CONNOR GROUP

Generative AI Governance Framework 2.0

Harness the power of generative artificial intelligence (GenAI) and appropriately manage the risks.

Authors

Scott A. Emett, PhD

Associate Professor, Arizona State University

Marc Eulerich, PhD, CIA

Dean and Professor, University of Duisburg-Essen

Jason Pikoos

Director, Modern Finance, Meta

David A. Wood, PhD

Professor, Brigham Young University

Contributor

Matt MacLachlan

Partner, Financial Operations, Connor Group

Foreword

We are grateful to the over 1,000 reviewers, contributors, endorsers, and sponsors of this enormous undertaking. Building proper governance models for disruptive and rapidly evolving technologies requires considering many points of view. As such, we've involved thought leaders and process experts from industry, academia, and regulatory bodies.

This updated version reflects learning from the past year, feedback received and experiences gained from applying this framework to a variety of companies.

Table of Contents

Introduction

This framework aims to help organizations harness the power of generative artificial intelligence (GenAI) and AI while appropriately managing its risks. More than 1,000 practitioners and academics contributed to the development of the original framework. Participating experts include GenAI specialists, internal and external auditors, regulators, audit committee members, C-suite executives, and others. We crafted this framework to benefit organizations across various sectors, including for-profit, not-for-profit, governmental, and more.

GenAI pushes the boundaries of governance by creating entirely new information that did not exist before. As such, it introduces a multitude of new possibilities and risks that organizations must confront.

While individuals frequently use GenAI directly through purchased products like OpenAI's ChatGPT or Google's Gemini, they may also engage with it unwittingly. For example, employees might unknowingly use AI solutions through software programs that embed GenAI components, such as Microsoft's Copilot. Moreover, GenAI can be integrated into organization-specific GenAI solutions, like a "Company GPT." This framework aims to assist in each of these situations by identifying and mitigating GenAI-related risks.

This version has been updated to incorporate best practices, feedback, and observations from users of the framework during the past year.

Endorsements

"This governance framework is more than a set of rules—it's a practical, user-friendly tool that empowers teams to innovate responsibly while maintaining critical controls. It strikes the right balance between driving automation and ensuring coordination, prioritization, and trust at every step. It can help organizations of all sizes to find success with GenAI."
Aaron Anderson, Chief Accounting Officer, Meta Platforms, Inc.

"We find ourselves in a new and exciting time when it comes to AI and its current and prospective effects on society and business. Conceptualizing a coherent way for organizations to approach AI governance in the wilds of this rapidly developing environment becomes crucial. I see this effort as a significant and important step forward in this vital space, and I commend the authors as insightful early movers!"
Douglas F. Prawitt, PhD, CPA – Director of Brigham Young University School of Accountancy and Lead Director of Committee of Sponsoring Organizations (COSO) Board

"The AI Governance framework presents a fantastic approach for internal auditors, but also for other assurance providers and the board to create and validate an effective AI governance structure."
Dorothea Mertmann – CEO of IIA Germany (Deutsches Institut für Interne Revision e.V.)

"We will soon encounter generative AI in many parts of our everyday working lives. With this framework, internal audit can deal with the risks at an early stage. It can sensitize the audited parties and support them in setting up suitable governance and a control environment. From this perspective, the Generative AI Governance Framework is an ideal tool for positioning internal audit as a reliable point of contact for risks associated with the use of artificial intelligence."
Gabrielle Rudolf von Rohr – President, IIA Switzerland

"Effective AI adoption will be a massive competitive advantage but many don't know where to start and how to apply it. A few AI tools exist now with many on the way, and they are coming fast. Having a smart AI adoption strategy with underlying controls, data and processes that are ready for AI takes time. The most competitive companies are doing these things now."
Jeff Pickett – Chair, Connor Group

The GenAI Governance Framework breaks down governance into five essential domains.

1. Strategic Alignment and Control Environment

2. Data and Compliance Management

3. Operational and Technology Management

4. Human, Ethical, and Social Considerations

5. Transparency, Accountability, and Continuous Improvement

GenAI Governance Framework

Operational and Technology Management
- Integrate GenAI into operational processes.
- Manage GenAI technology and IT security.

Transparency, Accountability, and Continuous Improvement
- Ensure transparent and traceable GenAI decision-making.
- Monitor evolution of GenAI and update governance practices.

Data and Compliance Management
- Establish processes for identifying, assessing, and mitigating data-related risks.
- Ensure compliance with legal and regulatory standards.

Strategic Alignment and Control Environment
- Align GenAI initiatives with organizational goals, strategies, and risk appetite/tolerance.
- Develop comprehensive GenAI governance policies.

Human, Ethical, and Social Considerations
- Conduct GenAI training and manage human resource risks.
- Ensure ethical GenAI use that mitigates bias.
- Assess and manage reputational and social impacts.
- Assess and manage environmental impacts.

Within each of these domains, the framework identifies several risks and control considerations. By delineating risks and control considerations, the framework helps organizations (1) to understand how GenAI can threaten organizational objectives and (2) to craft governance approaches that mitigate those risks. We provide a complete set of risks and control considerations at the end of this document.

This framework should help organizations achieve the following objectives:

- Enhance overall GenAI risk management

- Establish GenAI governance structures

- Drive strategic improvement and compliance

- Secure stakeholder engagement and trust

- Benchmark for continuous improvement

How to Use the Framework

Before using the framework, organizations should consider their risk appetite and risk tolerance in the context of GenAI. As with any other technology, an organization must decide how much risk they are willing to accept when adopting GenAI applications and solutions. This framework guides organizations in aligning GenAI risks with their established risk appetite. We recommend that organizations adopt the framework in five steps.

STEP 01

Define GenAI Objectives and Goals

Define specific GenAI objectives and goals. Ensure they align with:

- Established corporate strategy and digitalization objectives
- Stakeholder expectations
- Compliance and regulatory requirements
- Budgetary constraints

STEP 02

Establish Appropriate Framework Scope for Your Organization

The GenAI Governance Framework aims to serve a variety of organizations. Therefore, some of the framework's domains, risks, and control considerations may not apply to your organization. Organizations should align the scope of the framework with their organizational needs and priorities:

- Identify priority **domains** in the governance framework for your organization.
- Identify the **key risks** within each domain that are most relevant to your organization.
- Determine the **functions** within your organization that are most impacted by GenAI risks (e.g., department, business unit).
- Identify **processes, projects, and technologies** that are most exposed to GenAI risks.
- Select appropriate **stakeholders** to be involved in GenAI governance.

STEP 03

Perform an Initial Risk Assessment:

To assess GenAI risk, start by documenting your existing AI systems in use and planned implementations, along with your underlying technology. Then identify what could go wrong and evaluate your potential exposure by analyzing both likelihood and impact.

• **AI Inventory and Plan**

- Audit the GenAI technologies currently in use across your organization.

- Outline the AI tools and projects you plan to implement over the next 12 months.

- Document the ownership, function, purpose, and deployment scope of each AI solution.

• **Define Use Cases and AI Technology Types**

- Chat/Drafting

- Analytics/Insights

- Workflow/Process Support

- External/Client-facing Outputs

- Agentic AI/Workflow Automation

What Could Go Wrong?

When evaluating AI risks, focus on both the probability and severity of potential issues across your organization. Financial threats can emerge through payment errors and fraud exposure, while inaccurate reporting may compromise your financial controls and compliance obligations. Your organization also faces regulatory challenges, particularly around privacy violations and other compliance breaches that could trigger penalties. Beyond financial and regulatory concerns, consider how AI failures might disrupt daily operations through process breakdowns and service interruptions. Perhaps most critically, poor AI performance can erode client trust and damage your brand reputation, creating long-term consequences that extend far beyond immediate operational issues.

STEP 04

Complete an GenAI Governance Assessment

We recommend the following approach approach to GenAI risk assessment, with a deliverable produced in each stage. The initial risk identification and assessment of GenAI in your organization can follow the traditional risk assessment procedures presented in the figure. We provide additional details and a survey that allows you to perform a detailed GenAI governance maturity assessment at the following link: **genai.global**

Stage	Activities	Deliverable
Planning & Preparation	• Develop scope, objectives and confirm timelines. • Perform initial risk assessment. • Identify stakeholders and conduct a kick-off. • Gather documentation and complete survey.	**DELIVERABLE:** • Project kick-off and plan • AI risk profile
Data Collection & Review	• Review survey results and relevant documentation (e.g., policies, strategy documents). • Hold interviews and/or conduct workshop with senior leadership in finance, engineering, IT, legal, etc.	**DELIVERABLE:** Survey results and benchmarking
Risk Assessment & Prioritization	• Benchmark organization's existing GenAI landscape against GenAI Governance Framework. • Identify unmitigated risks. • Prioritize risks using survey and working sessions.	**DELIVERABLE:** Summary of prioritized unmitigated risks
Recommendations & Roadmap	• Propose actionable mitigation strategies for top high priority unmitigated risks. • Develop an implementation roadmap and timeline.	**DELIVERABLE:** Prioritized recommendations and roadmap
Report Results	• Prepare executive summary report. • Review with key stakeholders • Align on go-forward plans and next steps.	**DELIVERABLE:** Final executive report

STEP 05

Execute Your Defined Plan (based on your Risk Assessment)

In Step 5, organizations integrate the GenAI governance plan into their strategic plans based on the risks. Effective governance requires adapting existing methods and resources to support the unique risks and control considerations of GenAI projects. We recommend that organizations treat GenAI governance and controls as a critical priority given their emerging importance and unique risks.

Conclusion

This framework aims to help organizations create an effective and efficient governance structure for GenAI. It has been vetted and prepared by numerous groups and professionals.

The GenAI Governance Framework

On the following pages, you will find the entire governance framework, including risks and control considerations. The framework is provided as a free resource. To complement the framework, we have developed a maturity model available at genai.global.

The framework is not designed to address all data and technology risks, and we therefore recommend that it be used in conjunction with other existing governance frameworks like COSO Internal Control – Integrated Framework, COSO Enterprise Risk Management framework, COBIT, and the Three Lines Model, as well as COSO's GenAI-specific internal-control guidance, *Achieving Effective Internal Control Over Generative AI (GenAI)*.

Finally, we expect this framework to continue to evolve as GenAI technology evolves and adoption expands. As such, the authors, with help from sponsoring organizations, will regularly provide updates as changes occur.

Using this Framework with COSO's GenAI Internal Control Guidance

As Finance and Compliance teams expand their use of AI, strong, practical governance remains essential to manage evolving AI-related risk consistently across the organization. Our updated GenAI Governance Framework provides a top-down, materiality-based foundation for right-sized GenAI governance before teams move into more specific internal control and compliance objectives, such as those described in the recently published *Achieving Effective Internal Control Over Generative AI*. Authored by the same team, the two resources span the journey from strategy to execution: this framework sets the enterprise-wide GenAI governance foundation, and the internal-control guidance shows how to translate that foundation into specific controls and ICFR practices.

GenAI Governance Framework

Operational and Technology Management

- Integrate GenAI into operational processes.
- Manage GenAI technology and IT security.

Data and Compliance Management

- Establish processes for identifying, assessing, and mitigating data-related risks.
- Ensure compliance with legal and regulatory standards.

Strategic Alignment and Control Environment

- Align GenAI initiatives with organizational goals, strategies, and risk appetite/tolerance.
- Develop comprehensive GenAI governance policies.

Transparency, Accountability, and Continuous Improvement

- Ensure transparent and traceable GenAI decision-making.
- Monitor evolution of GenAI and update governance practices.

Human, Ethical, and Social Considerations

- Conduct GenAI training and manage human resource risks.
- Ensure ethical GenAI use that mitigates bias.
- Assess and manage reputational and social impacts.
- Assess and manage environmental impacts.

DOMAIN	DESCRIPTION	KEY OBJECTIVE	KEY RISKS ADDRESSED
Strategic Alignment and Control Environment	Domain focuses on ensuring that GenAI initiatives are in harmony with the organization's overall goals and strategies. It involves setting the appetite and direction for GenAI use and establishing the control environment for it.	• Align GenAI initiatives with organizational goals, strategies, and risk appetite/tolerance. • Develop comprehensive GenAI governance policies.	• Strategic and Planning Risks • Control Environment Risks
Data and Compliance Management	Domain focuses on identifying, assessing, and mitigating data-related risks; and ensuring compliance with all relevant legal and regulatory standards.	• Establish processes for identifying, assessing, and mitigating data-related risks. • Ensure compliance with legal and regulatory standards.	• Data-Related Risks • Legal and Regulatory Regime Risks
Operational and Technology Management	Domain focuses on the integration of GenAI into business processes, managing the technology itself, and ensuring IT security. It addresses the practical application of GenAI in daily operations.	• Integrate GenAI into operational processes. • Manage GenAI technology and IT security.	• Process Management Risks • Technology Evaluation and Selection Risks • Enhanced Operational and IT Security and Access Risks
Human, Ethical, and Social Considerations	Domain addresses the impact of GenAI on the workforce, ethical considerations, and broader social implications. It emphasizes the importance of addressing the human-centric aspects of GenAI deployment.	• Conduct GenAI training and manage human resource risks. • Ensure ethical GenAI use that mitigates bias. • Assess and manage reputational and social impacts. • Assess and manage environmental impacts.	• Knowledge and Training Risks • HR and Employment Risks • Ethical and Bias Risks • Reputation and Social Risks • ESG Risks
Transparency, Accountability, and Continuous Improvement	Domain focuses on ensuring that the use of GenAI in decision-making is transparent and accountable. It also focuses on the continuous improvement of GenAI governance practices, adapting to new challenges and technologies.	• Ensure transparent and traceable GenAI decision-making. • Monitor evolution of GenAI and update governance practices.	• Transparency, Traceability, and Trust Risks • Continuing Evolution of the Technology Risks • Miscellaneous Risks • High Conceptual or Hypothetical Risks

Key Control Considerations for Mitigating GenAI Risks

Strategic Alignment and Control Environment

Strategic and Planning Risks and Control Considerations

RISKS
Not aligning GenAI initiatives with long-term organizational goals.

CONTROL CONSIDERATIONS	
GenAI Risk Management Framework	Develop and implement a framework for governing GenAI risk. The framework should integrate with or update other frameworks (e.g., COSO Internal Control – Integrated Framework, COSO Achieving Effective Internal Control Over Generative AI (GenAI), COSO Enterprise Risk Management framework, COBIT).
Strategic GenAI Roadmap	Develop a strategic roadmap with cross-functional buy-in for GenAI integration that aligns with organizational goals.
Regular Strategy Review	Establish a regular review process to align GenAI initiatives with evolving organizational strategies.
Stakeholder Engagement	Involve key stakeholders in GenAI project planning to ensure alignment with business objectives and risk appetite.
Measure Performance and Return on Investment (ROI)	Set up metrics and key performance indicators (KPIs) to measure the effectiveness of GenAI initiatives in achieving strategic goals and ROI. Regularly monitor changes in GenAI capabilities to align measures with strategic objectives.
Performance Monitoring	Establish a regular cadence for evaluating the performance of GenAI initiatives and ROI achieved; take steps to realign initiatives as strategic goals evolve.
Contingency Planning	Develop contingency plans for GenAI projects to manage unexpected outcomes or changes in strategic direction.
Competitive Landscape Monitoring	Regularly evaluate market trends, competitor use of GenAI technologies, and evolving customer expectations to ensure organizational competitiveness in a rapidly changing technology landscape.
Scenario Planning and Forecasting	Implement scenario planning for GenAI initiatives to anticipate and prepare for potential unexpected events.

Control Environment Risks and Control Considerations

RISKS
Needing to develop new or updated policies, educating users about GenAI management, structuring responsibilities within GenAI governance, and managing the residual responsibility of decision-makers who rely on GenAI recommendations.

CONTROL CONSIDERATIONS	
Policy Development and Governance	Oversee comprehensive GenAI governance and usage policies based on risk appetite, strategy, and relevant legal guidelines. Regularly monitor compliance with policies, including appropriate usage.
Clear Roles and Responsibilities	Define and communicate roles and responsibilities related to GenAI governance within the organization.
Establish GenAI Governance	Establish a committee or comparable institution to oversee GenAI governance and policy implementation. The committee should have broad representation both vertically and horizontally within the organization to integrate all necessary aspects of GenAI use.
GenAI Inventory	Ensure a centralized inventory of all GenAI use cases in development or production across the organization is maintained.
Regular Policy Review and Update	Establish a regular review process to ensure GenAI policies are updated to reflect new developments and insights.
GenAI Ethics Framework	Implement an GenAI ethics framework to guide decision-making in GenAI projects.
Incident Response Plan	Develop an incident response plan specifically for GenAI-related issues, for example, security breaches or driving business decisions incorrectly.

Data and Compliance Management

Data-Related Risks and Control Considerations

RISKS
Risks related to data breaches, unauthorized access, mismanagement, the propagation of incorrect information by GenAI systems, overreliance on GenAI (GenAI Dependence), and the threat of competitors using GenAI to gather intelligence.

CONTROL CONSIDERATIONS	
Data Governance Framework	Establish a comprehensive data governance framework to manage risks across data collection, storage, accessibility, quality, confidentiality, retention, security, deletion, and exportation. Frequently review and update.
Access Control Policies	Implement strict access control policies, including role-based access, for sensitive tools and data.
Data Encryption and Anonymization	Use data encryption and anonymization techniques to protect sensitive information.
GenAI Data Lineage Tools	Track data lineage across the organization to ensure transparency into how data is used by GenAI systems.
Regular Data Audits	Conduct regular audits to ensure data integrity and to detect any unauthorized access or breaches.
Self-learning Models	Establish a clear audit and monitoring process for self-learning models to address potential risks as soon as possible. Self-learning models are GenAI systems that autonomously improve their performance and adapt over time by learning from new data and experiences without explicit human instruction.

Legal and Regulatory Risks and Control Considerations

RISKS
This risk category addresses the risks associated with compliance with changing laws and government mandates specific to GenAI, including adapting to regulatory constraints, fulfilling transparency and reporting requirements, and managing legal liabilities for GenAI actions. It also involves staying current with international legal standards, protecting intellectual property, and developing strategies for engagement with regulatory bodies and rapid response to legal changes.

CONTROL CONSIDERATIONS	
Documentation and Reporting Processes	Maintain thorough documentation and reporting to ensure transparency and facilitate compliance for all GenAI solutions in the organization.
Compliance Monitoring	Implement a process for the continuous monitoring of, and compliance with, relevant laws and regulations.
GenAI Legal Risk Assessment	Regularly conduct legal risk assessments for GenAI initiatives.
Monitoring and Training on Regulatory Changes	Regularly monitor, update, and train staff on new regulatory developments affecting GenAI.
Cross-border Compliance Strategy	Develop strategies to manage compliance across different jurisdictions, especially in multinational operations.
Regulatory and Investor Reporting	Establish processes to comply with reporting requirements around GenAI, like SEC filings, regulatory disclosures, etc.
Insurance Risk Management	Establish recurring processes to assess new or changes to insurance risks arising from the use of GenAI technologies.

Operational and Technology Management

Process Management Risks and Control Considerations

RISKS
Risks of the operational use of GenAI, including risks in validating GenAI applications and outputs.

CONTROL CONSIDERATIONS	
Standard Operating Procedures for GenAI Use	Develop and implement standard operating procedures (SOPs) for GenAI applications within business processes.
GenAI Performance Monitoring	Establish regular and recurring processes to evaluate the performance of GenAI applications. Conduct red teaming exercises and adversarial testing of GenAI systems at regular intervals (or continuously), especially for high-risk use cases. Testing should simulate misuse, prompt injection, and evasion scenarios. Align red teaming protocols with requirements under regulations such as the EU AI Act and document mitigations for identified vulnerabilities. Regularly validate retrieval-augmented generation (RAG) systems for freshness of retrieved content and model-version alignment. Document content refresh intervals and ensure alignment between source datasets and model outputs. Versioning controls should be in place to track changes in RAG pipeline components.
Validation and Testing Protocols	Implement rigorous validation and testing protocols with stakeholder approval for GenAI applications before deployment. Measure and document hallucination rates of GenAI systems, especially in critical or externally facing applications. Track performance over time and communicate known error rates to stakeholders. Incorporate thresholds for acceptable output reliability, aligned with regulations like the EU AI Act guidance, SOX compliance, etc.
Change Management Procedures	Develop change management procedures for GenAI implementation to minimize operational disruption, achieve required levels of accuracy and reliability, and address relevant bias and ethical risks. Change management procedures must account for the continuously evolving nature of GenAI models and tools.

Technology Evaluation and Selection Risks and Control Considerations

RISKS
This risk category addresses the need to maintain data confidentiality, secure GenAI systems against threats, manage data transfer risks, and address GenAI social engineering and other cybersecurity threats.

CONTROL CONSIDERATIONS	
Technology Assessment Framework	Create a framework for assessing and selecting GenAI technologies that align with organizational goals, needs, and compliance (security, confidentiality, controls) requirements.
Vendor Risk Assessment	Conduct thorough risk assessments of key vendors (e.g., technology providers, suppliers, professional services) and their GenAI solutions or tools they use, before implementation and engagement. Embed GenAI review as part of third-party risk management and vendor onboarding processes, including ongoing monitoring to reflect the evolving nature of the technology and use by vendors.
GenAI Feature Integration and Management Protocol	Establish a protocol for vetting, integrating, and managing new GenAI features in existing systems. This protocol should include a comprehensive assessment process.
Third-Party Contract Management	Ensure all contractual arrangements with vendors appropriately contemplate and define GenAI risks, responsibilities, and technologies used or offered by vendors. Contracts should be re-evaluated periodically as GenAI technologies evolve and vendor usage changes.
Post-Implementation Review	Conduct post-implementation reviews to assess the effectiveness and impact of GenAI technology.

Operational and Technology Management

Enhanced Operational, IT Security, and Access Risks and Control Considerations

RISKS
This risk category addresses the need to maintain data confidentiality, secure GenAI systems against threats, manage data transfer risks, and address GenAI social engineering and other cybersecurity threats.

CONTROL CONSIDERATIONS	
Robust IT Security Policies	Ensure GenAI systems comply with other organizational policies. As needed, draft supplemental policy/procedure language to meet any gaps posed by the GenAI system.
Data Security Training for Employees	Provide comprehensive data security training to employees involved in GenAI operations.
Incident Response and Recovery Plans	Establish incident response and recovery plans for potential security breaches or major operational failures in key GenAI systems.
Access Management and Authentication	Strengthen access management and authentication mechanisms for GenAI systems and those systems connected to GenAI systems. Evaluate GenAI access to all systems.
Continuous Threat Detection and Response	Maintain continuous monitoring systems to detect and respond to security threats promptly (e.g., AI-driven cyberattacks, video deepfakes).
Prompt Management and Leakage Prevention Controls	Implement controls to manage and secure prompts, especially in applications where prompts include sensitive or proprietary data. Ensure prompts are not stored or reused unless explicitly permitted. Monitor for prompt-leakage risks and restrict access to prompt histories within GenAI tools.

Human, Ethical, and Social Considerations

Knowledge and Training Risks and Control Considerations

RISKS
This risk category addresses the need to train users on the risks and limitations of GenAI.

CONTROL CONSIDERATIONS	
Transparently Communicate Model Data and Weights	Ensure that users are aware and regularly evaluate how up to date the model is, what data it is sourcing for responses, and if available, the weights embedded in the model that impact outcomes and decisions.
Training Plan for Employees	Develop a training plan to teach employees how to use GenAI models, potential limitations of GenAI models, and other risks involved in using GenAI.

Human Resource and Employment Risks and Control Considerations

RISKS
This category addresses risks related to human resources, including the impact of GenAI on employment rates, the potential replacement of jobs by GenAI in specific sectors, and the fear among personnel of job loss due to GenAI implementation.

CONTROL CONSIDERATIONS	
Transparent Communication Strategy	Develop a strategy for transparent communication about GenAI's impact on jobs and roles.
GenAI-related Job Creation Strategies	Identify and develop new job roles and opportunities created by GenAI advancements.
Employee Involvement in GenAI Implementation	Involve employees in the design and implementation of GenAI solutions to foster acceptance and understanding.
Reskilling and Upskilling Programs	Implement programs to reskill and upskill employees affected by GenAI integration.
GenAI Integration Feedback Loops	Create mechanisms for employees to provide feedback on GenAI integration.

Human, Ethical, and Social Considerations

Ethical and Bias Risks and Control Considerations

RISKS
This category addresses the risks that GenAI systems may perpetuate biases or be used unethically.

CONTROL CONSIDERATIONS	
Bias Detection and Mitigation Framework	Develop and implement a framework to identify and mitigate biases in GenAI systems.
Bias Compliance Monitoring	Establish a regular review cadence to ensure GenAI tools consistently adhere to the organization's ethics and bias framework.
Diverse Data	Ensure diversity in data sets if training GenAI to reduce the risk of inherent biases.
Regular Ethics Training	Conduct regular ethical considerations and bias awareness training for employees using and managing GenAI.
User Feedback Mechanisms	Implement mechanisms to receive and address user feedback.
Third-Party Audits for Ethical Compliance	Perform audits and/or review audit reports and controls for GenAI tools purchased from external parties.

Reputation and Social Risks and Control Considerations

RISKS
This risk category addresses the risks related to reputational damage from GenAI-based communication.

CONTROL CONSIDERATIONS	
Implement "Human-in-the-Middle" Policies for Sensitive Disclosures	For external communications or disclosures deemed important or sensitive, require that someone reviews all AI-generated content before release.
Reputation Response Team	Designate and train a group on how to respond to any negative reactions to AI-generated content.

Human, Ethical, and Social Considerations

Environmental, Social, and Governance (ESG) Risk and Control Considerations

RISKS
This risk category addresses environmental impacts of GenAI systems, social implications such as workforce displacement or societal disruption, and governance challenges.

CONTROL CONSIDERATIONS	
Governance Framework for Environmental, Social, and Governance Impact	Use and modify existing ESG framework to manage the ESG impact of GenAI.
Environmental Impact Assessments for GenAI	Evaluate the environmental impact of GenAI systems (e.g., energy consumption).
Social Impact Assessment for GenAI	Evaluate potential unethical and/or undesired impacts (see also Ethical and Bias Risks and Control Considerations).
Governance Impact Assessment for GenAI	Evaluate potential impacts on other governance and assurance functions.
Sustainable GenAI Development Practices	Adopt environmentally sustainable practices in GenAI development and deployment.
ESG Training for GenAI Teams	Provide training on ESG considerations for teams involved in GenAI development and operations.

Transparency, Accountability, and Continuous Improvement

Transparency, Traceability, and Trust Risks and Control Considerations

RISKS
This risk category addresses the need for clarity in GenAI decision-making processes, ensuring outcomes and decisions are traceable, and mitigating the risk of overconfidence or authority bias when accepting GenAI's judgment without sufficient scrutiny.

CONTROL CONSIDERATIONS	
Gen AI Decision-Making Documentation	Implement requirements for documenting how GenAI is used and reported, including audit trails and source references used to track and review GenAI decisions and their outcomes.
Traceability Protocols in GenAI Development	Incorporate traceability protocols in GenAI development and deployment phases.
Regular Reviews of GenAI Decision Processes	Schedule regular reviews to ensure the continuous traceability of GenAI decisions.
Stakeholder Reporting on GenAI Decisions	Establish reporting mechanisms to communicate GenAI decision-making to stakeholders. Require the use of secure watermarking or metadata tagging when sharing AI-generated content externally (e.g., with customers, investors, regulators). Ensure watermarking mechanisms are tamper-resistant and make clear whether content was AI-generated, in line with transparency requirements.

Continuing Evolution of the Technology Risks and Control Considerations

RISKS
This risk category addresses the need for organizations to adapt GenAI governance to the rapid pace of technological advancements in GenAI.

CONTROL CONSIDERATIONS	
Technology Evolution Monitoring Program	Establish a dedicated program that continuously monitors the evolution of generative GenAI technology. The program should include input from a diverse set of employees spanning the organization.
Review and Update Governance Framework	Regularly review and update governance frameworks and policies to reflect significant changes in risks driven by developments in GenAI capabilities.
Innovation Labs and Pilot Programs	Create innovation labs or pilot programs to experiment with new GenAI technologies in a controlled environment. These labs can provide insights into the practical implications of emerging GenAI technologies and inform risk management strategies.

Transparency, Accountability, and Continuous Improvement

Miscellaneous Risks and High Conceptual or Hypothetical Risks and Control Considerations

RISKS
The Miscellaneous Risk category addresses a variety of risks, including a lack of awareness of GenAI's capabilities and limitations, potential for abuse, challenges in standardization, and geopolitical or geostrategic impacts on global balances arising from GenAI. The Conceptual or Hypothetical Risk category addresses theoretical risks that GenAI could become uncontrollable or achieve a level of superintelligence.

CONTROL CONSIDERATIONS	
GenAI Awareness and Education Programs	Develop and deliver programs to relevant internal and/or external stakeholders to enhance awareness about GenAI capabilities, risk, limitations, and appropriate use.
Abuse Prevention Mechanisms	Implement mechanisms to prevent and to detect the misuse or abuse of GenAI technologies.
Rapid Response and Mitigation Teams	Set up rapid response teams equipped to deal with unexpected GenAI-related incidents or crises. These teams should have clear protocols for assessing situations, making decisions, and implementing mitigation strategies quickly to minimize impact.
Stakeholder Engagement and Dialogue	Facilitate ongoing dialogue with stakeholders, including customers, regulators, and the public, to discuss concerns and expectations related to GenAI. This engagement can help identify emerging risks and societal concerns that may not be immediately apparent.

About Our Authors

Scott A. Emett, PhD
Associate Professor, Arizona State University

Scott Emett is an associate professor at Arizona State University. His research examines how producers and consumers of financial disclosures make judgments and decisions, often focusing on how technological disruptions shape those judgments and decisions. He strives to conduct research that offers valuable insights for practitioners in the field, bridging the gap between academic research and practical application. His research has been published in major journals, such as Journal of Accounting and Economics; The Accounting Review; Contemporary Accounting Research; Accounting, Organizations, and Society; Review of Accounting Studies; and Auditing: A Journal of Practice and Theory, among others.

Marc Eulerich, PhD, CIA
Dean and Professor, University of Duisburg-Essen

Marc Eulerich, is the Chair for Internal Auditing and the Dean at the Mercator School of Management, University Duisburg-Essen, Germany. He also heads the Center for Internal Auditing Excellence and the Mercator Audit & Artificial Intelligence Research Center (MAARC), both at the same university. He has published over 150 scientific and practitioner articles and books about corporate governance, internal auditing, and strategy. His research is published in numerous national and international journals. Prof. Dr. Eulerich also supports the Global internal audit profession with numerous talks and consulting projects to intensify the relationship between theory and practice

Jason Pikoos
Director, Modern Finance, Meta

Jason Pikoos is the Director of Modern Finance at Meta. Jason brings over 20 years of accounting, operational and technology experience, working with high-growth and technology companies. He is a leader in helping companies drive operational excellence through processes improvement, technology & automation, data and analytics and effective governance. Jason graduated from the University of Cape Town and spent over 10 years in public accounting prior to joining Connor Group, where he was a Managing Partner for 13 years.

David A. Wood, PhD
Professor, Brigham Young University

David A. Wood is the Glenn D. Ardis Professor of accounting at Brigham Young University. With over 200 publications in respected academic and practitioner journals, monographs, books, and cases, David's research focuses on technology, governance, risk management, and internal controls. His influential work has earned him recognition as one of the 100 most influential people in accounting by Accounting Today. David collaborates with companies of all sizes, accounting firms, and regulators, providing insights and expertise on emerging governance and accounting issues.

Contributor
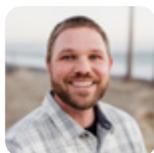
Matt MacLachlan
Partner, Financial Operations, Connor Group

About Our Supporter

Connor Group (Sponsor and Contributor)

Connor Group is a specialized professional services firm of Big 4 alumni and industry executives. Our team of highly experienced professionals helps financial and operation executives with their most complex and significant matters, including digital solutions, financial accounting and operations, IPO and M&A services, and managed services. Our clients are the world's top growth companies, and we support them as they change the world and create new markets!

connorgp.com   AI & Automation Landing Page

For additional questions, contact us at:

United States	**U.S. Virgin Islands**	**Email**
(650) 300-5101	(340) 643-5100	ai_automation@connorgp.com