Global Economics and Finance Insights, Vol. 01, No. 01, 2026

CONCEPTUAL MAPPING OF INFORMATION RISK IN EXPENDITURE CYCLE AUDIT IN ENTERPRISE RESOURCE PLANNING ENVIRONMENT: A SYSTEMATIC LITERATURE REVIEW

Zahrina Qurrota A'yun

Department of Accounting, Sekolah Tinggi Ilmu Ekonomi Indonesia (STIESIA), Surabaya, Indonesia

Corresponding author: zahrina.zqa33@gmail.com

ABSTRACT

The rapid pace of digital transformation has made Enterprise Resource Planning (ERP) more important than ever as a coordinating backbone for organizations, especially in managing their expenditure cycles. While most researchers and commentators on ERP implementations have emphasized the positive impact of these systems on organizational integration and operational efficiency, some of the latest studies begin to focus on the generation of new and, in some cases, contradictory information-related risks. Such information risks stem from the relationship among a firm's technological configuration, its organizational structure and processes, and the discretion exercised by its auditors. This type of information risk demonstrates the value of taking an approach that is less exclusively focused on the technology involved. This paper is based on a qualitative Systematic Literature Review (SLR) of peer-reviewed articles sourced from the most reputable journals. From the thematic matrix of the objectives of the studies, their method, the principal findings, and the conclusions of the studies, a pattern of auditors' experiences, and the social and cognitive difficulties, is constructed. Several recurrent patterns have been found especially in regard to the social and cognitive difficulties auditors face in ERP-based structures. From the analysis of the data, three principal themes are apparent. The first is the "illusion of integration" and the loss of visibility of audit trails, which makes tracing and interpretive processes of transactions even more difficult. Secondly, the digital ambiguity of tasks creates an an tension professionally between the need for flexibility and the need to retain control. Third, the greater dependence on automation strengthens the focus of audits from manual checks to evaluations of the system, which diminishes the likelihood of professional skepticism. The author identifies for the first time the phenomenon of the information risk of ERP audits as a socio-technical phenomenon. The findings shape the socio-technical aspect of information risk in ERP audits and the literature on digital auditing, audit pedagogy, and normative policy frameworks. There are several digital, organizational, and auditing system interrelations that remain to be researched.

Keywords: Enterprise Resource Planning (ERP), Expenditure Cycle Audit, Information Risk, Socio-Technical Systems.

INTRODUCTION

In just a few short years, businesses and government agencies in Indonesia have undergone a transformational process that integrates technology and automation in a more efficient manner than ever before, resulting in the widespread adoption of Enterprise Resource Planning (ERP) systems. Generally, such systems are thought to simply provide integrative, real-time updates of information streams to sustain efficient business processes as well as improve vertical and horizontal operational integration. Their implementation impacts many dimensions of work and the organization of work that are professionally and operationally relevant to the organization. ERP systems are disruptive technologies that change the nature of work processes, the systems

of internal control, and the hierarchy of control and power relationships. In the specific case of internal auditors, accountants, and financial managers, the ERP implementation process is more than a change in technology; it is a transformation of work processes and control systems. The transformation of work processes and systems of internal control is most profoundly felt in the audit work of the procurement cycle, invoicing, and payment processes. The transition from a manual or a semi-automated system to an ERP-based system creates a unique information risk environment. Such information risks can be a result of the module configuration, control circumvention, inadequate data update frequency, and information access control that is overly reliant on role-based access control.

From the perspective of internal auditing, the implementation of ERP systems is a complex challenge. Although real-time reporting and digital audit trails are designed to increase transparency, system integration can simultaneously conceal hidden risks. The connectivity of the various ERP modules increases the risk profile, making potential risks less transparent in the early stages. Previous research has clearly shown that the lack of ERP implementation quality is often linked to poor governance, organizational, and internal control issues (Coşkun et al., 2022). Furthermore, a systematic literature review of ERP failures published in Data & Knowledge Engineering shows that implementation and configuration quality issues can contribute substantially to the risk of financial reporting integrity. These findings suggest that information risk in ERP systems cannot be attributed solely to technical failure but is also influenced by user behavior, professional expertise, and organizational culture.

Recent systematic literature reviews also demonstrate the growing interest in risk-based auditing in information systems. Munthe et al. (2025), for instance, highlight the pressing need for the implementation of risk-based information system audits in digital accounting environments. On the other hand, the study conducted by Handayani et al. (2023), based on the COBIT framework, indicates that the current maturity level of IT risk controls in most organizations is still low. Evidence from other studies also indicates that the results of ERP implementation, whether positive or negative, are mostly dependent on the quality of governance, cultural factors, and user capacity (Butarbutar et al., 2023; Rajapakse & Thushara, 2023). Taken together, this body of literature confirms that ERP risks are, in fact, multidimensional and deeply entrenched in organizational settings.

Notwithstanding the discovery of a number of key risk factors, the current literature is still dominated by quantitative approaches or normative models of evaluation. There is still a lack of understanding regarding the auditors' interpretation and construction of information risk, especially in the context of the expenditure cycle. The earlier literature has been dominated by technical considerations, often to the point of ignoring the interpretive processes involved in auditors' responses to system complexity. This highlights the need for qualitative research that can tap into the social and interpretive aspects of ERP-based auditing.

The relevance of this research is further emphasized by the current global environment that is characterized by big data integration and complex ERP system architectures (Gandasari & Mukhtaruddin, 2025). In the Indonesian context, there are still various organizations that continue to experience challenges in terms of their IT capabilities and governance structures that have not yet attained optimal maturity levels. Without a strong conceptual foundation for information risk in expenditure cycle audits, the risks of being vulnerable to fraud, financial misrepresentation, and inefficient operations would be increasingly hard to manage. This research therefore seeks to: (1) systematically uncover the types of information risk that are relevant to ERP-based expenditure cycle audits; (2) investigate how information risks have been conceptualized in the literature over the last five years; and (3) construct an integrative framework that bridges the technical and social aspects of ERP auditing. This research is limited

to a systematic literature review of information systems auditing, ERP risk, and internal control in the expenditure cycle.

THEORITICAL REVIEW

Information Risk in ERP as a Socio-Technical Phenomenon

The implementation of Enterprise Resource Planning (ERP) systems in contemporary organizations cannot be viewed exclusively as a technology implementation process. Instead, the implementation of ERP systems in organizations is a larger socio-technical change process that alters work interaction patterns, redefines authority, and alters internal control systems. Contemporary literature suggests that risks in ERP systems are not primarily caused by technology failures but instead by the interaction between human actors, technology, and governance structures (Setiawan, 2022). Based on this understanding, information risk in ERP systems is socially constructed through the interaction between system capabilities and social practices surrounding their use.

Within the spending cycle that includes procurement, accounts payable, and payment processing, ERP systems provide a platform that integrates transactional information. The degree of integration is expected to improve the traceability of transactions. However, the level of complexity in modular designs, the overdependence on role-based access control, and the risk of overriding automated controls are risk exposures that are not always easily identifiable by auditors. Evidence from the empirical study offered by Coşkun et al. (2022) shows that the failure of ERP systems often lies in governance issues and misalignment between system design and organizational practices.

A purely analytical approach focusing only on technical factors is thus insufficient to account for auditors' perceptions, interpretations, and reactions to these risks. In view of this, the current research is founded on three different yet complementary theoretical foundations: (1) Sociotechnical Systems Theory, (2) Institutional Theory in the context of digital governance, and (3) the sensemaking approach to risk-based auditing. These three theories can be combined to form a comprehensive perspective for studying the social processes, interpretive activities, and professional experiences involved in the construction and negotiation of information risk in ERP-based audit settings.

Sociotechnical Systems Theory: Interactions Between Technology and Organizational Practice

Sociotechnical Systems Theory (STS) specifically highlights that the technical and social aspects of an organization are, in essence, intricately intertwined and cannot be analyzed separately. In the context of ERP systems, information risk is thus influenced not only by the level of system architecture complexity but also by how organizational actors such as auditors interact with, make sense of, and adjust system functionalities in the course of their day-to-day work. Empirical evidence presented by Coşkun et al. (2022) suggests that most post-implementation failures in ERP systems are due to a lack of alignment between technological design and organizational readiness. Similarly, Heuvel (2025) suggests that the impact of digital transformation has shifted the classical role of auditors from a compliance-focused role to a more analytical one that demands an understanding of technological infrastructure and its implications for the effectiveness of internal controls. In this regard, auditors play a pivotal role in ensuring audit quality and organizational risk management practices. Kristiani et al. (2023) further suggest that enhanced audit quality is inextricably tied to the level of auditors' ERP knowledge and the enhancement of internal audit capabilities in managing risk and compliance processes (Kuntadi & Pramukty, 2023).

From the STS lens, the experiences of information risk by auditors can be interpreted as reactions to tensions between control mechanisms designed in a formal manner and the realities of operational practices. For example, while segregation of duties might be formally embedded in ERP system designs, the possibility of bypassing or overriding control mechanisms might still arise for some actors. This situation illustrates that risk is not merely grounded in technical failures, but is also embedded in organizational power relations and cultural beliefs. Therefore, STS conceptualizes ERP-related information risk as a complex phenomenon that goes beyond system configuration issues.

Institutional Theory and Digital Governance

Institutional theory regards organizations as socially embedded systems, whose structures and processes are influenced by regulatory needs, normative influences, and shared cognitive beliefs in the institutional environment. In the context of ERP system implementation and risk-based auditing, system implementation is often influenced not only by considerations of efficiency but also by the need for organizational legitimacy, including compliance with governance regulations, financial reporting requirements, and internationally accepted best practices. According to Elbardan et al. (2015), internal control structure modifications after ERP system implementation do not always result from internal operational needs. Instead, these modifications may reflect organizational responses to external institutional pressures. Similarly, Widyaningdyah and Ezra (2020) suggest that the effectiveness of internal controls incorporated in ERP systems is inextricably bound to the degree of institutional commitment and the development of a compliance culture within the organization. From an institutional theory perspective, information risk in expenditure cycle audits may therefore be regarded as arising from the gap between formal regulatory requirements and the realities of ERP system implementation and usage. This institutional theory perspective emphasizes that risk is not only a technical or procedural matter but is also influenced by broader institutional factors that shape organizational behavior and audit outcomes.

RESEARCH METHODOLOGY

This research adopts a qualitative methodology with a focus on an interpretive Systematic Literature Review (SLR). The selection of this methodology is very much attuned to the main purpose of this research, which is not to investigate causalities through statistical analysis but to develop a rich understanding of how information risk in expenditure cycle audits is conceptualized and explored in the current literature on Enterprise Resource Planning (ERP) settings. Since the phenomenon under investigation involves the intersection of technical characteristics of systems, governance structures, and social processes, a research methodology that is sensitive to conceptual richness and theoretical evolution is required. In this respect, the SLR serves not only as a systematic compilation of existing research but also as a reflective instrument for exploring the intellectual landscape that still remains inadequately investigated.

The research carried out a purposive and systematic literature review, choosing articles from credible academic journals on ERP systems, risks of information systems, risk-based auditing, and internal control in the digital environment. The literature review used structured keywords in the screening process, following the PRISMA flow from identification and abstract screening to full-text screening, finally focusing on the eleven most relevant articles to the topic, based on themes and quality of methodology. Rather than focusing on a particular organization or geographical area, the analysis takes a wider view in the academic and professional literature on audit practices as they are affected by digital transformation, considering the literature as a whole as the unit of analysis. The data collection included a thorough document analysis and coding in a synthesis matrix that included authorship, context, methods, and key contributions.

The inductive thematic analysis guided the research, beginning with open coding and moving on to more general codes such as technical risks, governance risks, and social risks, culminating in an interpretive synthesis that developed an integrated conceptual framework.

RESEARCH RESULT

The process of reviewing articles that satisfied the criteria for inclusion led to the development of a conceptual map that represents information risk in the expenditure cycle audit in the context of ERP systems. By using inductive thematic analysis, the results were synthesized into three themes that represent the auditors' professional experiences, organizational complexities, and complex interactions between technological infrastructure and human interpretation. To ensure consistency in reporting, excerpts were analytically reconstructed from the reviewed articles and referred to as A1-A11.

Theme 1: The Illusion of Integration and the Blurring of the Audit Trail

Contextual Background

"In theory, everything is recorded. But when we try to trace a single payment transaction, we get lost in layers of system configuration." (A3)

"The audit trail exists, but it's not always meaningful. We see the data, but we don't always understand its context." (A7)

Interpretative Insight

This theme captures the essence of a paradox between the technical transparency offered by ERP systems and the interpretability of information. Although integration offers a perception of overall visibility, analysis is still highly dependent on the auditors' technical knowledge and judgment. This complexity transcends the technical domain and affects the auditors' confidence in their findings and the overall effectiveness of internal controls. Thus, information risk in the context of ERP systems is a complex phenomenon that needs to be viewed from a socio-technical perspective (Handayani et al., 2023; Munthe et al., 2025).

Theme 2: Ambiguity in Segregation of Duties within the Digital Environment

Organizational Setting

Segregation of duties (SoD) is one of the most fundamental concepts of internal control. In the context of ERP systems, this concept is implemented by the use of access controls and role-based security. However, based on the literature reviewed, it is clear that access controls are often modified to suit operational requirements or management instructions. This often results in individual user accounts having a combination of rights that violate fundamental control concepts (Rajapakse & Thushara, 2023; Widyaningdyah & Ezra, 2020).

Illustrative Excerpts

"We found one user who could create vendor accounts and approve payments at the same time. Systematically, it's 'allowed,' but in principle, it's disruptive." (A5)

"Management says it's only temporary. But 'temporary' can last for months." (A9)

Interpretative Insight

This theme highlights the professional paradox that auditors are confronted with in trying to balance the need for efficiency gains with the need to protect control integrity. Information risk with regard to this issue can be attributed not only to technical failures but also to more

pragmatic considerations. The original intention of these systems was to improve internal control, but they can end up facilitating the accumulation of digital power when there is a lack of effective oversight (Kristanti et al., 2023; Kuntadi & Pramukty, 2023).

Theme 3: Dependence on Automation and the Erosion of Professional Skepticism

Situational Context

The ERP systems have automated controls such as three-way matching, approval processes, and alerts for anomalies. According to the literature, these aspects have minimized the need for manual verification, and auditors' focus has shifted to reviewing system logs instead of the details of transactions (Butarbutar et al., 2023; Gandasari & Mukhtaruddin, 2025).

Illustrative Excerpts

"If the system says 'matched,' we tend to believe it. We rarely question the logic behind its algorithm." (A2)

"Sometimes I feel like our role has changed, it's no longer checking the transaction, but checking whether the system checked the transaction." (A11)

Interpretative Insight

This theme indicates a shift in the professional identity of auditors in an ERP-based environment. The more the environment relies on automated processes, the more it may develop an implicit belief in the results of the system, which could lead to a reduction in the application of professional skepticism. The emphasis of audit work gradually moves from scrutinizing specific transactions to judging the credibility of the system. There is a degree of ambiguity between efficiency and professional judgment, where skepticism of automated processes could be seen as questioning organizational processes, but failure to do so could undermine professional obligations (Ou & Wu, 2025; Heuvel, 2025).

Table 1. Thematic Integration.

Main Theme	Subtheme	Core Interpretation
Illusion of integration	Configuration complexity; blurred audit trails	Formal technical transparency does not guarantee substantive interpretability
Ambiguity in segregation	Flexible access rights; policy compromises	Operational demands may conflict with the integrity of internal controls
Reliance on automation	Reduced manual verification; decline in skepticism	Excessive trust in system outputs can conceal underlying risks

Source: Author (2026).

These three themes are interrelated. The nature of integration affects the application of control structures, while automation changes the auditors' judgment and professional practice. These three themes show that information risk in the ERP-based expenditure cycle audit is constructed through the interaction of technological design, governance, and human interpretation. This theme can be explained using the theory of professional skepticism and the view of the changing identity of professionals in the digital age.

DISCUSSION

Close analysis of the literature reviewed indicates that there are three interrelated patterns that emerge in the interpretation of information risk in the context of ERP system-based expenditure cycle audits. Firstly, there is an underlying presumption that system integration necessarily provides for transparency, despite the fact that such integration is not necessarily accompanied

by a sufficient level of clarity in terms of tracing transactions. Secondly, there is a fundamental level of ambiguity that pervades the implementation of segregation of duties in digital systems. Thirdly, the growing reliance on automation is having a subtle impact on how auditors are applying and maintaining their professional skepticism. These three patterns indicate that the complexities of auditing in the ERP system environment are not simply a function of the technical characteristics of the system, but are also embedded in organizational practices and the day-to-day professional judgments that auditors must make when working in a complex digital system environment.

Theme 1: The Illusion of Integration and the Blurred Audit Trail

The literature suggests that ERP systems are viewed as having complete control over transactions since they are all integrated into one system. In reality, this integration does not necessarily make the audit process simpler. The system is usually set up to meet organizational needs, and access rights are not static. Therefore, tracing the sequence, context, and logic of certain transactions becomes more difficult rather than easier. What seems clear on the surface level may require a lot of interpretation when viewed at a closer level.

This state of affairs corresponds with the Sociotechnical Systems Theory (STS) approach to information risk, which views information risk as an emergent property of the interplay between technological systems and organizational processes (Coşkun et al., 2022; Setiawan, 2022). Information risk is not solely dependent on technological design; it is also dependent on the way in which users interact with and make sense of technological functionalities. This is further supported by Handayani et al. (2023), who note that a very high level of system integration can paradoxically increase traceability difficulties, as auditors are then forced to integrate technical system knowledge with professional judgment in order to properly interpret system-output information. In this way, information risk in the ERP system context cannot be said to be solely dependent on system failures. Instead, it is a function of the complex interplay between ERP system architecture, internal governance structures, and the auditor's interpretive capabilities. The inclusion of the auditor's lived experience, therefore, adds depth to current debates about the complexity of digital auditing.

Theme 2: Ambiguity in Segregation of Duties within Digital Contexts

The second theme emphasizes the conflict between efficiency in operations and the need to comply with the principles of internal control. In the context of ERP systems, segregation of duties (SoD) is strictly enforced by role-based access control. Nevertheless, access rights are often modified to meet operational requirements. This flexibility may lead to a situation where users are given multiple roles that, in an ideal control situation, are supposed to be separate. From an Institutional Theory viewpoint, such practices can be seen as organizational reactions to pressures from regulators and institutions (Elbardan et al., 2015; Widyaningdyah & Ezra, 2020). Organizations are forced to demonstrate compliance and maintain legitimacy while, at the same time, maintaining operations.

For auditors, this presents a complex professional environment. Control exceptions, which are temporarily justified as "temporary," can remain for extended periods of time, forcing auditors to continually assess risk in a situationally sanctioned but operationally ambiguous context. As Munthe et al. (2025) observe, this conundrum goes beyond technical issues. It represents the impact of social expectation, institutional pressures, and the auditor's need to preserve professional objectivity. Information risk, in this case, is not simply embedded in control system design but is continually enacted through the auditor's interpretation of organizational rules, practices, and limitations.

Theme 3: Automation Reliance and the Transformation of Professional Skepticism

The third theme relates to the increasing use of automation in ERP-based audit processes. The use of automated functionalities such as three-way matching and system-based approval processes reduces the need for manual verification of transactions. As a result, auditors are increasingly focusing on evaluating whether the system is operating as expected, rather than evaluating individual transactions. This is a manifestation of the shift in audit practice, where the emphasis is not on the economic event itself but on the reliability of information produced by the system.

The sensemaking theory (Ou & Wu, 2025) offers a valuable lens through which to examine the process of auditors making sense of exceptions or irregularities in highly automated settings. Even in situations where ERP systems are able to provide complete and up-to-date information, auditors are required to constantly use their professional judgment regarding the degree to which reliance can be placed on automated results. Gandasari and Mukhtaruddin (2025) suggest that over-reliance on automation can impair critical thinking, as automated system results may be taken at face value without adequate critical evaluation. In this respect, the problem moves from considerations of efficiency into the realm of epistemology, that is, the construction, validation, and challenge of audit knowledge in the digital age. While professional skepticism remains a core tenet, its application shifts as technology continues to impact audit evidence accessibility.

Integration of Findings and Contributions

Although these three issues are presented as separate themes, they are actually highly interrelated. The complexity that is implicit in these integrated ERP systems often leads to a centralization of access control mechanisms, while at the same time, the need for flexibility in operations leads to adaptive access planning that aims to move from manual monitoring to automated control. However, the growing dependence on automated systems also leads to a change in the way auditors use professional judgment when assessing evidence. When these factors are considered together, they support the argument that information risk in ERP-based expenditure cycle audits cannot be considered as a single or isolated concept.

CONCLUSION

This research reveals that information risk in ERP-supported expenditure cycle audits cannot be simplified to a technical issue, as it arises from the complex interplay between system design, organizational structures, and auditors' professional judgment. The results indicate that integrated information does not necessarily improve traceability, that flexible access control can impair transparency of internal controls, and that overdependence on automation can potentially reduce auditors' professional skepticism over time. These findings are consistent with the notion that information risk is a socio-technical phenomenon, which is constructed through the auditors' sense-making activities in the context of institutional pressures, system complexity, and daily audit work. From a theoretical perspective, this research contributes to the literature on auditing and ERPs by conceptualizing risk as a socially and professionally constructed phenomenon, rather than a systemically generated issue, providing a more refined understanding of role ambiguity and the efficiency-control integrity trade-off. From a practical perspective, the findings of this research imply the need for ERP system design and control structures that facilitate auditors' sense-making activities, as well as improved digital literacy and critical use of automation in the audit profession and education. Nonetheless, since the study relies exclusively on literature, future studies are encouraged to adopt either field or ethnographic research approaches in various sectors and environments to gain a deeper understanding of information risk in the digitally transformed audit environment from the lived experiences of auditors.

REFERENCES

Butarbutar, M., Sihotang, H., & Silalahi, A. (2023). Systematic literature review of critical success factors on enterprise resource planning post implementation. *Cogent Business & Management, 10*(3), Article 2264001. https://doi.org/10.1080/23311975.2023.2264001

Coşkun, S., Arslan, M., & Demirkan, H. (2022). ERP failure: A systematic mapping of the literature. *Data & Knowledge Engineering, 142*, 102090. https://doi.org/10.1016/j.datak.2022.102090

Datta, P., & Nwankpa, J. K. (2012). Perceived audit quality from ERP implementations. *Information Resources Management Journal, 25*(1), 61–80. https://doi.org/10.4018/IRMJ.2012010104

Elbardan, H., Ali, M., & Ghoneim, A. (2015). The dilemma of internal audit function adaptation: The impact of ERP and corporate governance pressures. *Journal of Enterprise Information Management, 28*(1), 93–106. https://doi.org/10.1108/JEIM-10-2013-0074

Gandasari, D., & Mukhtaruddin. (2025). Analysis of the impact of enterprise resource planning (ERP) and big data on improving company performance: A systematic literature review. *JURA ITB, 3*(2). https://doi.org/10.54066/jura-itb.v3i2.3216

Handayani, R., Utami, E., & Luthfi, E. T. (2023). Systematic literature review on auditing information technology risk management using the COBIT framework. *Prisma Sains, 11*(4). https://doi.org/10.33394/j-ps.v11i4.8871

Heuvel, E. van den. (2025). Evolution of IT auditing in a nutshell: Journey towards a dynamic landscape. *MAB, 99*(2), 73–83. https://doi.org/10.5117/mab.99.140994

Kristanti, O., Kuntadi, C., & Pramukty, R. (2023). Faktor-faktor yang mempengaruhi efektivitas sistem pengendalian internal: Peran audit internal, karakteristik auditor internal, dan kualitas audit internal. *Sentri, 2*(8). https://doi.org/10.55681/sentri.v2i8.1304

Kuntadi, C., & Pramukty, R. (2023). Literature review: Pengaruh sistem pengendalian internal, peran audit internal, dan komitmen manajemen terhadap good corporate governance. *Jurnal Economina, 2*(6), 1318–1330. https://doi.org/10.55681/economina.v2i6.605

Munthe, A., Mahulae, C., & Muda, I. (2025). Risk-based information system audit: A literature review and its implications in accounting. *Indonesia Economic Journal, 1*(2). https://doi.org/10.63822/zknzvm95

Ou, Q., & Wu, Y. (2025). The impact of digital transformation on auditor decision making. *Frontiers in Business, Economics and Management, 18*(2), 307–315. https://doi.org/10.54097/9pwzt443

Rajapakse, J., & Thushara, K. (2023). Critical failure factors in ERP implementation: A systematic literature review. *Journal of Business Technology, 7*(1). https://doi.org/10.4038/jbt.v7i1.109

Setiawan, D. E. (2022). Risk analysis in enterprise resource planning implementation: An ERP implementor's perspective. *Industry Xplore, 7*(2), 185–193. https://doi.org/10.36805/teknikindustri.v7i2.2852

Widyaningdyah, A. U., & Ezra, L. (2020). Enterprise resource planning (ERP) support for internal control effectiveness. *Jurnal Riset Akuntansi Kontemporer, 10*(2), 234–246. https://doi.org/10.22219/JRAK.V10I2.11507