International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 7 ||Issue|| 6 ||Pages 204-214 ||2025||

Harnessing the Digital Prometheus: A Strategic Framework for Generative AI Governance, Risk, and Control.

[1,]Adetunji Oludele Adebayo, [2,]Omowunmi Folashayo Makinde, [3,]Olatunde Ayomide Olasehan, [4,]Nathaniel Adeniyi Akande, [5,]Uju Judith Eziokwu

[1]*Information Security Manager /Independent researcher, University of Bradford, UK*
[2]*IT Support Engineer I/Independent Researcher, University of the Cumberlands, USA*
[3]*IT Engineer/Independent Researcher, Swansea University, UK*
[4]*Cyberscurity Analyst/Independent Researcher, University of Bradford, UK*
[5]*Data Analyst/Independent Researcher, University of Bradford, UK*

ABSTRACT: Generative Artificial Intelligence (GenAI) represents a transformative shift in computing that alters the relationship between human creativity and machine capability. Unlike traditional AI systems for classification or pattern recognition, GenAI creates new content across modalities, producing human-like text, images, audio, and code. This paper explores a strategic "Architecture of Control" to manage GenAI risks while balancing innovation and responsibility. The rapid adoption of GenAI across industries demonstrates its potential as a general-purpose technology, from healthcare and finance to education. However, this integration introduces risks, including privacy breaches, cybersecurity threats, and ethical challenges like algorithmic bias and intellectual property disputes. The proposed Governance, Risk, and Compliance (GRC) framework addresses these challenges through responsible adoption, ensuring organizations can leverage GenAI's benefits while mitigating risks. The framework aligns with global regulatory standards and establishes a governance model integrating strategic oversight, operational accountability, and technical safeguards. The effectiveness depends on balancing strong controls with innovation flexibility. The widespread adoption of GenAI requires strategic adaptations across organizations, affecting workforce reskilling and governance agility. Successful integration will depend on robust governance frameworks that enable organizations to harness its potential while ensuring accountability and safeguards.

I. INTRODUCTION

Generative artificial intelligence (GenAI) represents a system shift in computing that fundamentally alters how we understand the relationship between human creativity and machine capability (Dwivedi et al., 2021). Unlike traditional AI systems designed for classification, prediction, or pattern recognition, generative AI creates entirely new content across multiple modalities producing human-like text, photorealistic images, synthesized audio, and functional code (Treude & Storey, 2025). This transformation from AI as an analytical tool to AI as a creative partner marks one of the most significant technological developments since the advent of the internet (Aldoseri et al., 2024) Generative AI (GenAI) has its roots in early neural network and machine learning research from the 2010s, but it gained significant momentum with the advent of deep learning techniques (Raghvendra et al., 2024). The foundation of this transformation lies in the breakthrough of transformer architectures, introduced by (Vaswani et al. 2017), which marked a methodology shift in how models process and generate language. These neural architectures made way for the development of powerful large language models (LLMs) such as GPT (Generative Pre-trained Transformer) (Brown et al., 2020), BERT (Bidirectional Encoder Representations from Transformers) (Devlin et al., 2018), and PaLM (Pathways Language Model) (Chowdhery et al., 2022). Collectively, these models demonstrate unprecedented capabilities in understanding context, generating coherent text, and performing complex reasoning tasks (Ciubotaru, 2025; Yenduri et al., 2023). Generative AI adoption like ChatGPT for commercial use reached 100 million users in two months of its launch, this has been nothing but extraordinary (Milmo, 2023) This sets a record for the largest and fastest consumer application in history. Businesses have started adopting different generative AI in their business as it offers startups opportunities for innovations, efficiency and digital transformation (Gupta, 2024).

II. LITERATURE REVIEW

The central research question guiding this paper is: How can a strategic, multi-layered "Architecture of Control" be developed to manage the risks of GenAI while balancing innovation and responsibility? This question arises from the dual character of generative AI. On one hand, GenAI promises massive economic and societal benefits, from trillions of dollars in value creation to measurable productivity gains across industries such as healthcare, finance, and education. On the other hand, it introduces significant risks, including bias, misinformation, intellectual property disputes, labor market disruption, and the concentration of power in a small number of technology providers. Without clear mechanisms for governance, these risks threaten to undermine trust and limit the long-term sustainability of GenAI adoption. Addressing this gap requires more than a single policy or organisational measure. Because GenAI operates across borders and sectors, it demands a multi-layered approach that integrates enterprise practices, industry standards, national regulations, and global coordination. This research question therefore, frames the paper's objective: to explore how such an Architecture of Control can be structured to preserve innovation while establishing accountability, transparency, and safeguards against harm.

Foundational Concepts and Macro-Economic Analysis : GenAi is a type of artificial intelligence that focuses on creating different types of content, text, images, code or audio that is linked to the ways or patterns from the data it was trained on. Unlike conventional traditional AI, which is created to classify or predict or recognize patterns. Gen AI models generate new outputs that often mimic human creativity. (Narapareddy, 2025) Generative AI encompasses a range of machine learning technologies, including transformers, GANs (Generative Adversarial Networks), and diffusion models. These tools enable machines to generate new content, marking a shift from deterministic automation to creative co-pilots (Bengesi et al., 2024). GenAI is now recognized as a general-purpose technology (GPT), like electricity or the internet in its transformative potential (Vukmirović & Kresović, 2024).GenAI has evolved from early neural network models through deep learning techniques such as CNNs(Convolutional neural networks) and RNNS (Recurrent neural networks), towards advanced architectures like transformers and diffusion models, latest innovations like Hinton's forward-algorithm, Meta I-Jepa Model, Federated learning for privacy and the integration of reasoning agents illustrate the significant advances shaping the next frontier of generative AI (Parasuraman, 2024)

Macro-Economic Impact OF GEN AI : McKinsey and Company argues that Gen AI has a huge economic impact as it could add $2.6 to $4.4 trillion annually to the global economy, boosting overall value contributions by 15-40% if embedded into existing software (Chui et al., 2023). They also argue that about 75% of GenAI potential comes from customer operations, marketing and sales, software engineering, research and development. The total economic benefits from border applications across knowledge workers' tasks may reach $6.1 trillion to $ 7.9 trillion annually. (Brühl, 2024) also argues that GenAI technology's underpinnings in machine learning and transformer-based models, before turning to the rapidly evolving competitive landscape in which United States (US) Big Tech companies such as Microsoft, Google and Meta dominate, with only a handful of European actors like Aleph Alpha or Stability AI present. (Brühl, 2024) highlights the breadth of generative AI's possible applications, ranging from text and code generation to image, video and even 3D or virtual reality use cases, covering virtually all stages of the value chain. He highlights that generative AI can deliver measurable productivity gains for example in knowledge-intensive writing tasks while also warning that the economic and strategic challenge for Europe lies in avoiding technological dependency on non-European platforms. A central part of the analysis concerns the forthcoming EU Artificial Intelligence Act, which Brühl mentions as a crucial regulatory development intended to balance innovation with safeguards on risk, transparency and accountability Illustrating that AI is not only in terms of efficiency improvements but also in relation to Europe's position in global digital competition and the need for a regulatory environment that enables adoption while mitigating concentration and inequality.

(Merali & Merali, 2023) complement this global perspective by emphasising the potential macroeconomic shocks generative AI may trigger, particularly for advanced service-oriented economies like the UK. While they underline its power to restore productivity growth after years of stagnation, they caution that AI-driven cost reductions could place downward pressure on inflation, mirroring the disinflationary effects of China's integration into the global economy in the 1990s. At the same time, the labour market effects may be profound, large segments of white-collar employment, especially in legal, professional, and creative services, are exposed to partial or full automation. This disruption could produce short-term unemployment, slower re-employment, and long-term scarring effects, with higher-wage workers counterintuitively among the most at risk. Looking ahead, they argue that the macroeconomic environment may need to contend with both short-term deflationary dynamics and, if artificial general intelligence emerges, a scenario of explosive growth requiring much higher long-term interest rates. The macroeconomic potential of generative AI also stems from the underlying advances in large language models, first demonstrated at scale by (Brown et al., 2020) who introduced GPT-3 as a few-shot learner. Their work showed that a single general-purpose model, trained on massive datasets, could perform a wide variety of tasks with little or no task-specific training. This breakthrough fundamentally lowered the marginal cost of applying

AI across domains, enabling rapid diffusion into business, public services, and everyday life Taken together, these perspectives show that generative AI is both a driver of extraordinary productivity gains and a source of economic volatility, with implications for inflation, employment, and competitiveness. The macroeconomic impact will ultimately depend on the speed of diffusion, the balance between augmentation and displacement in labour markets, and the effectiveness of regulatory and policy responses that aim to secure widespread benefits while mitigating risks.

Applications Across Industries : The widespread adoption of Gen AI reinforces its role as a general-purpose technology with broad and transformative applications in different industries. In healthcare, GenAI models are being deployed for clinical documentation, automated summarization of patient notes, and synthesis of research findings across large medical studies (Sallam, 2023). They also support drug discovery, where generative models advance molecule design and protein structure prediction, significantly reducing research and development timelines (Yu et al., 2023). Also, patient-facing applications such as chatbots provide accessible health information and improve communication in resource-constrained contexts (Chow et al., 2024). In finance, banks and insurers are integrating GenAI into fraud detection systems, algorithmic trading, and automated customer support (FSB, 2024). These applications not only increase operational efficiency but also enhance risk management by detecting anomalies and potential compliance issues in real time. At the strategic level, financial firms use GenAI for market analysis and forecasting, enabling more responsive decision-making in volatile markets (Brühl, 2024). The creative industries including advertising, film, and digital art have embraced generative tools to augment content creation. Models like Stable Diffusion (Rombach et al., 2022) and MidJourney allow designers and marketers to produce high-quality images, videos, and campaign material at unprecedented speed. Musicians and writers use LLMs and multimodal models for lyrics, scripts, and audio synthesis, reshaping workflows in entertainment and publishing (Ciubotaru, 2025b)

In education, GenAI enables personalized tutoring systems, adaptive assessments, and curriculum generation. For example, (Chu et al., 2025) show that LLM-powered tutoring systems can explain complex topics in multiple ways, providing differentiated support to learners with diverse needs. At the same time, institutions are experimenting with automated grading and curriculum design, reducing faculty workloads while raising questions about academic integrity.In software engineering, developers increasingly rely on LLM-powered assistants such as GitHub Copilot and OpenAI Codex to generate boilerplate code, debug errors, and produce documentation (Chen et al., 2021). Studies suggest that these tools can improve developer productivity by up to 50%, freeing engineers to focus on higher-level problem-solving (Gupta, 2024b). Enterprises and small businesses are also leveraging generative models to modernize legacy systems and accelerate digital transformation. Taken together, these applications highlight GenAI's transformative potential across industries. By enhancing productivity, creativity, and decision-making, GenAI is reshaping workflows and business models globally. At the same time, its rapid diffusion raises challenges of governance, bias mitigation, and ethical adoption, reinforcing the need for robust frameworks that balance innovation with accountability.

Governance, Risk, and Control: Towards an Architecture of Control : The rapid diffusion of Generative AI underscores the need for a structured governance approach that can both harness innovation and mitigate risk. A strategic, multi-layered architecture of control can be envisioned as a system operating across four interdependent levels:

1. Enterprise-Level Controls: Organizations must implement internal safeguards such as bias testing, model audits, explainability tools, and transparency reporting. These mechanisms ensure accountability for how models are trained, deployed, and monitored.
2. Industry-Level Standards: Sector-specific frameworks (e.g., healthcare compliance for medical AI, financial regulations for algorithmic trading) provide tailored safeguards. Professional associations and technical bodies (like ISO or IEEE) can define best practices for safety, reliability, and fairness.
3. National Regulation: Governments provide legal oversight through legislation such as the EU AI Act or the NIST AI Risk Management Framework in the U.S. National-level policies establish enforceable rules for high-risk use cases, transparency obligations, and liability.
4. Global Coordination: Since AI systems transcend borders, international principles (e.g., OECD AI Guidelines, UN initiatives) are critical to harmonize standards, prevent regulatory arbitrage, and address global challenges like disinformation or concentration of power.

This layered design reflects the reality that no single control point is sufficient. Enterprise measures prevent misuse at the point of development, industry standards promote sectoral trust, national laws provide enforceability, and global frameworks ensure alignment across jurisdictions.

Ultimately, the effectiveness of this architecture depends on balance: strong enough to safeguard against risks such as bias, misuse, and economic disruption, but flexible enough to preserve innovation and unlock the transformative potential of GenAI.

III. METHODOLOGY

This study develops a Governance, Risk, and Compliance (GRC) framework for Generative Artificial Intelligence (GenAI). The methodology focuses on constructing a comprehensive "Architecture of Control" designed to guide organisations in the responsible and secure adoption of GenAI technologies. The approach synthesises information from leading global regulatory standards, extensive industry analysis, and documented real-world security incidents. By integrating these diverse sources, the methodology establishes a multi-layered control system that addresses the technical, procedural, and strategic challenges of Genai. This process ensures the resulting framework is not only theoretically sound but also practically applicable to the complex operational environments of modern enterprises.

Research Design : The research design focuses on developing a strategic GRC framework. This "Architecture of Control" offers a structured approach for managing GenAI by integrating four key components. First, it builds on global regulatory pillars, specifically the National Institute of Standards and Technology (NIST) AI Risk Management Framework and the European Union's AI Act (European Union, 2024; NIST, 2023). Second, it establishes a formal corporate governance structure, clearly defining roles and responsibilities from the executive board to development teams. Third, it details essential procedural safeguards, such as data governance protocols and human-in-the-loop oversight. Finally, it includes technical protections by explaining the use of Privacy-Enhancing Technologies (PETs) like Differential Privacy and Federated Learning.

Data Collection : To develop a relevant and robust framework, this study draws upon a broad range of authoritative sources. Data collection involved reviewing foundational regulatory and guidance documents, including the NIST AI Risk Management Framework and the EU AI Act, which form the compliance backbone of the proposed architecture (European Union, 2024; NIST, 2023). The study also incorporates macroeconomic and industry-specific analyses from leading institutions such as McKinsey & Company and Goldman Sachs to contextualise the technology's impact (McKinsey & Company, 2025). Furthermore, the research gathers real-world examples of GenAI risks, security vulnerabilities, and use cases from technical reports and cybersecurity analyses to ensure the framework's controls address current and emerging threats.

Data Analysis : The analysis concentrates on identifying and categorising the main risks linked to GenAI to guide the development of targeted controls. The study systematically considers risks across three key areas: data privacy, cybersecurity, and ethics. For data privacy, it evaluates vulnerabilities such as training data leakage and unauthorised data exposure through user prompts. In cybersecurity, the analysis explores the weaponisation of GenAI for creating advanced phishing attacks, deepfake fraud, and polymorphic malware. The ethical review addresses issues like algorithmic bias, the spread of misinformation, and infringement of intellectual property. The results from this thorough risk assessment directly inform the procedural and technical controls recommended within the GRC framework, ensuring each safeguard aligns with a specifically identified vulnerability.

IV. DATA PRIVACY RISKS AND MITIGATION

Training Data Analysis : Generative AI (GenAI) models find their functionality in generating content, such as text, images, videos, audio, and computer code. GenAI combines algorithms, deep learning, and a neural network approach in analyzing large datasets and learns from the vast amount of patterns in the datasets to emulate the structure to replicate a wide array of historical content (Low et al., 2025). The GenAI models incorporate information from datasets and 'learn' the patterns of words within a given context, and when queried, they predict the most likely combination of words, and then generate a natural-language response to the user’s prompt (Smith, 2024). These texts are memorized and stored by the AI model and can be regurgitated verbatim in response to a user query or prompt, which raises concerns about intellectual property rights violations. GenAI models can inadvertently memorize and leak sensitive information from their training datasets, and with the large amounts of data used to train these models, which sometimes include personal or confidential information, the models can enhance the risk of privacy violations (Hu et al., 2024).To mitigate the data leakage, differential privacy techniques must be employed during training, data minimization, and anonymization. Additionally, to enhance traceability and allow organizations to detect and limit unintentional disclosure, regular auditing and watermarking the generated outputs of GenAI should be enforced.

Shadow AI and User Behaviour Analysis : There are significant data privacy risks when employees provide organization-sensitive data when using public GenAI tools without organizational oversight. The unrestricted approach of unguarded use of GenAI tools by employees can expose organizations to data risks (Powar & Beresford, 2023). Unknowingly to many employees, sensitive information is shared while interacting with these tools, creating vulnerabilities that can be exploited by malicious actors. Because many interactions occur through personal accounts, organizations lose visibility and control over data flows, increasing the likelihood of non-compliance with data protection regimes such as NDPR, GDPR and CCPA (Babalola, 2022). Employees must undergo regular training in the safe use of data and the risks associated with exposing proprietary or personal information when interacting with external tools.

Adversarial Techniques and Extraction Risks : Beyond accidental exposure, malicious actors may deliberately exploit GenAI models to extract sensitive information. One technique employed is the prompt injection, where the input prompts to the Gen AI are manipulated to elicit unintended responses (Liu et al., 2024). This approach can easily bypass security measures, leading to unauthorized data access. Another technique is the Model inversion attacks, where sensitive training data are reconstructed and exploited by the adversaries to retrieve confidential information (Aditya et al., 2024). The API-probing attacks are another attack technique employed by adversaries to query trained data and internal mechanisms for the purpose of revealing sensitive information (Huang et al., 2024).

V. SECURITY AND ETHICAL RISK ANALYSIS

Cybersecurity Threats : The GenAI advancement has enabled adversaries to also create hyper-realistic phishing, deepfakes, and evasive malware, making these attacks difficult to recognize. For instance, the adversaries can utilize generative media tools to develop deepfakes for audio and video impersonation. Reports have also shown that GenAI attackers can develop polymorphic code to bypass signature-based detection systems (Sahin, 2024). All these scenarios demonstrate the risks posed by GenAI and the urgency required to integrate these risk scenarios into organizational cybersecurity strategies.

Ethical Risks : The deployment of GenAI raises ethical concerns, and the negative impacts created pose significant challenges, thereby preventing fair and inclusive outcomes in decision-making processes (Shin, 2024). Additionally, the use of GenAI also raises questions about the right ownership of created content, making it difficult to address intellectual property (Vasa, 2024). Defining what makes GenAI “ethical” extends beyond compliance as it involves proactive identification and mitigation of risks such as social harm, legal violations, reputational loss, and technical failure throughout the full AI lifecycle, that is, from data acquisition and modeling to deployment and monitoring.

Societal Implications : While GenAI promises productivity gains, there are also risks associated with workforce Job displacement, hence the urgent need for workforce reskilling to remain relevant. With the rapid adoption of GenAI technologies, its implications on employment and the need for employees to develop necessary skills to thrive in an AI-driven economy can not be overemphasized (Mishra, 2024). With AI systems becoming increasingly sophisticated and integrated into critical aspects of society, the governance structures must also be committed to, without compromising ethical and legal standards (Lacsa, 2024). Therefore, creating a culture of responsibility in organizations involves continuous training for employees, promoting ethical awareness, and embedding governance in performance metrics, which are essential as ongoing education promotes ethical awareness among employees and embeds governance into organizational culture.

VI. FRAMEWORK DEVELOPMENT AND EVALUATION

Development of a Governance Model : The proposed governance model establishes a comprehensive blueprint for corporate AI governance that integrates strategic oversight, operational accountability, and technical safeguards. This multi-layered architecture addresses the unique challenges posed by GenAI while enabling organizations to harness its transformative potential responsibly.

AI Governance Committee Structure : At the apex of the governance model sits the AI Governance Committee, a cross-functional body responsible for strategic direction, risk oversight, and policy formulation. This committee comprises senior executives from technology, legal, compliance, risk management, and business operations, ensuring that AI governance decisions reflect both technical realities and business imperatives. The committee meets quarterly to review AI risk assessments, approve high-risk AI deployments, and ensure alignment with evolving regulatory requirements such as the EU AI Act and NIST AI RMF (Papagiannidis et al., 2025).

The committee's primary responsibilities include establishing enterprise-wide AI policies, defining risk appetite and tolerance levels for AI systems, approving budgets for AI governance infrastructure, and serving as the escalation point for critical AI incidents. By positioning governance at the executive level, organizations signal that AI risk management is a strategic priority rather than merely a technical concern (Batool et al., 2025).

C-Suite Role Definition : The governance model assigns specific AI-related responsibilities across the C-suite, recognizing that effective AI governance requires distributed accountability. The Chief Executive Officer (CEO) bears ultimate responsibility for AI strategy alignment with corporate values and long-term business objectives. The CEO champions a culture of responsible AI adoption and ensures that governance mechanisms receive adequate resources and executive attention (Schmitt, 2024). The Chief Information Officer (CIO) oversees the technical infrastructure supporting AI systems, including data pipelines, model deployment platforms, and monitoring tools. The CIO ensures that AI systems integrate seamlessly with existing IT architecture while maintaining security, scalability, and reliability standards (Li et al., 2021). The Chief Data Officer (CDO) manages data governance frameworks critical to GenAI success. This includes establishing data quality standards, implementing data minimization and anonymization protocols, and ensuring compliance with data protection regulations such as GDPR and CCPA. The CDO also oversees training data curation, addressing concerns about bias, representativeness, and intellectual property rights (Taeihagh, 2025). The Chief Information Security Officer (CISO) leads cybersecurity efforts specific to AI systems, including protection against adversarial attacks, prompt injection, model inversion, and API-probing threats. The CISO implements technical safeguards such as differential privacy, federated learning, and secure model deployment practices. The Chief Risk Officer (CRO) maintains the enterprise AI risk register, conducts regular risk assessments, and ensures that AI-related risks integrate into the organization's broader enterprise risk management framework. The CRO coordinates with internal audit to verify that AI controls operate effectively. The Chief Compliance Officer (CCO) ensures that AI deployments comply with applicable laws, regulations, and industry standards. This includes monitoring regulatory developments, conducting compliance assessments for high-risk AI applications, and maintaining documentation required for regulatory audits (Jedrzejewski et al., 2024).

Operational Governance Layers : Beneath the executive level, the governance model establishes operational structures that translate strategic direction into day-to-day practice. AI Development Teams implement technical controls during model development, including bias testing, explainability mechanisms, and security hardening. These teams follow secure development lifecycle practices adapted for AI systems (Papagiannidis et al., 2022).
The AI Ethics Review Board evaluates proposed AI applications for ethical implications, including potential for discrimination, privacy violations, or societal harm. This board includes diverse perspectives, incorporating voices from affected communities and subject matter experts in ethics, law, and social sciences (Radanliev, 2025). The Data Governance Council enforces data policies, approves data access requests for AI training, and monitors data usage to prevent unauthorized exposure of sensitive information. This council works closely with the CDO to implement technical controls such as data lineage tracking and access logging (Tewari, 2025).

Evaluation of the Framework

Alignment with NIST AI Risk Management Framework : The proposed governance model aligns closely with the NIST AI RMF's four core functions: Govern, Map, Measure, and Manage. The AI Governance Committee and C-suite role definitions directly address the "Govern" function by establishing accountability structures and risk management processes. The framework's emphasis on risk identification and categorization supports the "Map" function, while requirements for continuous monitoring and auditing fulfill the "Measure" function. Finally, the technical and procedural controls implement the "Manage" function by providing mechanisms to mitigate identified risks (Tabassi, 2023). The NIST framework's risk-based approach resonates with the proposed model's emphasis on risk appetite definition and tiered controls based on AI system criticality. Both frameworks recognize that not all AI applications pose equal risk and that governance mechanisms should be proportionate to potential harm (Papagiannidis et al., 2025).

Comparison with EU AI Act Requirements : The EU AI Act establishes a risk-based regulatory regime categorizing AI systems into prohibited, high-risk, limited-risk, and minimal-risk categories. The proposed governance framework anticipates these requirements by incorporating risk classification processes and enhanced controls for high-risk applications (Ebers, 2024). For high-risk AI systems as defined by the EU AI Act (such as those used in employment decisions, credit scoring, or law enforcement), the framework mandates additional safeguards including human oversight, comprehensive documentation, bias testing, and transparency measures. The AI Ethics Review Board serves as the mechanism for evaluating whether proposed applications fall into high-risk categories requiring enhanced governance (Fedele et al., 2024).

The framework's emphasis on transparency, explainability, and documentation aligns with the EU AI Act's requirements for high-risk systems. Organizations following this governance model will be well-positioned to demonstrate compliance with EU requirements, including maintaining technical documentation, implementing quality management systems, and enabling regulatory audits (Kilian et al., 2025).

Comparison with Existing Methods

Addressing Novel GenAI Risks : Traditional security and compliance frameworks, designed for conventional software systems, prove inadequate for GenAI's unique risk profile. Legacy approaches focus on perimeter security, access controls, and deterministic system behavior. However, GenAI introduces probabilistic outputs, emergent capabilities, and novel attack vectors such as prompt injection and model inversion that existing frameworks do not address (Radanliev et al., 2025). The proposed multi-layered GRC framework specifically targets GenAI risks that legacy methods overlook. For instance, traditional data loss prevention tools cannot detect when a language model inadvertently memorizes and reproduces sensitive training data. The framework addresses this through differential privacy during training, output monitoring, and watermarking techniques absent from conventional security toolkits. Shadow AI, where employees use public GenAI tools without organizational oversight, represents another risk category that traditional IT governance fails to address. The framework incorporates user behavior monitoring, approved tool catalogs, and employee training programs specifically designed for GenAI contexts(Taeihagh, 2025).

Integration Rather Than Replacement : Importantly, the proposed framework does not replace existing security and compliance mechanisms but rather extends them to address GenAI-specific challenges. Traditional controls such as network security, identity and access management, and incident response remain foundational. The framework layers GenAI-specific controls atop this foundation, creating a comprehensive defense-in-depth strategy (Nadella et al., 2025). This integrated approach recognizes that GenAI systems operate within broader IT ecosystems and must align with existing governance structures. By defining clear interfaces between traditional IT governance and AI-specific controls, the framework enables organizations to leverage existing investments while addressing new risks systematically (Taeihagh, 2025).

VII. RESULTS AND DISCUSSION: STRATEGIC ADAPTATION

The analysis shows that Generative Artificial Intelligence (GenAI) has become an integral element within our technological framework, with its rapid spread across industries making avoidance impractical. The adoption rate of tools like ChatGPT, which reached 100 million users within two months (Milmo, 2023), highlights GenAI's transformative potential as a general-purpose technology like electricity or the internet (Vukmirović and Kresović, 2024). Across healthcare, finance, education, and creative industries, GenAI's applications, including automated clinical documentation, fraud detection, personalized tutoring, and content creation, demonstrate its ability to enhance productivity and foster innovation (Chu et al., 2025). However, this integration brings significant risks, including data privacy breaches, cybersecurity threats like prompt injection, and ethical challenges like algorithmic bias and intellectual property disputes (Hu et al., 2024). The proposed multi-layered GRC framework addresses these challenges by providing a structured approach to responsible adoption, ensuring organizations can leverage GenAI's benefits while mitigating risks. The Governance, Risk, and Compliance (GRC) framework, as an "Architecture of Control," harmonizes innovation with accountability through enterprise controls, industry standards, and regulations. At the enterprise level, the AI Governance Committee and C-suite roles provide strategic oversight, ensuring alignment with organizational objectives and regulations like the EU AI Act and NIST AI Risk Management Framework. Operational layers, including AI Development Teams, Ethics Review Board, and Data Governance Council, implement this strategy through technical safeguards and procedural measures like bias testing and human oversight (Papagiannidis et al., 2025). The framework's alignment with NIST AI RMF's functions - Govern, Map, Measure, and Manage - ensures a risk-based approach prioritizing transparency for high-risk applications.

The framework's efficacy is shown by its ability to address GenAI-specific risks overlooked by traditional IT governance, such as training data leakage and shadow AI. By using Privacy-Enhancing Technologies (PETs) like differential privacy and federated learning, the framework mitigates privacy violations. The continuous monitoring and watermarking of outputs enhance traceability (Hu et al., 2024). Compared to EU AI Act's requirements for high-risk systems, the framework's risk classification and controls ensure compliance while fostering stakeholder trust (Ebers, 2024). This adaptability helps organizations navigate regulations, reducing fines and reputational risks while maintaining innovation. The widespread adoption of GenAI necessitates strategic adaptations across organizations, with three key implications: workforce reskilling, human-AI collaboration, and governance agility. First, workforce reskilling is critical to address job displacement, particularly in knowledge-intensive sectors like legal, professional, and creative services, where GenAI can automate tasks traditionally performed by white-collar workers (Merali and Merali, 2023). Organizations must invest in continuous training to foster ethical awareness and technical proficiency, ensuring employees can thrive in an AI-driven economy (Lacsa, 2024). Second, the emergence of human-AI collaboration is redefining operational workflows. Generative AI tools, such as GitHub Copilot and large language model-powered tutoring systems, function as creative co-pilots, enhancing productivity by up to 50% in domains such as software engineering and education (Chu et al., 2025). This collaboration necessitates the integration of human oversight into AI workflows within organizations to ensure that outputs adhere to ethical and legal standards. The proposed framework's focus on human-in-the-loop mechanisms and the AI Ethics Review Board facilitates this transition by assessing outputs for bias and societal impact, thereby fostering trust and accountability (Fedele et al., 2024). Governance agility is crucial for keeping pace with GenAI evolution and regulatory developments. The dynamic nature of transformer-based models and techniques like federated learning require flexible governance structures to address risks. The framework's multi-layered design, with risk assessments by the CRO and compliance monitoring by the CCO, ensures organizations can respond to evolving threats and regulations like the EU AI Act (Kilian et al., 2025). This agility helps balance innovation with control, mitigating risks while unlocking GenAI's potential to generate economic value of $2.6 to $4.4 trillion annually (Chui et al., 2023).

REFERENCES

1. Aditya, H., Chawla, S., Dhingra, G., Rai, P., Sood, S., Singh, T., Wase, Z. M., Bahga, A., & Madisetti, V. K. (2024). Evaluating privacy leakage and memorization attacks on large language models (LLMs) in generative AI applications. *Journal of Software Engineering and Applications*, *17*(05), 421–447. https://doi.org/10.4236/jsea.2024.175023
2. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). AI-powered innovation in digital transformation: Key pillars and industry impact. *Sustainability*, *16*(5), 1790. https://doi.org/10.3390/su16051790
3. Babalola, O. (2022). Data Protection Compliance Organizations (DPCO) Under the NDPR, and Monitoring Bodies Under the GDPR: Two Sides of the Same Compliance Coin? *Global Privacy Law Review*, *3*(Issue 2), 98–106. https://doi.org/10.54648/gplr2022010
4. Batool, A., Zowghi, D., & Bano, M. (2025). AI Governance: A systematic literature review. *AI and Ethics*, *5*(3), 3265–3279. https://doi.org/10.1007/s43681-024-00653-w
5. Bengesi, S., El-Sayed, H., Sarker, M. K., Houkpati, Y., Irungu, J., & Oladunni, T. (2024). Advancements in generative AI: A comprehensive review of GANs, GPT, autoencoders, diffusion model, and Transformers. *IEEE Access*, *12*, 69812–69837. https://doi.org/10.1109/access.2024.3397775
6. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D., Wu, J., Winter, C., … Amodei, D. (2020). Language Models are Few-Shot Learners. *Advances in Neural Information Processing Systems*, *33*, 1877–1901.
7. Brühl, V. (2024). *Generative artificial intelligence – foundations, use cases and economic potential*. Intereconomics. https://www.intereconomics.eu/contents/year/2024/number/1/article/generative-artificial-intelligence-foundations-use-cases-and-economic-potential.html?utm_
8. Chen, M., Tworek, J., Jun, H., Yuan, Q., Pinto, H. P. de O., Kaplan, J., Edwards, H., Burda, Y., Joseph, N., Brockman, G., Ray, A., Puri, R., Krueger, G., Petrov, M., Khlaaf, H., Sastry, G., Mishkin, P., Chan, B., Gray, S., … Zaremba, W. (2021, July 7). *Evaluating large language models trained on code*. arXiv.Org. https://arxiv.org/abs/2107.03374
9. Chow, J. C. L., Wong, V., & Li, K. (2024). Generative Pre-Trained Transformer-Empowered Healthcare Conversations: Current trends, challenges, and future directions in Large Language Model-enabled medical chatbots. *BioMedInformatics*, *4*(1), 837–852. https://doi.org/10.3390/biomedinformatics4010047
10. Chowdhery, A., Narang, S., Devlin, J., Bosma, M., Mishra, G., Roberts, A., Barham, P., Chung, H. W., Sutton, C., Gehrmann, S., Schuh, P., Shi, K., Tsvyashchenko, S., Maynez, J., Rao, A., Barnes, P., Tay, Y., Shazeer, N., Prabhakaran, V., … Fiedel, N. (2022, April 5). *PaLM: Scaling language modeling with Pathways*. arXiv.Org. https://arxiv.org/abs/2204.02311
11. Chu, Z., Wang, S., Xie, J., Zhu, T., Yan, Y., Ye, J., Zhong, A., Hu, X., Liang, J., Yu, P. S., & Wen, Q. (2025, March 14). *LLM agents for education: Advances and applications*. arXiv.Org. https://arxiv.org/abs/2503.11733
12. Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L., & Zemmel, R. (2023, June 13). The economic potential of generative AI: The next productivity frontier. *McKinsey &*

Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier?

13. Ciubotaru, B.-I. (2025a). *Generative AI and large language models: A comprehensive scientific review*. MDPI AG. https://doi.org/10.20944/preprints202504.0413.v2
14. Ciubotaru, B.-I. (2025b, April 10). *Generative AI and large language models: A comprehensive scientific review*. Preprints.Org. https://www.preprints.org/manuscript/202504.0413/v2
15. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2018, October 11). *BERT: Pre-training of deep bidirectional Transformers for language understanding*. arXiv.Org. https://arxiv.org/abs/1810.04805
16. Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., … Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002
17. European Union. (2024). *AI Act*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
18. Ebers, M. (2024). Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act. *European Journal of Risk Regulation*, *16*(2), 684–703. https://doi.org/10.1017/err.2024.78
19. Fedele, A., Punzi, C., & Tramacere, S. (2024). The Altai Checklist as a tool to assess ethical and legal implications for a trustworthy AI development in education. *Computer Law &amp; Security Review*, *53*, 105986. https://doi.org/10.1016/j.clsr.2024.105986
20. FSB. (2024, November 14). *The financial stability implications of artificial intelligence*. Financial Stability Board. https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/
21. Ganguly, A. (2025). Large language models. In *Scaling Enterprise Solutions with Large Language Models* (pp. 129–182). Apress. https://doi.org/10.1007/979-8-8688-1154-8_4
22. Gupta, V. (2024a). An empirical evaluation of a generative artificial intelligence technology adoption model from entrepreneurs' perspectives. *Systems*, *12*(3), 103. https://doi.org/10.3390/systems12030103
23. Gupta, V. (2024b). An empirical evaluation of a generative artificial intelligence technology adoption model from entrepreneurs' perspectives. *Systems*, *12*(3), 103. https://doi.org/10.3390/systems12030103
24. Hu, F., Liu, S., Cheng, X., Guo, P., & Yu, M. (2024). Risks of generative artificial intelligence and multi-tool governance. *Academic Journal of Management and Social Sciences*, *9*(2), 88–93. https://doi.org/10.54097/stvem930
25. Huang, K., Goertzel, B., Wu, D., & Xie, A. (2024). GenAI model security. In *Future of Business and Finance* (pp. 163–198). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54252-7_6
26. Jedrzejewski, F. V., Thode, L., Fischbach, J., Gorschek, T., Mendez, D., & Lavesson, N. (2024). Adversarial Machine Learning in industry: A Systematic Literature Review. *Computers &amp; Security*, *145*, 103988. https://doi.org/10.1016/j.cose.2024.103988
27. Kilian, R., Jäck, L., & Ebel, D. (2025). European AI standards – technical standardisation and implementation challenges under the EU AI act. *European Journal of Risk Regulation*, 1–25. https://doi.org/10.1017/err.2025.10032
28. Lacsa, J. E. M. (2024). Can AI revolutionize workplace safety without compromising ethical standards and regulatory oversight? *Journal of Public Health*, *47*(3), e436–e436. https://doi.org/10.1093/pubmed/fdae195
29. Li, J., Li, M., Wang, X., & Thatcher, J. B. (2021). Strategic directions for AI: The role of cios and boards of directors. *MIS Quarterly*, *45*(3), 1603–1644. https://doi.org/10.25300/misq/2021/16523
30. Liu, X., Yu, Z., Zhang, Y., Zhang, N., & Xiao, C. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models. *arXiv.Org*, *abs/2403.04957*. https://doi.org/10.48550/arxiv.2403.04957
31. Low, D. M., Rankin, O., Coppersmith, D. D. L., Bentley, K. H., Nock, M. K., & Ghosh, S. (2025). *Using Generative AI to create lexicons for interpretable text models with high content validity*. https://doi.org/10.31234/osf.io/vf2bc_v2
32. McKinsey & Company. (2025). *The economic potential of generative AI: The next productivity frontier*. Retrieved from https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontier.pdf

33. Merali, S., & Merali, A. (2023). *The Generative AI Revolution* (A. Hawksbee, Ed.). Https://Www.Ukonward.Com/Wp-Content/Uploads/2023/05/Generative-AI-Revolution-Final.Pdf; Onward. https://www.ukonward.com/wp-content/uploads/2023/05/Generative-AI-Revolution-Final.pdf
34. est-growing-app
35. Milmo, D. (2023, February 2). ChatGPT reaches 100 million users two months after launch. *The Guardian*. https://www.theguardian.com/technology/2023/feb/02/chatgpt-100-million-users-open-ai-fast
36. Mishra, A. (2024). Scalable AI governance and ethics. In *Scalable AI and Design Patterns* (pp. 147–165). Apress. https://doi.org/10.1007/979-8-8688-0158-7_9
37. Nadella, G. S., Addula, S. R., Yadulla, A. R., Sajja, G. S., Meesala, M., Maturi, M. H., Meduri, K., & Gonaygunta, H. (2025). Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy Management. *Computers*, *14*(2), 55. https://doi.org/10.3390/computers14020055
38. Narapareddy, V. S. R. (2025). Generative AI and foundation models. *Universal Library of Innovative Research and Studies*, *Volume 2*(Issue 2).
39. National Institute of Standards and Technology. (2023). *AI risk management framework (AI RMF 1.0)*. U.S. Department of Commerce. Retrieved from https://www.nist.gov/itl/ai-risk-management-framework
40. Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2022). Toward AI governance: Identifying best practices and potential barriers and outcomes. *Information Systems Frontiers*, *25*(1), 123–141. https://doi.org/10.1007/s10796-022-10251-y
41. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, *34*(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885
42. Parasuraman, B. (2024). Introduction to generative AI and large language models (LLMs). In *Mastering Spring AI* (pp. 1–34). Apress. https://doi.org/10.1007/979-8-8688-1001-5_1
43. Powar, J., & Beresford, A. R. (2023). SoK: Managing risks of linkage attacks on data privacy. *Proceedings on Privacy Enhancing Technologies*, *2023*(2), 97–116. https://doi.org/10.56553/popets-2023-0043
44. Radanliev, P. (2025). Ai ethics: Integrating transparency, fairness, and privacy in AI development. *Applied Artificial Intelligence*, *39*(1). https://doi.org/10.1080/08839514.2025.2463722
45. Radanliev, P., Santos, O., & Ani, U. D. (2025). Generative AI cybersecurity and resilience. *Frontiers in Artificial Intelligence*, *8*. https://doi.org/10.3389/frai.2025.1568360
46. Raghvendra, K., Sandipan, S., & Sudipta, B. (2024). *The pioneering applications of generative AI*. IGI Global.
47. Rombach, R., Blattmann, A., Lorenz, D., Esser, P., & Ommer, B. (2021, December 20). *High-Resolution image synthesis with latent diffusion models*. arXiv.Org. https://arxiv.org/abs/2112.10752
48. Şahin, O., & Karayel, D. (2024). Generative artificial intelligence (GenAI) in business: A systematic review on the threshold of transformation. *Journal of Smart Systems Research*, *5*(2), 156–175. https://doi.org/10.58769/joinssr.1597110
49. Sallam, M. (2023). ChatGPT utility in healthcare education, research, and practice: Systematic review on the promising perspectives and valid concerns. *Healthcare*, *11*(6), 887. https://doi.org/10.3390/healthcare11060887
50. Schmitt, M. (2024). Strategic integration of artificial intelligence in the C-suite: The role of the chief ai officer. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4812654
51. Shin, D. (2024). Misinformation and algorithmic bias. In *Artificial Misinformation* (pp. 15–47). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-52569-8_2
52. Smith, N. (2024). *Scalable training, simulation, and serving of large language models and traffic systems: A comprehensive review*. Center for Open Science. https://doi.org/10.31219/osf.io/vnwk9
53. Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. https://doi.org/10.6028/nist.ai.100-1
54. Taeihagh, A. (2025). Governance of generative AI. *Policy and Society*, *44*(1), 1–22. https://doi.org/10.1093/polsoc/puaf001
55. Tewari, S. (2025). AI powered data governance - ensuring data quality and compliance in the era of Big Data. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *8*(1), 187–197. https://doi.org/10.60087/jaigs.v8i1.364
56. Treude, C., & Storey, M.-A. (2025, February 12). *Generative AI and empirical software engineering: A paradigm shift*. arXiv.Org. https://arxiv.org/abs/2502.08108
57. Vasa, Y. (2024). Ethical implications and bias in generative AI. *International Journal for Research Publication and Seminar*, *15*(3), 500–511. https://doi.org/10.36676/jrps.v15.i3.1541

58. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017, June 12). *Attention is all you need*. arXiv.Org. https://arxiv.org/abs/1706.03762
59. Vukmirović, D. V., & Kresović, D. S. (2024). Transformacioni potencijal generativne veštačke inteligencije. *Napredak - Časopis Za Političku Teoriju i Praksu*, *5*(2), 29–42. https://doi.org/10.5937/napredak5-52069
60. Yenduri, G., M, R., G, C. S., Y, S., Srivastava, G., Maddikunta, P. K. R., G, D. R., Jhaveri, R. H., B, P., Wang, W., Vasilakos, A. V., & Gadekallu, T. R. (2023, May 11). *Generative pre-trained transformer: A comprehensive review on enabling technologies, potential applications, emerging challenges, and future directions*. arXiv.Org. https://arxiv.org/abs/2305.10435
61. Yu, P., Xu, H., Hu, X., & Deng, C. (2023). Leveraging generative AI and large language models: A comprehensive roadmap for healthcare integration. *Healthcare*, *11*(20), 2776. https://doi.org/10.3390/healthcare11202776