MATURITY MODEL

GenAI Governance Framework Maturity Model

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

David A. Wood, PhD

Professor, Brigham Young University

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.

Table of Contents

Introduction 04

Strategic Alignment and Control Environment 06

Data and Compliance Management 08

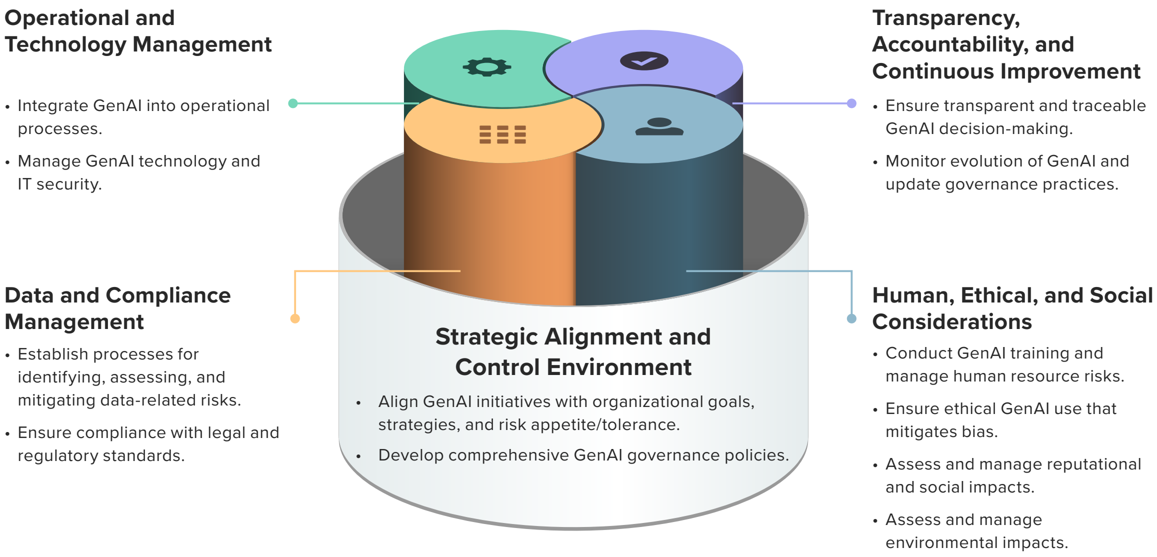
Operational and Technology Management 10

Human, Ethical, and Social Considerations 13

Transparency, Accountability, and Continuous Improvement 16

The GenAI Governance Framework shown in the image below and available at https://genai.global/, provides a comprehensive approach for helping organizations understand and manage the risks of generative AI (GenAI). As AI continues to evolve and integrate into various facets of business operations, the need for an effective governance framework becomes critical. This framework is designed to guide organizations through the complexities of AI risk management, offering a structured methodology to identify, assess, and mitigate potential risks.

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

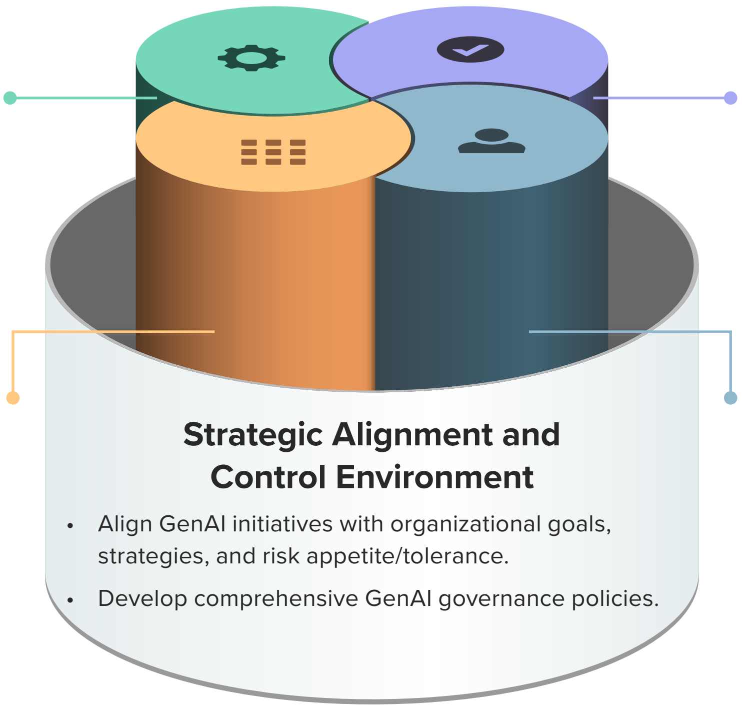
- Conduct GenAI training and manage human resource risks.
- Ensure ethical GenAI use that mitigates bias.
- Assess and manage reputational and social impacts.
- Assess and manage environmental impacts.

To enhance the utility of the GenAI Governance Framework, we developed a maturity model for each domain and the related control considerations outlined in the original document. This maturity model is a tool that enables organizations to evaluate their current governance practices, identify areas for improvement, and strategically plan for future enhancements. By assessing their maturity levels across various control considerations, organizations can gain insights into their strengths and weaknesses, thereby facilitating targeted actions to bolster their AI governance.

We also provide you with the ability to fill out the maturity model online and receive benchmarking data of how your organization compares to peer organizations. To do this, go to https://genai.global/ and follow the benchmarking instructions. As part of the survey, you will be able to decide what data is shared.

Overall, the GenAI Governance Framework and its accompanying maturity model serve as essential resources for organizations seeking to navigate the evolving landscape of AI. By adopting these tools, organizations can enhance their preparedness, resilience, and capability to harness the benefits of AI while effectively managing its risks.

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 overall goals and strategies of the organization. It involves setting the appetite and direction for GenAI use and establishing the control environment around GenAI use.	• 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 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 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

Maturity Model for Each Control Consideration

Strategic Alignment and Control Environment

Strategic and Planning Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
GenAI Risk Management Framework	Initial or no formal framework exists; ad-hoc processes in place.	Basic framework developed but not fully integrated with other frameworks or partially implemented.	Structured framework in place, mostly integrated with other governance frameworks.	Comprehensive, integrated framework fully aligned with other governance frameworks; fully implemented.
Strategic GenAI Roadmap	Limited or no strategic roadmap; AI initiatives are sporadic and not aligned with organizational goals.	Defined strategic roadmap with some level of organizational buy-in; partial alignment with goals.	Detailed strategic roadmap with significant organizational buy-in; largely aligned with organizational goals.	Comprehensive strategic roadmap with full organizational buy-in; fully aligned with organizational goals.
Regular Strategy Review	Irregular or no reviews of AI strategy; lack of adaptation to changes.	Regular reviews occur but may not fully influence AI strategy adjustments.	Frequent, structured reviews influencing AI strategy and adaptations.	Regular, comprehensive reviews that effectively influence AI strategy and alignment with organizational strategies.
Stakeholder Engagement	Minimal stakeholder involvement; lacks comprehensive engagement.	Some key stakeholders are engaged, but engagement may not be systematic or fully inclusive.	Broad stakeholder engagement with systematic approach, but room for more inclusivity.	Full stakeholder engagement across all levels; systematic and comprehensive approach.
Performance Monitoring	No defined metrics or KPIs for AI initiatives; no monitoring of AI capabilities.	Basic metrics and KPIs defined; some monitoring of AI capabilities without comprehensive analysis.	Established metrics and KPIs with regular monitoring of AI capabilities.	Comprehensive metrics and KPIs fully integrated into performance management; ongoing monitoring and adjustment of AI capabilities.
Contingency Planning	No contingency plans for AI projects; reactive approach to unexpected outcomes.	Basic contingency plans in place but may not cover all critical aspects or be fully tested.	Well-developed contingency plans, regularly reviewed and updated.	Detailed, tested contingency plans covering a wide range of scenarios; proactive management of unexpected outcomes.
Scenario Planning and Forecasting	No scenario planning; unprepared for potential events.	Scenario planning exists but may be limited in scope or detail; preparation for unexpected events is moderate.	Advanced scenario planning in place, preparing for a broad set of potential events.	Comprehensive scenario planning and forecasting; robust preparation for a wide range of potential events.

Maturity Model for Each Control Consideration

Strategic Alignment and Control Environment

Control Environment Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Policy Development and Governance	AI policies are nonexistent or very basic; lack of alignment with organizational risk appetite and strategy.	Basic AI governance and usage policies are developed but may not cover all necessary aspects or be fully aligned with risk appetite.	Detailed AI governance and usage policies in place, largely aligned with risk appetite and strategy.	Comprehensive AI governance and usage policies are fully developed, aligned with organizational risk appetite, strategy, and legal guidelines.
Clear Roles and Responsibilities	Roles and responsibilities for AI governance are unclear or not communicated.	Roles and responsibilities are defined but may not be widely communicated or understood.	Clear roles and responsibilities, with improved communication and understanding across the organization.	Clear roles and responsibilities are well-defined, communicated across the organization, and understood by all relevant stakeholders.
Establish AI Governance Committee	No formal governance committee for AI; lack of oversight.	An AI governance committee exists but may have limited representation or effectiveness.	AI governance committee established with broad representation, effectively overseeing AI governance.	An effective AI governance committee is established with broad representation, overseeing AI governance and policy implementation efficiently.
AI Inventory	Basic or nonexistent inventory of AI applications; informal tracking.	Initial formal inventory process; partial catalog of AI systems.	Comprehensive, structured inventory of AI systems; regularly updated.	Dynamic, integrated inventory management; leverages AI for tracking.
Regular Policy Review and Update	AI policies are seldom reviewed and updated; outdated policies.	AI policies are reviewed periodically, but updates may not be timely or fully reflective of new developments.	Regular, timely reviews and updates of AI policies reflecting new developments.	AI policies are regularly reviewed and updated to reflect the latest developments, insights, and best practices.
AI Ethics Framework	No ethics framework in place; ethical considerations are not systematically addressed in AI projects.	An AI ethics framework is in place but may not be fully integrated into decision-making processes.	Well-developed AI ethics framework, increasingly integrated into AI decision-making.	Well-developed AI ethics framework, increasingly integrated into AI decision-making.
Incident Response Plan	No incident response plan for AI-related issues; unstructured response to incidents.	A basic incident response plan exists, but it may not be comprehensive or fully tested.	A structured incident response plan is in place and periodically tested, covering most AI-related issues.	A comprehensive, tested incident response plan is in place, specifically addressing AI-related issues effectively and efficiently across all scenarios.

Data and Compliance Management

Data-Related Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Data Governance Framework	No formal data governance framework; ad-hoc management of data risks.	Basic data governance framework in place but may lack comprehensiveness or enforcement.	Structured and operational data governance framework in place, addressing most key data risks.	Comprehensive and fully implemented data governance framework addressing all key data risks.
Access Control Policies	Minimal or no access controls; widespread access to sensitive data.	Basic access control policies implemented but may not be strictly enforced or comprehensive.	Enhanced access control policies in place, more consistently enforced with improved data protection.	Strict access control policies fully enforced, with role-based access to sensitive data and tools.
Data Encryption and Anonymization	Lack of data encryption and anonymization; sensitive data exposed.	Some data encryption and anonymization practices in use, but not consistently applied.	Consistent application of data encryption and anonymization techniques to protect most sensitive information.	Advanced data encryption and anonymization techniques consistently applied to protect all sensitive information.
GenAI Data Lineage Tools	No use of data lineage tools; unclear how data is utilized within AI systems.	Limited use of data lineage tools; partial transparency in data usage.	Broad use of AI data lineage tools enhancing transparency in data utilization.	Comprehensive use of AI data lineage tools, ensuring full transparency in data utilization.
Regular Data Audits	Infrequent or no data audits; potential data integrity issues unaddressed.	Periodic data audits conducted but may not cover all critical areas or be fully systematic.	Frequent, more systematic data audits to ensure data integrity and security.	Regular, systematic data audits to ensure data integrity and security, addressing unauthorized access or breaches effectively.
Self-learning Models	No specific process for auditing or monitoring self-learning models; risks unmanaged.	Basic audit and monitoring processes for self-learning models but may lack depth or timeliness.	Established processes for auditing and monitoring self-learning models, with timely risk identification.	Robust audit and monitoring processes for self-learning models, addressing risks promptly and efficiently.

Data and Compliance Management

Legal and Regulatory Regime Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Documentation and Reporting Processes	Inconsistent or incomplete documentation and reporting; lacks transparency and complicates compliance efforts.	Basic documentation and reporting processes in place but may not be comprehensive or fully systematic.	Well-structured documentation and reporting processes enhancing transparency and compliance.	Thorough and systematic documentation and reporting processes ensure full transparency and facilitate compliance.
Compliance Monitoring System	No formal compliance monitoring system; reactive approach to compliance issues.	Basic compliance monitoring system exists but may not cover all relevant laws or be fully continuous.	Improved compliance monitoring system, more comprehensive and continuous.	Advanced, continuous compliance monitoring system fully covering all relevant laws and regulations.
AI Legal Risk Assessment	Legal risk assessments for AI are infrequent or not conducted; unrecognized legal risks.	Periodic legal risk assessments conducted but may not be thorough or proactive.	Frequent and detailed legal risk assessments, improving risk management.	Regular, comprehensive legal risk assessments ensure proactive management of legal risks in AI initiatives.
Monitoring and Training on Regulatory Changes	Infrequent or no updates on regulatory changes to staff; lack of awareness and training on AI regulations.	Some monitoring and training on regulatory changes, but not consistently applied across the organization.	Regular updates and training sessions, improving regulatory awareness and compliance.	Consistent monitoring and comprehensive training on regulatory changes ensure full staff awareness and compliance.
Cross-border Compliance Strategy	No strategy for managing cross-border compliance; risks in multinational operations are unaddressed.	Basic cross-border compliance strategies developed but may not be fully effective or comprehensive.	More effective cross-border compliance strategies in place, covering significant areas of operation.	Robust cross-border compliance strategies effectively manage compliance risks in all jurisdictions of operation.

Operational and Technology Management

Process Management Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Standard Operating Procedures (SOPs) for GenAI Use	No SOPs for AI use; AI applications deployed without clear guidelines or processes.	Basic SOPs developed but may not be fully comprehensive or consistently applied.	Detailed SOPs in place, generally followed with minor inconsistencies.	Comprehensive SOPs for AI use are developed, implemented, and consistently followed across all AI applications.
GenAI Performance Monitoring	AI performance is not monitored or is done sporadically; lack of insight into AI application effectiveness.	Periodic AI performance monitoring; limited systems in place for evaluation.	Consistent AI performance monitoring with substantial systems for evaluation.	Regular and systematic AI performance monitoring with advanced systems to evaluate effectiveness comprehensively.
Validation and Testing Protocols	Minimal or no validation and testing of AI applications; deployment without stakeholder approval.	Some validation and testing protocols exist but may not be rigorous or fully approved by stakeholders.	Validation and testing protocols well-established, with broad stakeholder approval.	Rigorous validation and testing protocols in place, with full stakeholder approval before AI deployment.
Change Management Procedures	No formal change management procedures for AI; significant operational disruptions during AI implementation.	Basic change management procedures in place but may not fully minimize operational disruptions.	Structured change management procedures minimizing operational disruptions.	Effective change management procedures developed and implemented to ensure minimal operational disruption during AI changes.

Operational and Technology Management

Technology Evaluation and Selection Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Technology Assessment Framework	No formal framework for assessing AI technologies; selections made without alignment to organizational goals.	Basic technology assessment framework in place but may lack depth or full alignment with organizational goals.	Detailed technology assessment framework in use, aligned with most organizational goals.	Comprehensive technology assessment framework developed and used for all AI technology selections, fully aligned with organizational goals and compliance requirements.
Vendor Risk Assessment	Minimal or no risk assessments conducted on vendors; lack of due diligence.	Some risk assessments of vendors performed, but not thorough or consistent.	Systematic risk assessments of vendors and their solutions, improving selection process.	Thorough and systematic risk assessments of all vendors and their AI solutions before implementation.
AI Feature Integration and Management Protocol	No established protocol for integrating and managing AI features; ad-hoc processes.	Basic protocol for AI feature integration exists but may not be comprehensive or fully systematic.	Established protocol for AI feature integration, with consistent management practices.	Robust protocol for vetting, integrating, and managing new AI features, including comprehensive assessment processes.
Post-Implementation Review	Post-implementation reviews are not conducted; no assessment of AI technology impact.	Occasional post-implementation reviews conducted but may lack depth or fail to capture full impact.	Frequent post-implementation reviews, capturing significant impacts and improvements.	Regular, thorough post-implementation reviews conducted to assess the effectiveness and impact of AI technology systematically.

Operational and Technology Management

Enhanced Operational and IT Security Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Robust IT Security Policies	Generic IT security policies not tailored to AI; significant policy gaps.	Basic IT security policies that somewhat address AI systems but may have gaps.	Strong IT security policies addressing AI specifics, with minor gaps.	Comprehensive and robust IT security policies specifically tailored to AI systems, covering all necessary aspects.
Data Security Training for Employees	Lack of data security training for employees involved in AI operations.	Some data security training provided, but not comprehensive or regular.	Regular data security training provided to most employees involved in AI.	Comprehensive data security training regularly provided to all employees involved in AI operations.
Incident Response and Recovery Plans	No incident response or recovery plans for AI system breaches or failures.	Basic incident response and recovery plans in place but may not be fully tested or comprehensive.	Structured incident response and recovery plans, regularly updated and tested.	Well-developed, tested incident response and recovery plans ready for any AI system breaches or failures.
Access Management and Authentication	Weak access management and authentication for AI systems.	Some strengthening of access management and authentication but may not cover all AI systems or connections.	Strong access management and authentication mechanisms, covering most AI systems and connections.	Strict access management and authentication mechanisms fully implemented for all AI systems and connections.
Continuous Monitoring of Security Threats	Sporadic or no monitoring of security threats; reactive threat response.	Periodic monitoring of security threats, but not fully continuous or proactive.	Continuous monitoring of most security threats, with proactive response strategies.	Continuous and proactive monitoring of security threats with immediate response capabilities, ensuring comprehensive threat management.

Human, Ethical, and Social Considerations

Knowledge and Training Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Communicate Data Currency	No communication on data currency in AI models.	Some communication on data currency, but inconsistent.	Regular, clear communication on the latest data in AI models.	Continuous and transparent communication ensuring users are informed of data currency.
Training Plan for Employees	No training on AI model use, weaknesses, or risks.	Basic training plan in place, covering some aspects.	Comprehensive training plan, covering most use, weaknesses, and risks.	Extensive and continuous training programs, thoroughly covering AI model use, weaknesses, and risks.

Human Resource and Employment Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Transparent Communication Strategy	Lack of communication on AI's job impact.	Some communication on AI's impact, not fully transparent.	Comprehensive communication strategy on AI's impact on jobs.	Continuous and fully transparent communication, effectively informing employees about AI's impact.
GenAI-related Job Creation Strategies	No identification of new AI-related job roles.	Efforts to identify AI-related job opportunities but limited.	Proactive identification and development of AI-related job roles.	Strategic and ongoing development of new AI-related job opportunities and career paths.
Employee Involvement in GenAI Implementation	Minimal employee involvement in AI design and implementation.	Limited employee involvement; some acceptance efforts.	Significant employee involvement in all AI design and implementation stages.	Full employee engagement and co-creation in AI projects, fostering deep understanding and acceptance.
Reskilling and Upskilling Programs	No reskilling or upskilling programs for AI integration.	Basic reskilling and upskilling programs available.	Comprehensive programs, widely accessible for reskilling/upskilling.	Continuous learning and development ecosystem supporting AI integration.
GenAI Integration Feedback Loops	No feedback mechanisms on AI integration.	Basic feedback mechanisms in place, underutilized.	Effective feedback mechanisms ensuring concerns and suggestions are addressed.	Dynamic and responsive feedback systems for continuous AI integration improvement.

Human, Ethical, and Social Considerations

Ethical and Bias Risks and Control Considerations

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Bias Detection and Mitigation Framework	No framework for identifying or mitigating biases.	Basic bias detection and mitigation framework in place.	Comprehensive framework for bias detection and mitigation integrated into AI development.	Advanced and proactive bias management practices, continuously updated.
Diverse Data	Lack of diversity in training data sets.	Efforts to diversify data sets, somewhat effective.	Extensive use of diverse data sets in AI training.	Strategic and systematic approach to data diversity, minimizing bias risks.
Regular Ethics Training	No ethics training for AI teams.	Periodic ethics training provided, covering basic topics.	Regular, comprehensive ethics training enhancing ethical considerations and bias awareness.	Continuous ethics education, fostering a culture of ethical AI use and development.
User Feedback Mechanisms	No mechanisms for collecting user feedback on AI.	Basic user feedback mechanisms in place, limited effectiveness.	Robust mechanisms for actively soliciting and addressing user feedback.	Integrated user feedback loops for continuous improvement and ethical alignment.
Third-Party Audits for Ethical Compliance	No ethical compliance review of third-party AI tools.	Some review of third-party AI tools for ethical compliance.	Systematic and thorough audits for ethical compliance of all AI tools.	Continuous and comprehensive ethical compliance verification, including third-party audits.

Reputation and Social Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
“Human-in-the-Middle” Policies	No human review policies for AI-generated content.	Policies for human review of sensitive AI content, inconsistently applied.	Comprehensive policies requiring human review before release of sensitive content.	Fully implemented and strictly enforced “Human-in-the-Middle” policies for all sensitive disclosures.
Reputation Response Team	No team or plan for responding to negative AI reactions.	A reputation response team exists, lacking training or clear plan.	A well-trained reputation response team with clear response protocols.	A proactive and dynamic reputation management team, ready for any scenarios.

Human, Ethical, and Social Considerations

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

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Governance Framework for Environmental, Social, and Governance Impact	No ESG framework adapted for AI.	Basic ESG framework in place, not fully tailored for AI.	Comprehensive ESG framework adapted for AI's impacts.	Advanced ESG management practices, fully integrated and leading industry standards.
Environmental Impact Assessments for GenAI	Environmental impacts of AI systems not assessed.	Some environmental impact assessments conducted, not comprehensive.	Thorough environmental impact assessments, including energy consumption and efforts to minimize footprints.	Systematic and ongoing environmental impact assessments, driving sustainability in AI development.
Social Impact Assessment for GenAI	No assessment of the social impacts of AI.	Basic assessment of social impacts, lacking depth.	Comprehensive social impact assessments, considering ethical and bias risks.	Proactive and detailed social impact evaluations, informing AI strategy and development.
Governance Impact Assessment for GenAI	No evaluation of AI's impact on governance and assurance functions.	Some evaluation of AI's impact on governance, not integrated into decision-making.	Thorough governance impact assessments, integrated into organizational decision-making.	Continuous governance impact analysis, shaping policy and strategy for AI.
Sustainable GenAI Development Practices	No adoption of sustainable practices in AI development.	Some sustainable practices adopted, inconsistently applied.	Strong commitment to sustainable AI development practices, consistently applied.	Leadership in sustainable AI development, setting benchmarks for environmental responsibility.
ESG Training for GenAI Teams	No ESG-specific training for AI teams.	Basic ESG training provided, not comprehensive.	Comprehensive ESG training for AI teams, regularly updated.	Advanced ESG training programs, embedding sustainability and ethics at the core of AI initiatives.

Transparency, Accountability, and Continuous Improvement

Transparency, Traceability, and Trust Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Gen AI Decision-Making Documentation	No documentation requirements for AI use.	Basic documentation requirements in place, somewhat adhered to.	Comprehensive documentation requirements, including audit trails.	Advanced documentation and accountability standards exceeding industry norms.
Traceability Protocols in GenAI Development	Traceability protocols not incorporated in AI development.	Some traceability protocols used, inconsistently applied.	Traceability protocols incorporated into all AI development phases.	Cutting-edge traceability protocols, setting standards for the industry.
Regular Reviews of GenAI Decision Processes	No regular reviews of AI decision processes.	Periodic reviews conducted, somewhat systematic.	Regular, thorough reviews ensuring continuous traceability.	Continuous and proactive reviews, embedding accountability in AI processes.
Stakeholder Reporting on GenAI Decisions	No mechanisms for reporting AI decision-making to stakeholders.	Basic reporting mechanisms established, somewhat satisfying transparency needs.	Robust reporting mechanisms, ensuring transparency and stakeholder trust.	Innovative reporting practices, leading transparency and engagement efforts.

Continuing Evolution of the Technology Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
Technology Evolution Monitoring Program	No formal program for monitoring technology evolution.	Basic monitoring program exists, capturing significant trends.	Comprehensive monitoring program, proactively identifying new risks and opportunities.	Industry-leading monitoring and adaptation strategies, influencing technology evolution.
Review and Update Governance Framework	Governance framework seldom reviewed.	Governance framework reviewed periodically, addressing some new risks.	Regularly reviewed and updated governance framework, reflecting technological advancements.	Dynamic and agile governance, continuously evolving with technological trends.
Innovation Labs and Pilot Programs	No innovation labs or pilot programs in place.	Innovation labs or pilot programs with limited scope.	Robust innovation labs, actively exploring and integrating new technologies.	Pioneering innovation practices, significantly shaping AI risk management and exploitation.

Transparency, Accountability, and Continuous Improvement

Miscellaneous Risks and High Conceptual or Hypothetical Risks

CONTROL CONSIDERATIONS	MATURITY NASCENT	MATURITY EMERGING	MATURITY ESTABLISHED	MATURITY LEADING
GenAI Awareness and Education Programs	No AI awareness or education programs in place.	Basic AI awareness and education programs available.	Comprehensive programs, addressing all aspects of AI use and risks.	Leading-edge AI education initiatives, shaping industry standards and public perception.
Abuse Prevention Mechanisms	No mechanisms to prevent AI technology misuse or abuse.	Some abuse prevention mechanisms in place, partially effective.	Robust abuse prevention mechanisms, effectively safeguarding against misuse.	Advanced and proactive abuse prevention strategies, setting benchmarks for AI security.
Rapid Response and Mitigation Teams	No rapid response teams for AI-related incidents.	Basic rapid response teams with some incident handling protocols.	Advanced teams with comprehensive protocols for quick and effective incident management.	Industry-leading rapid response and crisis management capabilities, exemplary in AI incident handling.
Stakeholder Engagement and Dialogue	Minimal engagement with stakeholders on AI-related issues.	Some stakeholder engagement initiatives, lacking depth.	Ongoing, comprehensive stakeholder engagement, addressing concerns and expectations.	Strategic and proactive stakeholder dialogue, shaping AI policies and perceptions.

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.

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 160 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.

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.

About Our Supporter

Boomi (Sponsor and Contributor)

Boomi powers the future of business with intelligent integration and automation. As a category-leading, global software as a service (SaaS) company, Boomi celebrates more than 20,000 global customers and a worldwide network of 800 partners. Organizations turn to Boomi's award-winning platform to connect their applications, data, and people to accelerate digital transformation. For more information, visit boomi.com.

boomi.com AI & Automation Landing Page