Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Strengthening Internal Control Practices in AI-Driven Multinational Companies: A Strategic Approach to Sustainable Business Operations

Mark Anthony L. Herradura
University of Perpetual Help System Dalta - Las Pinas City
herraduramarkanthony@gmail.com

Dr. Jessie F. Sergote
Rizal Technological University Pasig Campus
jcfriser@gmail.com

Publication Date: August 25, 2025 DOI: 10.5281/zenodo.17034255

Abstract

The rapid integration of Artificial Intelligence (AI) into multinational corporations has transformed decision-making, optimized operational processes, and enhanced productivity. However, AI also introduces emerging risks such as algorithmic bias, data privacy concerns, and operational vulnerabilities that may undermine corporate objectives if not properly managed.

This study aims to address the challenges namely the risks of algorithmic bias, data privacy issues, and operational vulnerabilities, by proposing the RAISE Strategic Control Framework, a structured approach that aligns internal control practices with the dynamic realities of AI-driven business environments. Specifically, it evaluates the framework's effectiveness, relevance, and applicability in multinational contexts.

This study employed an Explanatory Sequential Mixed Methods Design to evaluate the effectiveness, relevance, and applicability of the RAISE Strategic Control Framework in AI-driven multinational corporations. The respondents included 368 employees from Internal Audit, Compliance and Risk Management, Digital Infrastructure and IT, Finance and Accounting, and Operations and Business Process departments of multinational IT corporations operating in the Philippines. Senior leaders and decision-makers were also interviewed to provide strategic perspectives. Purposive sampling was used to ensure inclusion of participants with direct expertise in internal controls and AI integration. Data were collected through a validated survey questionnaire. Quantitative data were analyzed using descriptive and inferential statistics, while qualitative data underwent thematic analysis to explore challenges, best practices, and implications for corporate governance.

Findings reveal that implementing the RAISE framework strengthens organizational governance, enhances risk identification and mitigation, and fosters a culture of ethical AI use. Results also highlight its potential to serve as a strategic tool for sustainable business operations by bridging the gap between AI innovation and robust internal control systems.

The study concludes that integrating RAISE into corporate governance policies can enhance regulatory compliance, support organizational adaptation to AI transformation, and promote ethical AI practices. Future research directions include longitudinal assessments of RAISE implementation, cross-cultural evaluations of AI governance perceptions, and refinement of

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

human–AI collaboration models. The implications extend to policy formulation through harmonized AI governance standards and program development, including corporate training, certification initiatives, and cross-sector pilot projects to expand adaptability.

Keywords: *Artificial Intelligence, Internal Controls, Multinational Corporations, RAISE Strategic Control Framework, Corporate Governance, Risk Management, COSO*

INTRODUCTION

Every new development and organizational change come with associated risks. Proper management of these risks is essential to ensure that objectives and goals are met; thus, effective internal control must be in place to mitigate adverse effects. Internal controls are the bedrock of corporate governance and resilience, enabling organizations to protect assets, comply with regulations, practice ethical values, and remain credible entities. In contrast, the absence of a strong internal control system exposes organizations to financial losses, operational disruptions, penalties, fines, and reputational damage (COSO, 2023).

Recently, Artificial Intelligence (AI) has been embedded in nearly every aspect of business activities and corporate functions due to its evident capabilities and advantages. AI technologies now automate tasks, processes, supply chains, and customer interactions, contributing to operational efficiency and helping companies remain competitive in today's fast-changing business environment. However, while AI provides wide opportunities, it also introduces new layers of complexity and risk. These concerns include algorithmic bias, lack of transparency, cybersecurity threats, and the compromised security of personal data (Gartner, 2022; PwC, 2021).

Because of these challenges, there is a need to revisit internal control systems. Traditional methods may not work effectively in AI-driven contexts, and re-evaluation is necessary to ensure risks are properly managed. This gap between conventional controls and emerging AI-related risks highlights the need for new strategies. Reports show that more than 60% of corporate leaders admit to deficiencies in their AI risk management frameworks, with algorithmic bias, lack of transparency, and weak cybersecurity cited as major concerns (Deloitte, 2023; KPMG, 2023). In the Philippines, this study is anchored on legislations such as the Data Privacy Act of 2012 (Republic Act No. 10173) and the E-Commerce Act of 2000 (Republic Act No. 8792), which emphasize the importance of responsible data processing, digital accountability, and security in business operations.

The objective of this study is therefore to ascertain how internal control practices in AI-driven environments can be reoriented or streamlined to achieve sustainable business operations. It further aims to offer organizations strategic models for adapting internal controls in light of new AI-driven technologies, with the goal of minimizing risks and ensuring sustainable organizational performance.

1. How do the respondents assess the effectiveness of internal controls in their respective organizations based on the five components of the COSO framework;

    1.1 Control Environment

    1.2 Risk Assessment

    1.3 Control Activities

    1.4 Information and Communication

    1.5 Monitoring Activities

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

2. Is there a significant difference in the assessment of internal control components (Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring Activities) when respondents are grouped according to their demographic profile?

3. How do respondents describe their organization's current internal control processes in relation to the COSO Framework's five components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities?

4. Considering the COSO Framework's five components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities), how do the respondents describe the influence brought by the adoption of AI on their internal control processes? Which components have shown the greatest improvements, and what potential risks or vulnerabilities has AI introduced.

5. What primary challenges do respondents indicate their organizations face when integrating AI into internal controls and business processes? Among the COSO Framework's five components, Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities, which are perceived to present the most significant difficulties? How do organizations typically address and overcome these challenges?

6. Based on the results of the study, what strategic control framework may be developed to strengthen internal control effectiveness and ensure sustainable business operations in AI-driven multinational corporations?

MATERIALS AND METHODS

Research Design

The study adopted a mixed-methods explanatory sequential design. This framework allowed for a comprehensive understanding of how internal controls can be strategically strengthened within multinational IT corporations operating in the Philippines to support sustainable business operations. Quantitative data collection and analysis preceded the qualitative phase to provide deeper insights into AI-driven internal control practices.

Participants

The study involved a purposive sample of 368 employees from the Philippine operations of Company A, Company B, and Company C, representing departments such as Internal Audit, Compliance and Risk Management, Digital Infrastructure and IT, Finance and Accounting, and Operations and Business Process. Inclusion criteria required participants to be regular employees, rank-and-file or managerial staff, with at least six (6) months of service. Excluded were interns, contractors, or employees on leave. For the qualitative phase, senior leaders and decision-makers (Directors, VPs, Senior Managers) were interviewed based on their oversight of internal controls, risk management, IT governance, or AI initiatives. They were required to have at least three (3) years of leadership experience and provide informed consent for a semi-structured 30–60 minute interview.

Instruments

Data were collected using a self-constructed survey questionnaire anchored in the COSO Internal Control–Integrated Framework, covering five components: Control Environment, Risk Assessment,

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Control Activities, Information and Communication, and Monitoring. The tool included the assessment of internal control practices. A 4-point Likert scale (1 = Strongly Disagree to 4 = Strongly Agree) measured perceptions of internal control effectiveness. The instrument underwent validation by a panel of experts (two academicians and three industry practitioners in IT audit, governance, and finance) using the Delphi method. Items rated below 3.50. Reliability testing using Cronbach's alpha (0.96) confirmed excellent internal consistency. A pilot test with 20 professionals refined clarity and structure. In addition, semi-structured interviews were conducted with selected leaders to explore AI-related challenges, compliance strategies, governance practices, and sustainability integration. Secondary sources such as corporate governance reports, sustainability disclosures, and audit committee charters were also analyzed.

Procedure

Quantitative data were gathered through an online survey distributed via corporate email and professional networks using Google Forms. Respondents provided informed consent before participation. After screening for completeness, responses were encoded and statistically analyzed. For the qualitative phase, purposively selected leaders were interviewed to provide contextual insights. Each interview lasted 30–60 minutes and focused on AI adoption in internal controls, risk mitigation, and sustainability objectives. Approvals were obtained from company management prior to interviews. Ethical standards were strictly observed. Participants were informed that participation was voluntary and had no effect on employment. Confidentiality was ensured by anonymizing data, coding responses, and storing files securely in compliance with the Philippine Data Privacy Act of 2012 (RA 10173). Ethical clearance was secured from the university research ethics committee and organizational approval was obtained from the subject companies.

Data Analysis

Quantitative data were analyzed using descriptive and inferential statistics. Tools included weighted mean and ranking (internal control effectiveness), standard deviation (response consistency), independent samples t-test (sex, civil status, position), one-way ANOVA (age, education, company, length of service), and Tukey's HSD post hoc test (group differences). Levene's Test was applied to check equality of variances. Reliability of scales was assessed with Cronbach's alpha. Qualitative data from interviews were subjected to thematic analysis to identify recurring patterns, challenges, and best practices in AI-driven internal control systems. Triangulation of survey, interview, and secondary data ensured validity and richness of findings.

RESULT

.

Table 1

Table on Assessment of Internal Control Effectiveness

Indicators	Mean	Verbal Interpretation	Rank
1. Control Environment	3.65	Strongly Agree	1
2. Risk Assessment	3.53	Strongly Agree	2
3. Control Activities	3.35	Agree	4.5

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

4. Information & Communication	3.48	Agree	3
5. Monitoring Activities	3.35	Agree	4.5
Composite Mean	**3.47**	**Agree**	

LEGEND: STRONGLY AGREE/Highly Effective (4) =3.51-4.0); AGREE/Effective (3) =2.51-3.50); DISAGREE/Slightly Effective (2) =1.51-2.50); STRONGLY DISAGREE/Not Effective at All (1) =1.0-1.50)

Table 1 presents the assessment of internal control effectiveness across its five components: control environment, risk assessment, control activities, information and communication, and monitoring activities. It is noted that among the components, Control Environment received the highest mean of 3.65, interpreted as *strongly agree*, and ranked first. This suggests that ethical leadership, well-defined governance structures, and a clear code of conduct are the strongest aspects of the organization's internal control framework. Hence, Control Activities and Monitoring Activities both have the lowest mean of 3.35 (*agree*), tied for fourth place. These scores suggest that while policies, procedures, and monitoring systems are in place and functioning effectively, they are perceived to be less robust compared to other components. Improvements in fraud/error prevention mechanisms, segregation of duties, and more frequent evaluation of AI-integrated processes could elevate their effectiveness.

.

Table 2

Significant Difference in the Assessment of Internal Control Components as to Sex

INDICATORS	SEX	MEAN	SD	T-VALUE	SIG VALUE	DECISION ON HO	INTERPRETATION
1. Control Environment	Male	3.66	0.36	0.76	0.38	Accept	Not Significant
	Female	3.64	0.38				
2. Risk Assessment	Male	3.53	0.39	22.87	0.00	Reject	Significant
	Female	3.53	0.44				
3. Control Activities	Male	3.33	0.37	11.20	0.00	Reject	Significant
	Female	3.38	0.43				
4. Information and Communication	Male	3.57	0.37	1.95	0.16	Accept	Not Significant
	Female	3.43	0.40				
5. Monitoring Activities	Male	3.27	0.40	4.64	0.03	Reject	Significant
	Female	3.40	0.43				
OVERALL	Male	3.47	0.30	**29.94**	**0.00**	**Reject**	**Significant**
	Female	3.48	0.38				

@.05 Level of significance

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Table 2 presents the significant difference in the assessment of internal control components when grouped according to sex. The overall assessment (Male: M = 3.47, SD = 0.30; Female: M = 3.47, SD = 0.38), with 29.94 T-value result and a significance value of 0.00, which is less than 0.05, means that there is an overall significant difference between male and female respondents' perceptions of internal control effectiveness. This implies that sex is a contributing factor in shaping respondents' views on risk assessment, control activities, and monitoring activities, even though the mean values are relatively close.

Table 3

Post Hoc Test on Significant Difference in the Assessment of Internal Control Components as to Age

INDICATORS	AGE	18-25 Years Old	25-35 Years Old	36-45 Years Old	46-55 Years Old
1. Control Environment	18-25 Years Old			*	
	26-35 Years Old				
	36-45 Years Old				
	46-55 Years Old				
2. Risk Assessment	18-25 Years Old		*		*
	26-35 Years Old				
	36-45 Years Old				
	46-55 Years Old				
4. Information and Communication	18-25 Years Old				
	26-35 Years Old			*	
	36-45 Years Old				
	46-55 Years Old			*	
5. Monitoring Activities	18-25 Years Old				
	26-35 Years Old			*	*
	36-45 Years Old				
	46-55 Years Old				

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

@.05 Level of significance

Table 3 presents the results of the Post Hoc Test identifying which specific age groups differ significantly in their assessment of internal control components. The findings further elaborate on the significant differences identified in Table 3. For Control Environment, a significant difference exists between respondents aged 18-25 years old and 36-45 years old. For Risk Assessment, significant differences were observed between 18-25 years old and 26-35 years old, and between 18-25 years old and 46-55 years old. For Information and Communication, significant differences were noted between 26-35 years old and 36-45 years old, as well as between 46-55 years old and 36-45 years old. This may reflect variations in communication preferences, access to information, or trust in communication channels among different age groups. For Monitoring Activities, significant differences exist between 26-35 years old and 36-45 years old, and between 26-35 years old and 46-55 years old. This could imply that perceptions of oversight, auditing, and monitoring systems differ between younger mid-career employees and those in more senior career stages, possibly due to differences in involvement with audit processes and system evaluations.

Table 4 presents the significant difference in the assessment of internal control components when respondents are grouped according to civil status. The overall assessment (Single: M = 3.45, SD = 0.36; Married: M = 3.50, SD not specified) has a 12.24 T-value and a significance value of 0.00, which is less than 0.05, leading to the rejection of the null hypothesis. This indicates that there is an overall significant difference in the perception of internal control effectiveness when grouped according to civil status.

Table 4

Significant Difference in the Assessment of Internal Control Components as to Civil Status

INDICATORS	CIVIL STATUS	MEAN	SD	T-VALUE	SIG VALUE	DECISION ON HO	INTERPRETATION
1. Control Environment	Single	3.60	0.38	0.88	0.35	Accept	Not Significant
	Married	3.75	0.34				
2. Risk Assessment	Single	3.48	0.43	7.40	0.01	Reject	Significant
	Married	3.63	0.39				
3. Control Activities	Single	3.37	0.42	5.52	0.02	Reject	Significant
	Married	3.35	0.40				
4. Information and Communication	Single	3.46	0.40	1.84	0.18	Accept	Not Significant
	Married	3.53	0.38				
5. Monitoring Activities	Single	3.36	0.42	2.63	0.11	Accept	Not Significant
	Married	3.32	0.44				
	Single	**3.45**	**0.36**	**12.24**	**0.00**	**Reject**	

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

OVERALL	**Married**	**3.52**	**0.32**				**Significant**

@.05 Level of significance

Table 5

Significant Difference in the Assessment of Internal Control Components as to Educational Attainment

INDICATORS	MEAN	SD	F-VALUE	SIG VALUE	DECISION ON HO	INTERPRETATION
1. Control Environment	3.65	0.37	9.81	0.00	Reject	Significant
2. Risk Assessment	3.53	0.42	9.62	0.00	Reject	Significant
3. Control Activities	3.36	0.41	1.50	0.23	Accept	Not Significant
4. Information and Communication	3.48	0.39	1.39	0.25	Accept	Not Significant
5. Monitoring Activities	3.35	0.42	1.08	0.34	Accept	Not Significant
OVERALL	**3.48**	**0.35**	**4.58**	**0.01**	**Reject**	**Significant**

@.05 Level of significance

Table 5 presents the significant difference in the assessment of internal control components when respondents are grouped according to their educational attainment. The overall mean score of 3.48 ($p = 0.01$) shows a significance value less than 0.05, meaning there is an overall significant difference in internal control assessments when grouped by educational attainment. This indicates that while perceptions of certain operational aspects are similar, differences in views on governance and risk management contribute to varying overall evaluations.

Table 6

Significant Difference in the Assessment of Internal Control Components as to Company Affiliation

INDICATORS	Company	MEAN	SD	F-VALUE	SIG VALUE	DECISION ON HO	INTERPRETATION
	Company A	3.65	.37	14.30	.000	Reject	Significant

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

1. Control Environment	Company B	3.54	.41				
	Company C	3.87	.19				
	Total	3.65	.37				
2. Risk Assessment	Company A	3.44	.40	23.80	.000	Reject	Significant
	Company B	3.55	.46				
	Company C	3.87	.23				
	Total	3.53	.42				
3. Control Activities	Company A	3.24	.35	27.87	.000	Reject	Significant
	Company B	3.45	.42				
	Company C	3.66	.44				
	Total	3.36	.41				
4. Information and Communication	Company A	3.42	.38	27.30	.000	Reject	Significant
	Company B	3.43	.39				
	Company C	3.83	.22				
	Total	3.48	.39				
5. Monitoring Activities	Company A	3.18	.35	56.83	.000	Reject	Significant
	Company B	3.52	.44				
	Company C	3.70	.28				
	Total	3.35	.42				
OVERALL	Company A	3.39	.30	31.60	.000	Reject	Significant
	Company B	3.50	.41				
	Company C	3.79	.23				
	Total	3.48	.35				

@.05 Level of significance

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Table 6 presents the significant difference in the assessment of internal control components when respondents are grouped according to company affiliation. The results indicate that for all five components, Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities, the computed significance values are 0.000, all less than the 0.05 alpha level. This leads to the rejection of the null hypothesis for each component, indicating significant differences in the assessments across the three companies.

Table 7

Significant Difference in the Assessment of Internal Control Components as to Position

INDICATORS	POSITION	MEAN	SD	T-VALUE	SIG VALUE	DECISION ON HO	INTERPRETATION
1. Control Environment	Staff / Rank-and-File	3.61	0.40	17.81	0.00	Reject	Significant
	Supervisor / Line Manager / Middle Manager	3.71	0.31				
2. Risk Assessment	Staff / Rank-and-File	3.51	0.42	2.14	0.15	Accept	Not Significant
	Supervisor / Line Manager / Middle Manager	3.56	0.44				
3. Control Activities	Staff / Rank-and-File	3.34	0.40	2.72	0.10	Accept	Not Significant
	Supervisor / Line Manager / Middle Manager	3.39	0.43				
4. Information and Communication	Staff / Rank-and-File	3.45	0.37	10.23	0.00	Reject	Significant
	Supervisor / Line Manager / Middle Manager	3.53	0.42				

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

5. Monitoring Activities	Staff / Rank-and-File	3.30	0.41	2.51	0.11	Accept	Not Significant
	Supervisor / Line Manager / Middle Manager	3.42	0.44				
OVERALL	Staff / Rank-and-File	3.45	0.35	0.02	0.90	Accept	Not Significant
	Supervisor / Line Manager / Middle Manager	3.52	0.34				

@.05 Level of significance

Table 7 presents the significant difference in the assessment of internal control components when respondents are grouped according to their position in the company staff/rank-and-file and supervisor/line manager/middle manager. The overall assessment (Staff: M = 3.45, SD = 0.35; Supervisors/Managers: M = 3.52, SD = 0.34) has a significance value of 0.90, far above the 0.05 threshold, indicating no significant difference in overall internal control perceptions between the two position levels.

Table 8
Post Hoc Test on Significant Difference in the Assessment of Internal Control Components as to Length of Service

INDICATORS	**Length of Service**	1-3 Years	4-6 Years	7-10 Years
1. Control Environment	1-3 Years			
	4-6 Years			*

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

	7-10 Years			

@.05 Level of significance

Table 8 presents the results of the Post Hoc Test to determine which specific length-of-service groups differ significantly in their assessment of internal control components. This table elaborates on the significant difference found in Control Environment component. The results show that a significant difference exists between employees with 4-6 years of service and those with 7-10 years of service. This suggests that perceptions of the organization's control environment covering leadership integrity, ethical climate, and governance structure vary notably between mid-tenure and long-tenure employees.

Table 9 shows that most respondents (n=5) described a strong control environment, attributing this to leadership's commitment to ethics and compliance. Risk assessment (n=4) was frequently enhanced by the use of analytics, predictive tools, and scheduled reviews. Control activities (n=3) were mainly discussed by IT respondents, who emphasized embedded and automated measures. Information and communication processes (n=3) were characterized by secure and structured channels, while monitoring activities (n=4) relied on continuous audits, real-time dashboards, and follow-up mechanisms.

Table 9

Thematic Summary of Respondents' Descriptions of

Current Internal Control Processes

Theme / COSO Component	Responses Across Key Informants	Number of Respondents (n)
Control Environment	Strong ethical culture and leadership support (KI1, KI2, KI3, KI5, KI6). "Leadership mismo yung nagse-set ng tone for ethical practices" (KI1). Company B notes a "clear code of conduct and top management commitment" (KI3), Company C highlights "integrity and accountability" (KI5).	5
Risk Assessment	Use of analytics, predictive tools, and regular risk reviews (KI1, KI3, KI4, KI5). Company A uses "analytics at regular workshops" (KI1), Company B conducts "formal risk reviews" (KI3), Company C holds "quarterly and annual reviews" (KI5).	4

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Control Activities	Embedded and automated controls in workflows (KI2, KI4, KI6). Includes "role-based access control" (KI2), "automated change management" (KI4), "strict access control and encryption" (KI6).	3
Information & Communication	Well-established, secure channels for timely updates (KI1, KI3, KI5). Company A uses "local and global channels" (KI1), Company B ensures "transparent process" (KI3), Company C applies "upward and downward communication" (KI5).	3
Monitoring Activities	Continuous monitoring through audits, dashboards, and follow-ups (KI1, KI4, KI5, KI6). Company A has "continuous audit cycles" (KI1), Company B uses "real-time dashboards" (KI4), Company C has "follow-up mechanisms" (KI5).	4

Legend: KI = Key Informant: KI1 – Internal Audit and KI2 – IT from Company A, KI3 – Internal Audit and KI4 – IT from Company B, KI5 – Internal Audit and KI6 – IT from Company C

Table 10

Thematic Summary of Respondents' Views on AI Influence

Theme / COSO Component	Responses Across Key Informants	Number of Respondents (n)
Control Environment	AI adoption requires cultural adaptation and user trust (KI1, KI5). "Kailangan baguhin ang mindset ng tao kasi may fear na AI will replace them" (KI5).	2
Risk Assessment	Improved anomaly detection and predictive capabilities (KI1, KI2, KI3, KI5, KI6). "Mas mabilis naming ma-identify ang anomalies kasi automated na ang data analysis" (KI1).	5

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Control Activities	AI enables automation of compliance checks and system monitoring (KI2, KI4, KI5, KI6). "AI automates compliance checks and detects irregularities early" (KI2).	4
Information & Communication	Need for accurate interpretation of AI-generated reports (KI3, KI4). "Kailangan ma-interpret ng tama ang AI reports para hindi mag-lead sa wrong decisions" (KI3).	2
Monitoring Activities	Real-time monitoring and predictive alerts (KI1, KI2, KI3, KI4, KI6). "Nag-level up yung monitoring... predictive alerts na ngayon" (KI3).	5

Legend: KI = Key Informant: KI1 – Internal Audit and KI2 – IT from Company A, KI3 – Internal Audit and KI4 – IT from Company B, KI5 – Internal Audit and KI6 – IT from Company C

Table 10 shows AI adoption most strongly impacted risk assessment and monitoring activities (n=5 each), enabling faster anomaly detection, predictive alerts, and automated analysis. Control activities (n=4) also benefited from automation features. However, the control environment (n=2) and information and communication (n=2) highlighted adaptation challenges, including user trust in AI outputs and correct interpretation of AI-generated reports. Respondents emphasized the need for training, human oversight, and secure implementation.

Table 11

Thematic Summary of Respondents' Views on AI Integration Challenges

Theme / COSO Component	Responses Across Key Informants	Number of Respondents (n)
Control Environment	Resistance to change and trust issues with AI outputs (KI1, KI3, KI4, KI5, KI6). "Not everyone is ready to trust AI outputs" (KI1). Company B respondents note a "cultural shift" is needed (KI4), while Company C highlights that "leadership buy-in is essential" (KI6).	5

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Risk Assessment	AI models sometimes generate false positives requiring human verification (KI1, KI5). "AI can flag too many false positives" (KI5).	2
Control Activities	Difficulty in embedding AI into existing workflows and legacy systems (KI1, KI2, KI5, KI6). "Integrating AI into legacy systems is complex" (KI2). Company C noted "AI workflows require adaptation and redefinition of processes" (KI5).	4
Information & Communication	Need to clearly explain AI findings to non-technical users (KI4). "Kailangan maipaliwanag clearly ang AI findings" (KI4).	1
Monitoring Activities	While AI aids monitoring, embedding it into the control environment still requires leadership support (KI6). "Integration sa control environment is harder kasi kailangan ng buy-in from leadership" (KI6).	1

Legend: KI = Key Informant: KI1 – Internal Audit and KI2 – IT from Company A, KI3 – Internal Audit and KI4 – IT from Company B, KI5 – Internal Audit and KI6 – IT from Company C

Table 11 shows that the control environment emerged as the most challenging component (n=5), with respondents citing organizational resistance, trust issues with AI outputs, and the need for leadership endorsement. Control activities followed closely (n=4), where integration with legacy systems, adaptation of existing workflows, and redesigning procedures for AI compatibility posed significant obstacles. Fewer respondents identified risk assessment (n=2) as a major challenge, mainly due to false positives in AI detection. Information and communication (n=1) and monitoring activities (n=1) were the least cited, with concerns centering on interpretation of AI reports and leadership buy-in. To address these issues, organizations implement training programs, phased rollouts, pilot projects, and blended human AI decision-making processes.

DISCUSSIONS

The focus of this study is to assess the effectiveness of internal control practices in AI-driven multinational corporations and to examine how demographic and organizational factors influence perceptions of control effectiveness. The findings provide insights into strengths and gaps across COSO's five components such as control environment, risk assessment, control activities, information and communication, and monitoring activities, and highlight how differences in sex, age, civil status, education, company affiliation, position, and length of service shape employee assessments.

As shown in Table 1, respondents generally agreed that internal controls are effective, with the strongest emphasis on the control environment and risk assessment. This means that organizations demonstrate strong ethical leadership, governance structures, and proactive risk identification practices, consistent with COSO's (2023) framework, which identifies these elements as foundational. However, lower ratings in

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

control activities, monitoring, and communication highlight areas needing reinforcement, particularly in fraud prevention, oversight of AI-driven processes, and transparency in reporting.

Table 2 exhibits that sex is a contributing factor in shaping respondents' views on risk assessment, control activities, and monitoring activities, even though the mean values are relatively close. This result aligns with studies such as that of Nurlia et al. (2023), which found that demographic variables like sex can influence risk perception and engagement in control activities, often due to differences in professional roles, experiences, and interaction with organizational processes. However, the absence of significant differences in the control environment and communication components may indicate that these aspects are well-established and consistently perceived across genders, as supported by Uddin (2023), who noted that strong ethical culture and transparent communication tend to elicit uniform responses regardless of demographic differences. Uddin further emphasized that transparency in ethical leadership, particularly through clear communication of decisions, reinforces organizational trust and ethical behavior. In conclusion, Table 2 reveals that while male and female respondents share similar views on the control environment and information/communication processes, significant differences exist in their assessment of risk assessment, control activities, and monitoring activities. This finding underscores the importance of considering demographic perspectives when evaluating internal control systems to ensure inclusivity and balanced policy implementation.

The post hoc analysis reveals that the observed significant differences in Table 3 are not evenly distributed across all age groups but are concentrated in specific pairwise comparisons. These results support the notion that career stage and organizational tenure influence how employees perceive various aspects of internal control. Consistent with North (2022), age and tenure impact workplace dynamics and perceptions of fairness, suggesting that older employees may perceive governance and control processes through a different lens, shaped by their accumulated experiences and organizational context.

Table 4 indicates that there is an overall significant difference in the perception of internal control effectiveness when grouped according to civil status. These findings are consistent with the observations of Gulan and Aguiling (2022), who noted that employees' perceptions of their organizational environment, which may be influenced by their civil status and life situation, can affect their career intentions and adaptability to workplace changes. However, the absence of significant differences in the control environment, communication, and monitoring suggests that these areas are well-established and uniformly implemented, leading to consistent perceptions across civil status groups. Thus Table 4 reveals that while single and married respondents share similar views on the control environment, information and communication, and monitoring activities, their assessments significantly differ in risk assessment, control activities, and in the overall evaluation of internal control effectiveness. This indicates the importance of considering civil status as a demographic factor that may influence certain aspects of internal control perception.

As indicated in Table 5 educational attainment influences how respondents perceive the control environment and risk assessment processes, leading to overall differences in internal control evaluations. However, operational, communication, and monitoring practices appear to be uniformly understood and implemented across all educational backgrounds.

Table 6 shows that company affiliation significantly influences perceptions of internal control effectiveness across all components. Company C consistently received the highest ratings, suggesting that its internal control practices, particularly in AI-related processes, are perceived as more robust compared to Company A and Company B. These findings highlight the need for benchmarking and knowledge-sharing among companies to improve consistency in internal control implementation and perception.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

As presented Table 7 demonstrates that while staff and supervisors/managers generally share similar overall views on internal control effectiveness, differences emerge in the control environment and communication components, with supervisors/managers rating these areas more positively. This highlights the importance of fostering greater transparency and engagement among rank-and-file employees to align perceptions across organizational levels.

Table 8 indicates that differences in perception of the control environment are primarily between employees with 4-6 years of service and those with 7-10 years, suggesting that tenure influences how governance and leadership integrity are evaluated. This finding aligns with the observations of Ahmad et al. (2021), who noted that longer tenure tends to enhance perceptions of empowerment and trust in leadership, suggesting that established employees may assess governance and control effectiveness based on accumulated experiences rather than recent developments. The variation in ratings between these two groups highlights the importance of maintaining consistent ethical practices and communication strategies that resonate with both mid-tenured and veteran employees. Thus, addressing potential perception gaps through continuous engagement and transparent leadership practices could help harmonize views across tenure groups.

As shown in Table 9, respondents described their organizations' internal control processes as generally strong across the COSO framework. The control environment stood out as the most emphasized, with leadership setting the ethical tone, one key informant noted that "*leadership mismo yung nagse-set ng tone for ethical practices*" (KI1), underscoring top management's role in fostering integrity. Risk assessment was enhanced through analytics, predictive tools, and scheduled reviews, while control activities were reinforced by automated measures such as role-based access controls. Information and communication were supported by secure and transparent channels, ensuring timely updates across levels. Monitoring relied on continuous audits, dashboards, and follow-up mechanisms. Overall, these accounts suggest that strong ethical leadership, coupled with technology-driven practices, anchors the effectiveness of internal controls in AI-driven environments.

Table 10 highlights that AI adoption has the most significant influence on *risk assessment* and *monitoring activities*. Respondents noted that AI-driven tools improved anomaly detection, predictive alerts, and automated analysis, making these processes faster and more proactive. As one internal auditor explained, *"Mas mabilis naming ma-identify ang anomalies kasi automated na ang data analysis"* (KI1), showing how AI strengthens risk detection and response. Similarly, monitoring activities were seen to have "leveled up" through real-time dashboards and predictive alerts (KI3), ensuring more dynamic oversight. Control activities also benefited, with automation streamlining compliance checks and irregularity detection (KI2). However, fewer respondents highlighted the control environment and information and communication. Challenges emerged around cultural adaptation—such as employee fears of AI replacing jobs (KI5)—and the need for accurate interpretation of AI-generated reports (KI3). These findings suggest that while AI enhances efficiency and strengthens certain COSO components, its effectiveness depends on user trust, proper training, and human oversight to mitigate risks of misinterpretation and resistance to adoption.

As shown in Table 11, the most common challenge in AI integration lies in the control environment, where resistance to change and trust issues with AI outputs were most evident. One respondent noted, "Not everyone is ready to trust AI outputs" (KI1), reflecting the need for stronger cultural adaptation and leadership support. These concerns parallel Alsawalhah et al. (2024), who warned that while AI adoption improves transparency and oversight, it introduces governance risks tied to model reliability and stakeholder trust. Beyond cultural barriers, control activities also posed difficulties, particularly in integrating AI into legacy systems and adapting workflows, echoing Rane et al.'s (2024) observation that modifying existing processes creates significant operational challenges. Risk assessment was likewise affected by false positives that demanded human verification, underscoring the need for continued human

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

oversight. Monitoring activities were least cited, though still dependent on leadership buy-in. These findings indicate that while AI strengthens internal controls, its success relies on cultural readiness, leadership endorsement, and hybrid human–AI decision-making.

Conclusion

Based on the analysis of both quantitative and qualitative findings, several conclusions were drawn regarding the effectiveness of internal control components in AI-integrated business processes among the selected multinational IT corporations in the Philippines.

1. The overall internal control environment within these organizations is strong, with leadership playing a central role in fostering an ethical culture, integrity, and accountability. Ethical principles are well-embedded and supported by clear governance structures, setting a solid foundation for AI-enabled operations.
2. Risk assessment processes are robust, particularly in the use of analytics, predictive tools, and scheduled reviews to identify and manage AI-related risks. While proactive measures are evident, fostering greater employee participation in risk reporting could further strengthen these mechanisms.
3. Control activities are adequately implemented but remain an area for improvement. Although policies and procedures for AI operations are in place, enhancements in fraud prevention, misuse detection, and integration of AI into legacy workflows are necessary to fully optimize operational safeguards.
4. Information and communication systems effectively support AI oversight and internal control functions, yet there is a need to improve clarity and accessibility of reporting channels. Strengthening feedback loops and ensuring accurate interpretation of AI-generated outputs will help address both operational and cultural challenges.
5. Monitoring activities, while functional, are the least developed among the five COSO components. Although continuous auditing, dashboards, and follow-ups are employed, more structured and comprehensive evaluation frameworks are required to ensure consistent oversight of AI-integrated processes.
6. AI adoption has significantly enhanced technical capabilities in risk assessment, monitoring, and compliance automation. However, cultural adaptation, trust-building, and leadership endorsement remain crucial in maximizing AI's benefits. Addressing these human factors, alongside technical integration, will be vital for achieving sustainable, resilient, and adaptive internal control systems in AI-driven business environments.

Recommendations

In light of the study's findings and conclusions, the following recommendations are proposed to strengthen the effectiveness of internal controls in AI-integrated business processes for multinational IT corporations:

Strengthen Ethical Leadership and Cultural Adaptation

- Continue fostering a strong ethical culture by ensuring top management visibly demonstrates commitment to integrity and accountability in AI deployment.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

- Conduct regular leadership-led communication and training programs to address resistance to change and build trust in AI-generated outputs.
- Integrate AI ethics modules into corporate values orientation and leadership development programs to align employee mindset with technological advancements.

Enhance Employee Engagement in Risk Reporting

- Implement structured channels and incentive systems for bottom-up risk reporting to capture emerging AI-related threats from all levels of the organization.
- Conduct regular workshops and simulation exercises to improve staff capability in identifying and communicating potential AI-related risks.

Improve Preventive and Detective Control Activities

- Upgrade AI-integrated fraud detection systems and anomaly prevention mechanisms to address the identified gaps in preventive controls.
- Prioritize the modernization of legacy systems to enable seamless AI integration and ensure that automated controls operate effectively.
- Establish cross-functional AI governance teams to monitor compliance and continuously refine control procedures.

Strengthen Information and Communication Channels

- Develop simplified and user-friendly AI reporting formats to make insights accessible to non-technical users.
- Establish whistleblowing mechanisms specifically tailored to AI-related ethical concerns, ensuring confidentiality and prompt resolution.
- Encourage regular feedback loops between technical teams and management to refine AI-generated reports and recommendations.

Expand Monitoring Frameworks for AI Systems

- Implement a structured, organization-wide monitoring framework that incorporates real-time analytics, predictive alerts, and performance benchmarking for AI-enabled processes.
- Ensure monitoring activities are integrated into broader strategic planning, with clear escalation procedures for detected anomalies.

Promote Hybrid Human-AI Oversight

- Maintain a balance between AI-driven automation and human judgment in critical decision-making processes to prevent over-reliance on AI outputs.
- Introduce phased rollouts and pilot testing for new AI controls to allow for iterative refinement before full-scale implementation.

Policy Formulation and Compliance Alignment

- Develop and adopt AI governance policies aligned with both local regulations and international best practices such as the COSO Framework and ISO AI standards.
- Regularly review and update internal control policies to reflect evolving AI technologies, regulatory changes, and global risk trends.

Suggestions for Future Research

- Expand the scope of future studies to include other industries where AI integration in internal control systems is emerging.
- Conduct longitudinal studies to measure the long-term impact of AI adoption on internal control effectiveness and organizational resilience.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

- Explore the intersection of AI ethics, data privacy, and internal controls to develop more comprehensive governance models.

Proposed Strategic Control Framework: RAISE Framework for Strengthening Internal Control Practices in AI-Driven Multinational Companies

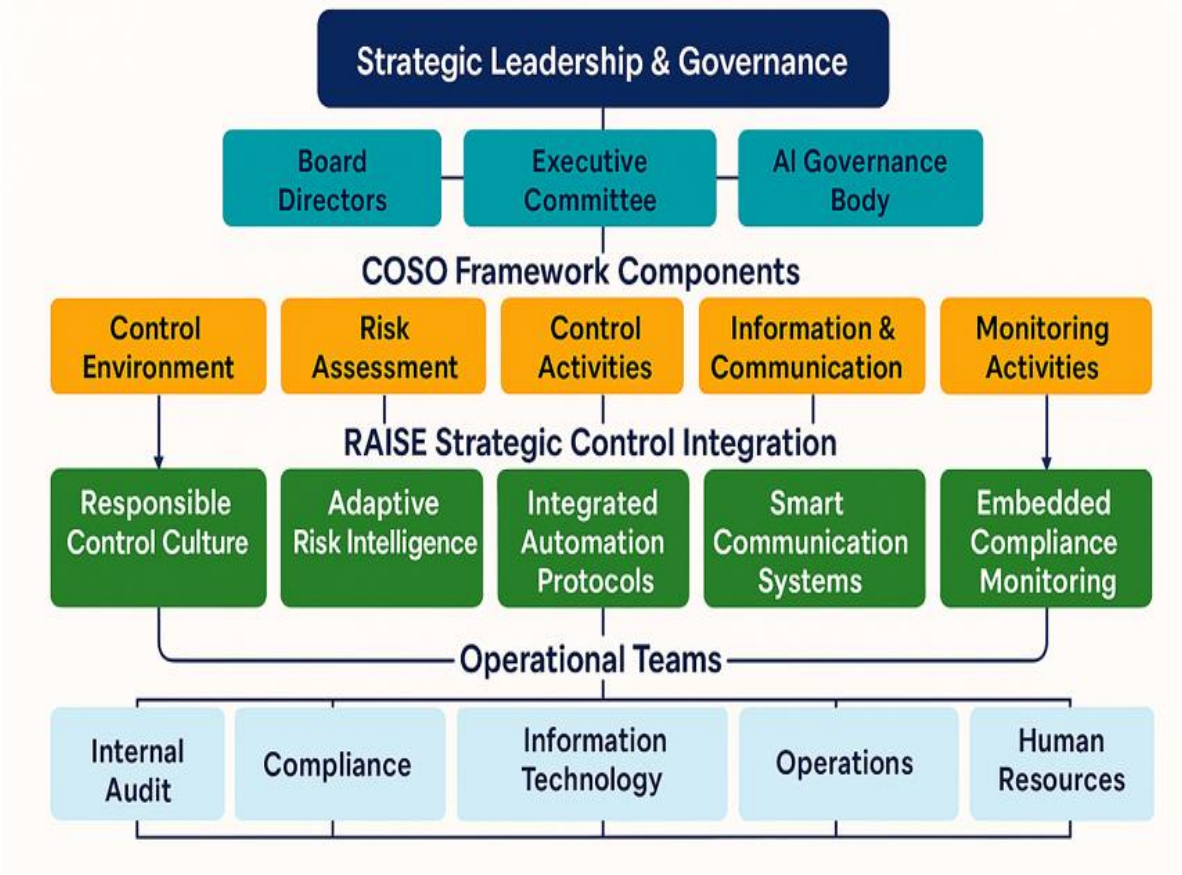

Figure 1. RAISE Framework, Responsible AI-Integrated Systems for Enterprise Controls. (Herradura, 2025)

Figure 1 shows the proposed strategic control structure for this study, the RAISE Framework, Responsible AI-Integrated Systems for Enterprise Controls. Developed in response to the findings and objectives of the research titled *"Strengthening Internal Control Practices in AI-Driven Multinational Companies: A Strategic Approach to Sustainable Business Operations,"* the RAISE framework offers a forward-looking internal control structure that addresses the operational, technological, and compliance challenges faced by multinational enterprises (MNEs) in the age of artificial intelligence.

This framework aligns with the COSO Internal Control-Integrated Framework while also integrating the realities of AI deployment in large-scale operations. RAISE is built on five core pillars: Responsible Control Culture, Adaptive Risk Intelligence, Integrated Automation Protocols, Smart Communication Systems, and Embedded Compliance Monitoring. Each component represents a strategic response to specific gaps and vulnerabilities highlighted during the study's qualitative assessment of internal control environments in leading AI-enabled organizations.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

The Responsible Control Culture pillar emphasizes the importance of ethical governance, leadership accountability, and organizational readiness when integrating AI into internal control systems. It responds directly to concerns identified in the study regarding over-reliance on automation, reduced human oversight, and the lack of AI-related policies. Establishing this foundation ensures that internal control practices remain principled, even as technological complexity increases.

The Adaptive Risk Intelligence component focuses on enabling real-time risk assessment through AI-driven anomaly detection and behavioral analytics. Instead of relying on static, periodic reviews, MNCs can shift toward continuous, dynamic evaluations of emerging threats, fraud indicators, and compliance breaches. This pillar strengthens the COSO components of risk assessment and monitoring activities, both of which were identified in the study as areas benefiting most from AI integration.

The Integrated Automation Protocols pillar ensures that internal control activities such as approval workflows, access controls, and transaction reviews are not only digitized but also aligned with compliance standards. The model promotes the adoption of robotic process automation (RPA), machine learning decision systems, and AI agents to enhance operational efficiency while preserving human oversight and auditability.

Smart Communication Systems represent the need for real-time, role-based control reporting and transparent information flow across complex, decentralized business structures. By utilizing AI-generated dashboards and alerts tailored to specific functions, this pillar addresses gaps in communication and supports faster, more informed decision-making among stakeholders. The study revealed that information and communication are critical enablers of sustainable internal controls, especially in environments where speed and clarity are vital.

Lastly, the Embedded Compliance Monitoring pillar incorporates continuous auditing, AI model validation, and traceable audit trails into the day-to-day internal control ecosystem. It reflects the study's emphasis on sustainability by ensuring that control systems are not only reactive but also preventive and adaptive. This helps organizations meet evolving regulatory requirements while maintaining a high standard of transparency and governance.

Figure 2. RAISED Framework Implementation Steps

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 1 Issue 8 (2025)

Figure 2 shows the RAISED Framework Implementation Steps diagram, which visually represents this process from assessment to continuous improvement. To operationalize the RAISE Framework, this study integrates the RAISED (Risk Assessment, AI Governance, Integration, Staff Training, Ethical Compliance, Data Security & Continuous Monitoring) implementation model. The process can be followed as a structured, cyclical sequence:

1. Risk Assessment - Identify and evaluate AI-related internal control risks, including compliance, fraud, operational disruptions, and ethical concerns.
2. AI Governance - Establish governance structures, policies, and oversight committees, such as an AI Steering Committee, to ensure accountability.
3. Integration - Embed AI capabilities into targeted internal control workflows, ensuring alignment with COSO principles.
4. Staff Training - Train staff, including Internal Audit and IT teams, on AI systems, governance policies, ethics, and bias mitigation, with hands-on sessions to build technical and operational readiness.
5. Ethical Compliance - Ensure that AI deployments adhere to legal requirements, such as the EU AI Act's FRIA, and maintain fairness, diversity, and transparency in outputs.
6. Data Security & Continuous Monitoring - Secure AI training data, implement intrusion prevention measures, and conduct continuous monitoring to detect and address performance issues, compliance risks, and system anomalies.

The continuous monitoring element ensures that implementation is not a one-time event but an ongoing cycle. Performance metrics, compliance indicators, and emerging risk factors are reviewed regularly, with adjustments made to AI models, internal control policies, and governance procedures as needed. This feedback loop ensures that internal control systems remain effective, adaptable, and aligned with strategic objectives.

Expected Strategic Outputs

The implementation of the RAISE Framework can generate a range of strategic outputs that significantly strengthen an organization's internal control environment. Among these are real-time risk and performance dashboards that provide continuous visibility into operational and compliance metrics, as well as predictive analytics reports that support proactive risk mitigation by identifying emerging threats before they escalate. The framework also enables the production of automated compliance documentation and audit-ready reports, reducing manual effort and ensuring accuracy in regulatory submissions. Additionally, AI-driven process optimization insights can be generated to streamline workflows, enhance resource allocation, and improve decision-making. Collectively, these outputs enhance transparency, operational efficiency, and governance integrity, enabling organizations to make faster, evidence-based decisions. By adopting the RAISE Framework, companies position themselves to gain a sustainable competitive advantage, capitalize on opportunities, mitigate potential risks, and accelerate innovation all while maintaining rigorous compliance and ethical standards.

Adoption Readiness and Feasibility

Adopting the RAISE Framework requires understanding a company's AI maturity, organizational readiness, and operational context. Interviews revealed varied adoption timelines, some companies have integrated AI for under two years (pilot stage), while others have over five years of experience (mature integration).

A critical determinant of feasibility is willingness to adopt or enhance existing AI-enabled controls. This depends on leadership vision and perceived alignment with ongoing initiatives. While some companies have existing AI enhancements, they may lack the governance, ethical safeguards, and continuous monitoring features that RAISE offers.

Key point persons for implementation include Internal Audit, IT, Risk Management, and Compliance leaders responsible for operationalizing the framework and maintaining ethical, secure, and compliant AI operations. Budget priorities center on Training & Development (T&D), the largest cost item, covering governance, ethics, bias mitigation, and continuous monitoring skills. Given rapid AI upgrades, companies must also budget for retraining, system updates, and enhancement of AI tools. Costs vary significantly depending on whether solutions are generic or highly specialized, the latter requiring higher investment for customization and integration. Finally, customization is essential, even within the same industry, internal control priorities differ. The RAISE Framework is designed as a configurable model adaptable to unique strategies, compliance requirements, and operational needs.

The adoption feasibility of the RAISE Framework hinges on a company's current level of AI integration, leadership commitment, and ability to allocate sufficient resources for training, upgrades, and customization. Organizations with mature AI adoption, strong executive support, and dedicated point persons in Internal Audit, IT, Risk Management, and Compliance are well-positioned to operationalize the framework effectively. However, even for those at earlier stages of AI adoption, a strategic focus on governance, continuous learning, and adaptability can enable successful implementation. By aligning budget priorities with long-term capability building and tailoring the framework to address unique operational needs, companies can ensure that the RAISE Framework delivers sustainable value, maintains relevance amid technological change, and drives competitive advantage in an increasingly AI-driven business landscape.

REFERENCES

Ahmad, A., Ambad, S. N. A., Mohd, S. J. A. N. S., & Lajuni, N. (2021). The moderation effect of job tenure on psychological empowerment and employee performance in malaysia public sector. *International Journal of Academic Research in Business and Social Sciences*, 11(4). https://doi.org/10.6007/ijarbss/v11-i4/9733

Alsawalhah, J. M., Al Dmour, H. H., Alghizzawi, M., & Al Madi, F. N. (2024). AI driven financial transparency and corporate governance: Enhancing accounting practices with evidence from Jordan. Sustainability, 16(9), 3818.

COSO. (2023). Enabling organizational resilience through effective enterprise risk management and internal control. Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2023, March 30). Achieving effective internal control over sustainability reporting (ICSR). Committee of Sponsoring Organizations of the Treadway Commission.

Deloitte. (2023). AI and internal controls: *Navigating new risks and responsibilities*. Retrieved from https://www2.deloitte.com/

Gartner. (2022). AI risk management and governance: Trends for 2022.

Gartner. (2022). The state of AI governance: Critical capabilities for audit, risk, and compliance leaders.

Gulan, X. M. D. and Aguiling, H. M. (2022). Examining the role of organizational climate on career adaptability and government employees' career intention. *International Journal of Research in Business and Social Science* (2147- 4478), 10(8), 129-137. https://doi.org/10.20525/ijrbs.v10i8.1521

North, M. S. (2022). Chinese versus united states workplace ageism as gate-ism: generation, age, tenure, experience. *Frontiers in Psychology*, 13. https://doi.org/10.3389/fpsyg.2022.817160

Nurlia, N., Daud, I., & Rosadi, M. E. (2023). Ai implementation impact on workforce productivity : the role of ai training and organizational adaptation. Escalate : *Economics and Business Journal*, 1(01), 01-13. https://doi.org/10.61536/escalate.v1i01.6

PwC. (2021). AI governance and controls: Balancing innovation with accountability.

PwC. (2021). Trust in AI: How to manage risks and build confidence in artificial intelligence.

Rane, N. L., Desai, P., & Choudhary, S. K. (2024). Challenges of implementing artificial intelligence for smart and sustainable industry: technological, economic, and regulatory barriers. *Artificial Intelligence and Industry in Society* 5.0. https://doi.org/10.70593/978-81-981271-1-2_5

Uddin, A. S. M. A. (2023). The era of ai: upholding ethical leadership. *Open Journal of Leadership*, 12(04), 400-417. https://doi.org/10.4236/ojl.2023.124019