to them. It emphasizes encryption, anonymization, and access controls to prevent unauthorized data use, AI model use and protect data privacy and information integrity. This is essential for GAI as GAI models typically rely on large datasets, including those containing sensitive information that requires strong access control. If the datasets are not only from within the organization, the fair and legal use of the datasets should also be protected.

NIST's "Detect" function allows for timely detection of anomalies related to AI assets and processes. For GAI, it needs to not only detect technical incidents resulting in lowered performance or unavailability of AI models but also detect biases in datasets, unfairness in prediction, inauthenticity in information outputs, and unethical practices related to AI.

NIST's "Respond" function manages, analyses and mitigates AI incidents and aims for containing and minimizing the impact of the adverse incidents. For instance, if an AI or GAI model was built upon a highly biased datasets and hence produced inaccurate predications unsuitable to new cases, the model could even be taken offline. Organizations need to report and communicate their actions to the related parties and even the public.

NIST's "Restore" function ensures corrective measures are in place before restoring incident-impacted AI assets and operations. For instance, in case data were biased, privacy was violated, or AI model was not

properly used, etc., the data should be ensured to be unbiased, privacy to be protected and AI models redesigned or retrained for proper use.

The above five NIST CSF functions are related and built upon precedents. NIST further elaborated on its "Identify" function in AI. In January 2023, NIST released a new framework specifically designed for AI risk management. The NIST AI RMU (AI Risk Management Framework) provides guidelines for managing AI-related risks by emphasizing "risks unique to or exacerbated by GAI" and their subsequent governance challenges (NIST, 2024b). For instance, it categorizes AI risks under hateful content, harmful bias or homogenization, data privacy, intellectual property, human-AI configuration, and even environmental impact, etc. (NIST, 2024b). The framework offers action IDs and actor tasks under subcategorized governance and managerial needs and aims for security, trust, fairness, transparency with information integrity and model clarity, suggesting detailed controls to mitigate threats like GAI-generated misinformation, data poisoning, and deepfakes misuse (NIST, 2024b).

Discussion

COBIT and NIST framework comparison

Organizations need to weigh the pros and cons of different governance frameworks according to their specific needs. Both COBIT and NIST frameworks provide benefits and value to organizations based upon their differing focuses.

As an IT governance framework, COBIT focuses on aligning IT with business objectives as well as providing a structured approach for managing enterprise IT risks, compliance, and performance through a set of governance principles and controls. In contrast, NIST is primarily a cybersecurity and risk management framework, offering detailed guidelines for securing IT environments, including AI/GAI-driven systems, and thus the framework's focus is more on technical security measures.

COBIT follows a governance-driven approach to risk management, emphasizing accountability, decision-making structures, and performance monitoring (Ergul, 2024). It provides a risk-based framework that aligns with business goals, ensuring that AI technologies, including GAI, are deployed responsibly. COBIT's principles guide organizations in assessing AI risks from a regulatory and operational perspective, ensuring that AI investments align with corporate risk appetite. NIST, on the other hand, follows a more structured cybersecurity risk management approach.

Naskar (2024) provided a general comparison of the respective advantages and disadvantages between the two frameworks of COBIT and NIST CSF. Naskar (2024) identified that one key difference between the two frameworks is their scope: NIST CSF primarily focuses on cybersecurity risk, while COBIT covers a broader range of IT governance areas, including risk management, strategic planning, and resource management. Additionally, the level of detail and complexity also differs between NIST CSF and COBIT: NIST CSF provides a high-level framework that organizations can adapt to their unique requirements, while COBIT offers a more detailed framework with specific control objectives and processes (Naskar, 2024). This difference may affect the feasibility and implementation efforts for organizations with varying resources and capabilities (Naskar, 2024).

In general terms, the NIST CSF 2.0 framework appears to be the more adaptable option that focuses more on the specific cybersecurity measures necessary to combat threats especially with its process-based approach, while COBIT 2019 would probably be more desirable for an organization that needs to address the AI challenge with a greater focus on overall governance of the organization. NIST AI RMF framework

initially released in January 2023 provides the most recent and comprehensive risk management framework for AI to date. Since it addresses the specifics of GAI technologies and risks in depth, we highly recommend to apply NIST AI RMF for GAI risk management. In addition, we recommend COBIT 2019 to serve as an overall organizational governance framework applicable to GAI and NIST CSF 2.0 to serve as a general process-based governance framework for addressing cybersecurity issues, including safeguarding against new threats created by GAI. Our suggestion of integration of IT governance frameworks echoes with World Economic Forum and Accenture's suggested 360 approach for resilience and regulation when governing in the age of GAI (Lazerson, Siddiqui & Amezaga, 2024).

Conclusion

As GAI continues to advance, the intersection of GAI and cybersecurity will require ongoing research, innovation, and collaboration among stakeholders to safeguard against the multifaceted risks that these technologies present. Ultimately, while GAI holds immense potential for positive applications, its misuse in the realm of cybersecurity presents an urgent challenge that demands comprehensive and proactive measures to protect individuals, organizations, and society at large from emerging threats.

Given that GAI is becoming ever more integrated into everyday life and every organization across industries, governance frameworks must be designed and regularly updated in order to manage and mitigate potential risks while still allowing for the maximization of GAI's transformative and innovative potential (Wong et al., 2024). To effectively manage these challenges while capitalizing on the benefits, organizations can still turn to the traditional IT governance frameworks as robust and practical governance solutions. As organizations navigate the complexities of this new digital GAI landscape, adopting a comprehensive, well-tested, governance framework like COBIT 2019, NIST CSF 2.0, and NISF AI RMF will be critical in balancing GAI's dual imperatives of harnessing innovation and safeguarding against potential threats. This traditional approach is practical for firms when the GAI landscape is still under development and serves as a stepping stone to the truly adaptive GAI governance in the near future.

References

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review. International Journal of Advanced Research in Computer and Communication Engineering, 11(9), 81-90. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317

Belani, G. (2024, April 1). The strategic role of AI in governance, risk and compliance (GRC). Security Boulevard. https://securityboulevard.com/2024/04/the-strategic-role-of-ai-in-governance-risk-and-compliance-grc/

Catanzano, S. (2024). Generative AI shines spotlight on data governance and trust. Data Management; TechTarget. https://www.techtarget.com/searchdatamanagement/opinion/Generative-AI-shines-spotlight-on-data-governance-and-trust

CyberTalents. (n.d.). Understanding COBIT framework: Definition, components, and benefits. CyberTalents Blog. https://cybertalents.com/blog/understanding-cobit-framework-definition-components-and-benefits

Ergul, O. (2024, August). NIST vs. COBIT: Comparison of cyber security frameworks. Tecnovy. https://tecnovy.com/en/nist-vs-cobit

F5. (2024). Generative AI: Application security and optimization. F5. https://www.f5.com/glossary/generative-ai-security

Forcepoint. (2024, January 5). Data in hot water: the cybersecurity risks of generative AI. Forcepoint. https://www.forcepoint.com/blog/insights/data-cybersecurity-risks-generative-ai

Goff, M. (2023, October 5). A very brief history of artificial intelligence. Freshfields. https://technologyquotient.freshfields.com/post/102ip8m/a-very-brief-history-of-artificial-intelligence

Karl, T. (2024, June 30). Top benefits of AI in modern software development. New Horizons. https://www.newhorizons.com/resources/blog/benefits-of-ai-in-software-development

Lazerson, R., Siddiqui, M., & Amezaga, K. Y. (2024). Governance in the age of generative AI: A 360º approach for resilient policy and regulation. White paper, World Economic Forum and Accenture. https://www.weforum.org/publications/governance-in-the-age-of-generative-ai/

Miller, J. A., & Eide, N. (2024, May 8). Generative AI is a looming cybersecurity threat. Cybersecurity Dive. https://www.cybersecuritydive.com/news/generative-ai-artificial-intelligence-cyber-threat/715531/

Naskar, S. (2024, April 6). Navigating frameworks: A comparative analysis of NIST CSF and COBIT. GRC-Docs. https://grc-docs.com/blogs/nist-csf/navigating-frameworks-a-comparative-analysis-of-nist-csf-and-cobit#:~:text=NIST%20CSF%20primarily%20focuses%20on,more%20suitable%20than%20the%20other

NIST. (2024a). The NIST cybersecurity framework (CSF) 2.0. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

NIST. (2024b). The NIST artificial intelligence risk management framework: Generative artificial intelligence profile. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

Olorunojowon,O. Z. (2017, December 12). Drive transparent and measurable value with COBIT 5 process metrics. https://www.isaca.org/resources/news-and-trends/industry-news/2017/drive-transparent-and-measurable-value-with-cobit-5-process-metrics

Polat, G. (2024, May 2). Unlocking AI's potential: How COBIT can guide your business transformation. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/unlocking-ais-potential-how-cobit-can-guide-your-business-transformation

PricewaterhouseCoopers. (n.d.). Managing the risks of generative AI. PricewaterhouseCoopers. https://www.pwc.com/us/en/tech-effect/ai-analytics/managing-generative-ai-risks.html

Reuel, A., Undheim, T. A. (2024). Generative AI Needs Adaptive Governance. https://arxiv.org/abs/2406.04554

Shelton, A. (2023, October 30). A double-edged sword: Understanding AI in cybersecurity. Skinner Technology Group. https://skinnertechgroup.com/a-double-edged-sword-understanding-ai-in-cybersecurity/

Shi, B.F., Li, B., Cai, H., Lu, Y., Liu, S.F., Pavone, M., Kautz, J., Han, S., Darrell, T., Molchanov, P., Yin, H.X. (2025). Scaling Vision Pre-Training to 4K Resolution. Nvidia. https://arxiv.org/pdf/2503.19903v1

Sinha, J. (2018, December 20). 5 Artificial Intelligence-based attacks that shocked the world in 2018. AIM. https://analyticsindiamag.com/ai-origins-evolution/5-artificial-intelligence-based-attacks-that-shocked-the-world-in-2018/

Spencer, P. (2023, December 18). AI for the good and bad in cybersecurity. Kiteworks. https://www.kiteworks.com/cybersecurity-risk-management/ai-for-the-good-and-bad-in-cybersecurity/

Wiggers, K. (2021, April 8). Survey finds 96% of execs are considering adopting 'defensive AI' against cyberattacks. VentureBeat. https://venturebeat.com/business/survey-finds-96-of-execs-are-adopting-offensive-ai-against-cyberattacks/

Wong, H., Chang, A., & Pugh, B. (2024, May 21). Advancing AI security through strategic governance. R Street. https://www.rstreet.org/commentary/advancing-ai-security-through-strategic-governance/