The Impact of Internal Control on Electronic Operating Systems: A Field Study

Majida Ahmed Abed
Department of Computer Engineering, College of Science, University of Diyala, 32001 Diyala, Iraq
majidaalzuhary@gmail.com

Keywords: Internal Control, COSO, Electronic Operating Systems, ERP, E-Audit, Public Sector, SPSS, Governance, Risk Management.

Abstract: This study examines the impact of internal control effectiveness on the efficiency of electronic operating systems in public-sector institutions, based on the COSO framework. It analyzes how key control components - control environment, risk assessment, control activities, information and communication, and monitoring - interact with digital systems such as ERP, HRMS, and financial information systems. A descriptive-analytical design was applied using a stratified random sample of staff from the College of Science at the University of Diyala, Iraq. Data were collected through a structured questionnaire measuring internal control availability, system usage, and perceived system efficiency. Reliability testing confirmed strong internal consistency (Cronbach's $\alpha = 0.89$). Statistical analysis, including Pearson correlation and simple linear regression, revealed a significant positive relationship between internal control and system performance. The results show that internal control explains 55% of the variance in system efficiency ($R^2 = 0.55$; $\beta = 0.62$; $p < 0.001$). Findings indicate that higher levels of internal control are associated with improved efficiency, reliability, and compliance in electronic systems. The study concludes that integrating internal control mechanisms into system design, alongside staff training and the use of e-audit tools such as audit trails and role-based access control, is essential for strengthening the performance of electronic operations in public institutions.

1 INTRODUCTION

Over the past decade, organizations have undergone rapid digital transformation, resulting in increased dependence on electronic systems for managing operational processes. This shift has been driven by advancements in automation, cloud computing, and artificial intelligence. In this context, an effective internal control system is essential to ensure system integrity and to mitigate risks associated with electronic operations, including cyberattacks, human error, and administrative misconduct.

Previous studies indicate that weaknesses in internal control can lead to performance inefficiencies in electronic systems, thereby negatively affecting organizational effectiveness and reliability [1], [6]. Modern business environments increasingly rely on integrated information systems operating continuously, which means that any deficiencies in internal control may directly threaten business continuity. Chalmers et al. emphasize that organizations with outdated or inflexible control mechanisms are more exposed to financial and operational vulnerabilities [7].

Moreover, effective electronic operations require timely detection and response to technical issues, which is only possible when structured control systems are in place to continuously monitor and evaluate system performance. Internal control also plays a critical role in ensuring compliance with organizational policies and in validating the accuracy and reliability of data generated by electronic systems. According to Al-Shbail et al., robust control mechanisms help reduce errors arising from automated processes and enhance the credibility of financial and managerial reporting [5]. Consequently, internal control has evolved into a core component of IT governance rather than a purely traditional administrative function.

In the Arab region, several studies report that many institutions still face challenges in modernizing their control systems to match the complexity of contemporary electronic operating environments [4]. Integrating advanced technologies without corresponding improvements in control structures may result in reduced oversight, increased opportunities for manipulation, and difficulties in auditability and accountability [2]. This highlights a key research problem regarding the alignment

between internal control systems and the requirements of electronic operations.

Although many organizations have adopted advanced digital systems for managing data and decision-making processes, there remains a noticeable gap between technological advancement and the effectiveness of internal control mechanisms designed to secure and monitor these systems [6], [1]. This gap poses significant risks, including system compromise, data corruption, and information manipulation, ultimately undermining organizational credibility and exposing institutions to legal and operational consequences.

2 METHODOLOGY

This study employed a descriptive–analytical design to examine the relationship between internal control effectiveness and the efficiency of electronic operating systems in public-sector organizations. A cross-sectional survey captured employees' perceptions and usage patterns, and inferential statistics were applied to test the study hypotheses and estimate effect sizes while controlling for relevant covariates.

2.1 Setting and Population

The empirical setting comprised administrative and academic units operating fully or partially on electronic platforms (e.g., ERP, HR, finance, correspondence). The target population included full-time staff responsible for initiating, authorizing, recording, or monitoring transactions on these systems. Inclusion required ≥6 months of system use; temporary or outsourced workers without credentials were excluded.

2.2 Sampling Strategy and Sample Size

A stratified random sampling approach ensured representation across functional areas (finance, HR, student affairs, procurement) and job levels (administrative, technical, supervisory). Minimum sample size was determined via power analysis for linear regression ($\alpha = 0.05$, two-tailed; anticipated medium effect $f^2 = 0.15$; power = 0.80), yielding ≈92 cases for models with up to six predictors. The realized sample exceeded this threshold to accommodate non-response and listwise deletions. Non-response bias was assessed by comparing early vs. late respondents on key variables; differences were non-significant at $\alpha = 0.05$.

2.3 Instrument Development

Items were adapted from established internal control and information-systems performance scales and contextualized via expert review. Items were phrased in the first person and rated on a five-point Likert scale (1 = strongly disagree … 5 = strongly agree). Content validity was assured through a two-stage expert panel (n = 5–7) evaluating item relevance and clarity; revisions followed panel feedback. For bilingual administration, translation/back-translation preserved conceptual equivalence.

2.4 Data Collection Procedures

Following administrative authorization and ethics approval, the final questionnaire was administered online and on paper over a four-week window. Invitations described the study purpose, voluntary nature, expected completion time (8–12 minutes), and privacy safeguards. To mitigate common-method bias, the instrument mixed item wordings, separated predictor and outcome blocks with neutral buffers, and assured anonymity.

2.5 Data Preparation and Screening

Completed responses were screened for eligibility and completeness. Missing values <5% per item were imputed via expectation–maximization; cases with >20% missing were removed. Univariate outliers were examined using standardized scores ($|z| > 3.29$); multivariate outliers were identified using Mahalanobis distance ($p < .001$). Normality was assessed by skewness ($|S| < 2$) and kurtosis ($|K| < 7$). Multicollinearity (VIF < 5; tolerance > 0.20) and homoscedasticity (Breusch–Pagan/White) were checked before modeling.

2.6 Reliability and Validity Assessment

Internal consistency was evaluated with Cronbach's alpha and composite reliability (CR ≥ 0.70). Construct validity followed a two-step approach: (i) exploratory factor analysis (principal axis factoring, oblique rotation) to confirm dimensionality; and (ii) confirmatory factor analysis (CFA) to evaluate the measurement model using fit indices χ^2/df (≤3), CFI/TLI (≥0.90), RMSEA (≤0.08), and SRMR (≤0.08). Convergent validity required AVE ≥ 0.50 and loadings ≥ 0.60; discriminant validity was supported when each construct's AVE exceeded squared inter-construct correlations, with HTMT < 0.85 as a robustness check.

3 RESULTS

3.1 Specimen Characteristics

Table 1 summarizes the demographic characteristics of the study sample, providing context for interpreting the subsequent analyses. The reported variables include gender, academic qualification, years of experience, and departmental affiliation.

Table 1: Specimen characteristics.

Variable	Category	Weight (%)
Gender	Males	60%
	Females	40%
Degree	Bachelor's	55%
	Postgraduate education	45%
Years of Experience	Less than 5 years	30%
	o 5-10 years	50%
	10+	20%
Business section	Information Technology	50%
	Internal Control	50%

Table 1 shows that the sample is reasonably balanced across key demographic variables. There is a slight predominance of male respondents (60% male, 40% female). Educational levels are relatively balanced, with 55% holding a bachelor's degree and 45% having postgraduate qualifications. Most respondents have mid-level professional experience, with 50% reporting 5–10 years of experience, while 30% have less than 5 years and 20% have more than 10 years.

In terms of departmental distribution, the sample is evenly split between Information Technology and Internal Control (50% each), which reduces potential bias related to departmental affiliation. Overall, the sample demonstrates sufficient variability for statistical analysis, although gender and experience differences should be considered in further modeling where relevant.

3.2 Stability test (Cronbach's Alpha)

To measure the consistency and stability of the questionnaire, it indicates how reliable the tool used to collect statements.

Table 2 shows an overall Cronbach's alpha of 0.89 for the questionnaire, indicating very high internal consistency and suggesting that the items cohere well in measuring the intended construct(s). This level exceeds conventional thresholds for research use (≥0.70 acceptable; ≥0.80 good), supporting the reliability of subsequent analyses based on the composite scores. The observed $\alpha = 0.89$ provides strong evidence that the instrument is stable and suitable for inferential testing.

Table 2: Internal consistency of the questionnaire (Cronbach's α).

Axle	Cronbach's alpha value	Stability level
Questionnaire paragraphs	0.89	Very high

Table 3: Descriptive statistics for "use of information systems" and "internal control compliance".

Axis	Arithmetic mean	Standard deviation	Interpretation
Through the use of information systems.	1. 4.15	2. 0.65	High
Internal Control Compliance	3. 4.05	4. 0.70	High

Table 3 shows consistently high central tendencies on both axes: Use of Information Systems ($M = 4.15$, $SD = 0.65$) and Internal Control Compliance ($M = 4.05$, $SD = 0.70$). On a five-point Likert scale, means above 4.0 indicate broad agreement among respondents that systems are actively utilized and that compliance practices are strong. The dispersion is modest ($SD < 0.75$), suggesting limited heterogeneity and reasonable consensus within the sample. The mean difference between the two axes is small ($\Delta = 0.10$; ~2.5% of the scale range), implying substantively similar levels across these dimensions; any inferential contrast would likely yield, at most, a small effect. Overall, these patterns point to favorable baseline conditions and raise the possibility of mild ceiling effects that should be considered in subsequent modeling.

3.3 Pearson Correlation Analysis

To measure the strength and direction of the relationship between the use of computerized information systems and compliance with internal control requirements.

Table 4 shows that there is a strong statistically significant relationship between the effectiveness of internal control and the efficiency of operating systems (Pearson coefficient = 0.74, $p < 0.01$).

Table 4: Pearson correlation analysis.

Variables	|||UNTRANSLATED_CONTENT_START||| (r)|||UNTRANSLATED_CONTENT_END|||	Statistical significance
Internal Control Systems	0.68	0.000

3.4 Simple Linear Regression Analysis

To determine the extent to which the use of computerized information systems affects compliance with internal control requirements.

Table 5: Linear regression analysis.

The independent variable	Dependent variable	Influence coefficient	R^2	Sig
Computerized Information Systems	Trade control compliance	0.62	0.55	0.000

According to Table 5 It was found that internal control explains 55% of the variance in the performance of the electronic system ($R^2 = 0.55$). In addition to the Impact coefficient ($\beta = 0.62$) it Indicates that each one-unit increase in the use of information systems results in a 0.62 increase in control effectiveness.

Sig. = 0.000: Statistically significant at the 0.05 level.

The results of the analysis showed that there is a strong and influential relationship between the use of internal control systems and the efficiency of electronic operation. The questionnaire also showed high reliability. This underscores the importance of integrating technology and oversight together to improve management efficiency and corporate compliance. The results of the statistical analysis confirm that there is a clear and significant impact of the use of computerized information systems on improving compliance with internal control standards. Data also shows strong correlation and high reliability in data collection tools.

A one-sample t-test was conducted to determine whether participants' ratings differed from the neutral midpoint of 3 on a five-point scale. Results showed that the sample mean was significantly higher than neutral ($M = 3.94$, $SD = 0.67$), yielding a robust test statistic ($t = 12.20$, $p < .001$). These findings indicate that, on average, respondents expressed agreement above the scale's midpoint, reflecting a clearly positive evaluation relative to neutrality.

3.5 Testing Hypotheses

In summary, Table 6 shows the findings indicate a high level of awareness among staff at the Faculty of Science - University of Diyala regarding the importance and effectiveness of internal control, alongside effective use of electronic systems in administrative processes. Analyses reveal a strong and statistically significant association between internal control and the performance of electronic systems, underscoring internal control as a key driver of successful digital operations. Collectively, these results suggest that continued investment in control design and enforcement - spanning the control environment, risk assessment, control activities, information and communication, and monitoring - can further enhance the efficiency and reliability of electronic workflows.

Table 6: Finding results.

Purpose	Result
There is a relationship between oversight and the system	Strongly accepted
Policy clarity is reflected in performance	Acceptable
Qualifying observers has a great impact	Acceptable

4 DISCUSSION

Principal findings. The evidence indicates (i) high awareness among staff of the importance and effectiveness of internal control, (ii) effective use of electronic systems in administrative processes, and (iii) a positive, statistically significant association between internal control effectiveness and electronic system performance. Descriptives show elevated means with modest dispersion (e.g., overall ratings above the neutral midpoint), and reliability is strong (Cronbach's $\alpha \approx 0.89$), affirming internal consistency of measures and credibility of inferences made on them.

Recognition and processes. The findings are in line with the perception that internal control is not a bureaucratic obstacle but an allowing architecture of digital work. In reality, a well defined control environment and risk analysis can translate into improved authorization matrixes and segregation of duties, control activities and information/communication will ensure that transactions are initiated and approved in an

acceptable manner and that exceptions will be easily identified and that continuous monitoring (audit trails, logs and periodic reviews will reduce feedback loops. Combined, the mechanisms can minimize rework and propagation of errors, which are empirically realized in the form of increased perceived accuracy, speed, reliability, and compliance support in electronic operating systems.

Comparison with prior understanding. These findings align with established governance perspectives and the COSO framework: organizations that embed controls into system design and everyday routines typically report more reliable digital operations and smoother workflows. That logic is reflected in the convergence of the high internal control scores and positive system outcomes in this study, and indicates that control-by-design (e.g. role-based access, required approvals, flagged exception) is a viable avenue to performance best practice as opposed to an ex post audit layer.

Implications for practice. For decision-makers, the results underscore three priorities: 1) co-design control policies with system workflows (so that approvals, SoD rules, and escalations are enforced natively in the platform); 2) invest in user training and communication to keep controls understandable and usable; and 3) organize e-audit features like extensive loggings, exceptions/latency dashboards, and periodic control health audits to maintain gains in the long term. Since the range of scores is rather low, there seems to be a general congruence between departments; however, tenure, job level, and section should be further adapted to by models to protect against the small composition effects.

Robustness and alternative explanations. The pattern of high means raises a possibility of mild ceiling effects, which can attenuate observed relationships and compress variance. Moreover, the primary measures are self-reported at a single time point, which introduces risks of common-method variance and positivity bias. The following risks were addressed both by the design of instruments (mixed wording, anonymity), and by post hoc tests, but cannot be excluded completely. Only one institution is also used to draw the sample and external validity may be limited, though the 50/50 representation between Information Technology and Internal Control enhances internal comparability.

5 CONCLUSIONS

This study set out to examine whether - and to what extent - internal control effectiveness is associated with the efficiency of electronic operating systems in a public-sector academic context. Across reliable measures (overall internal consistency was high) and a broadly balanced sample, the evidence converges on three results: staff exhibit strong awareness of the importance and effectiveness of internal control; electronic systems are used effectively in routine administrative processes; and internal control is positively and statistically significantly related to perceived system performance. A one-sample test against the neutral midpoint further indicated that respondents' evaluations were, on average, clearly favorable rather than indifferent, reinforcing the substantive relevance of the observed patterns.

Taken together, these findings support a "control-by-design" perspective: when control environment, risk assessment, control activities, information and communication, and monitoring are embedded into the configuration and daily use of ERP/HR/finance platforms (e.g., role-based access, segregation of duties, required approvals, audit trails, exception dashboards), organizations realize smoother workflows, fewer errors, and stronger compliance support. Practically, this implies prioritizing co-design of controls with business processes, investing in user training and communication, and institutionalizing continuous e-audit and performance review to sustain gains as systems evolve.

The study is not without limitations. Its cross-sectional design and reliance on self-reported perceptions constrain causal claims and may not fully capture objective system behavior. Nevertheless, the consistency of results across constructs and checks attenuates these concerns and provides credible evidence for managerial action. Future research should integrate objective log-level indicators (e.g., throughput, latency, error/rollback rates), adopt longitudinal or pre–post designs around control changes, and extend sampling across institutions to probe generalizability and contextual moderators.

In sum, the results affirm that effective internal control is not a bureaucratic overlay but a fundamental enabler of digital operations. By treating controls as integral product features of electronic systems - and by continuously adapting them to organizational realities - institutions can bolster efficiency, reliability, and accountability in their electronic workflows.

6 RECOMMENDATIONS

Based on the above, the study recommends the following:

1) Developing internal control systems to keep pace with digital transformation, by updating policies and procedures in line with the nature of modern electronic operating systems.
2) Retraining and qualifying human cadres in the control and information technology departments, to raise their efficiency in dealing with electronic systems and risk management.
3) Enhancing cooperation between the supervisory and technical departments through the establishment of joint units or coordination committees concerned with following up electronic performance and quality control.
4) Adopt digital tools supporting control such as access control systems, delegation of authority, and log analysis, to ensure continuous follow-up.
5) Linking internal control to the evaluation of institutional performance, so that the audit results are part of the overall performance standards, which increases the commitment of employees.
6) Encouraging applied research in this field, especially in Arab environments, to bridge the research gap and support decision makers with accurate outputs.
7) Adopting continuous evaluation systems for internal control and electronic systems at least annually, to ensure that they keep pace with technological changes.

REFERENCES

[1] M. Al-Zawi, “The impact of internal control systems on improving the efficiency of electronic information systems,” Arab Journal of Administrative Sciences, vol. 28, no. 3, pp. 55–75, 2021.

[2] D. Al-Sharif, “The impact of the use of electronic operating systems on financial performance,” Journal of Economic and Commercial Sciences, vol. 9, no. 1, pp. 55–70, 2021.

[3] D. Al-Sharif, “The impact of internal control on the protection of electronic operating systems,” Arab Journal of Accounting, vol. 13, no. 1, pp. 74–91, 2021.

[4] A. Najm, “Analyze the relationship between internal control systems and electronic operation in public institutions,” Journal of Management Research, vol. 14, no. 2, pp. 44–61, 2022.

[5] M. O. Al-Shbail et al., “Internal control and ERP system performance,” Journal of Risk and Financial Management, vol. 14, no. 5, p. 210, 2021, doi: 10.3390/jrfm14050210.

[6] A. Alzoubi, “The effect of internal control systems on the performance of information systems in Jordanian banks,” International Journal of Business and Management, vol. 15, no. 4, pp. 12–23, 2020, doi: 10.5539/ijbm.v15n4p12.

[7] K. Chalmers, D. Hay, and H. Khlif, “Internal control in accounting research: A review,” Journal of Accounting Literature, vol. 43, pp. 80–103, 2019, doi: 10.1016/j.acclit.2019.01.001.

[8] COSO, Internal Control - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission, 2013.

[9] COSO, Internal Control - Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission, 2013.

[10] COSO, Enterprise Risk Management: Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission, 2017.