Applied Computer Science 2026, vol. 22, no. 2, pp. 117–125
https://doi.org/10.35784/acs_8701

Submitted: 2025-11-08 | Revised: 2026-03-07 | Accepted: 2026-03-22

Keywords: internal audit, application controls, IT audit, ERP, systematic literature review

Sakchai TANGPRASERT [1], *Nalinpat BHUMPENPEIN* [1*]
[1] King Mongkut's University of Technology North Bangkok, Bangkok, Thailand, sakchai.t@sci.kmutnb.ac.th, nalinpat.b@itd.kmutnb.ac.th
[*] Corresponding author: nalinpat.b@itd.kmutnb.ac.th

Application control audit framework in the context of ERP systems

Abstract

The role of business operations driven by information technology systems is crucial, particularly the use of Enterprise Resource Planning (ERP) systems. Within organizations, both operational staff and management engage with ERP systems, which introduces potential vulnerabilities to operational errors or fraudulent activities. Consequently, auditing application controls becomes a matter. This study conducted a Systematic Literature Review (SLR) to investigate the scope of internal audit, with a focus on application control and associated risks. Based on the SLR results, an application controls audit framework for ERP is proposed. It consists of ten essential controls that must be implemented, including the software development process, access control, input control, process control, output control, change control, incident control, legal and ethical control, information security risk management, and continuity control. The framework evaluation, based on two case studies, demonstrated high effectiveness and received positive feedback from IT auditors, auditees, management, and executive boards.

1. INTRODUCTION

Today, organizations operate with increasingly diverse and complex business processes. Many aim to enhance operational efficiency, accuracy, error reduction, and fraud prevention (Laadar et al., 2019) to remain competitive in the business landscape. To achieve this, organizations have adopted Enterprise Resource Planning (ERP) systems to support their operations (Huang & Huang, 2012). To ensure the reliability of ERP systems, internal audits focusing on application controls are commonly conducted. However, there is currently no universal standard or framework to guide the auditing of application programs. Such a framework would validate the system's ability to process data accurately, ensure proper input controls and output displays, and maintain system stability during security incidents, while preventing user fraud. Although several studies have proposed various domains for auditing application programs, these domains often fail to comprehensively address the programs' quality and risk mitigation aspects (Song et al., 2011). Thus, this study aims to investigate the scope of internal audit, focusing on application control and associated risks, and develop an application controls audit framework.

2. SYSTEMATIC LITERATURE REVIEW

This study employs a Systematic Literature Review (SLR), a method for gathering the most relevant research while ensuring comprehensive and reliable information (Imran et al., 2023). SLR involves five steps: defining research questions; search strategy and selection process; data extraction and inclusion; quality assessment; and data analysis and synthesis.

2.1. Research question

This research aims to examine frameworks, audit programs, and domains of internal control, with a focus on application controls in the context of ERP systems. Thus, two research questions (RQs) guiding this review are as follows.

RQ1: What is the framework for internal auditing of application controls within the context of ERP systems?

RQ2: What are the risks affecting application controls within the context of ERP systems?

2.2. Search strategy and selection process

The review will be filtered by keywords of the papers, titles, abstracts, and primary papers published between 2010 and 2021 in the six reputable data sources, i.e., ACM, IEEE Xplore, Science Direct, Scopus, Springer, and Web of Science, used for selecting and collecting studies related to technology and information technology (Siemuri et al., 2022). The criteria and keywords used to search for relevant research were derived from the RQs. This process applied the principle of formulating search sentences (Khemakhem et al., 2022), where X represents internal audits, Y represents application controls, and Z represents ERP systems. These definitions were used to address the RQs. Based on the RQs, the following search sentences were formulated:

X = (Audit OR Auditing OR Control) AND (Framework OR Program)

Y = Risk OR Factor OR Domain

Z = Enterprise Resource Management OR ERP OR Enterprise Resource Management OR ERM

RQ1 = (X) AND Application Controls AND (Z)

RQ2 = (Y) AND Application Controls AND (Z)

This multi-step screening process ensures reliability and confidence that the selected papers are closely aligned with the RQs. Subsequently, the filtered papers that meet the predefined criteria will undergo further analysis and synthesis.

2.3. Data exclusion and inclusion process

The data extraction process was conducted using screening criteria and keywords identified to address the RQs. Selection criteria were established based on keywords, title, abstract, and metadata, respectively (Khan et al., 2013). To include a paper in this review, the paper must have been peer reviewed, available online, given permission to access, and written in English. Excluded from the search were editorials, prefaces, news, summaries of tutorials, panels, comments, and poster sessions. All papers that did not meet the inclusion criteria were excluded. This search strategy yielded 5,346, 608, 143, and 56 papers in the keyword, title, abstract, and primary selection stages, respectively.

Tab. 1. Number of papers in each selection stage

Criteria	RQ	Number of Papers							
		ACM	IEEE	Science Direct	Scopus	Springer	Web of Science	Total	
Keyword	RQ1	447	19	467	860	14	458	2,264	5,346
	RQ2	515	119	651	1,147	22	629	3,082	
Title	RQ1	80	6	62	68	6	46	268	608
	RQ2	65	55	45	102	5	68	340	
Abstract	RQ1	14	3	18	13	4	14	66	143
	RQ2	20	14	12	14	2	15	77	
Primary Paper	RQ1	9	2	4	1	4	1	21	56
	RQ2	5	13	9	6	2	0	35	

2.4. Quality assessment

We use quality assessment guided by Dybå and Dingsøyr (2008). The criteria encompass four main aspects, i.e., screening paper that aligns with the objectives of the study, rigor ensuring that clear objectives and appropriate explanation of the research details, reliability ensuring that the methodology and analysis of the results are conducted appropriately, and relevance ensuring that the relationship between the researchers and the sample groups is clearly explained. These aspects are defined in ten criteria, as shown in Table 2. Each criterion was graded on a dichotomous ("yes" or "no") scale. Finally, 56 papers out of the 143 papers graded "yes" on all criteria were accepted.

Tab. 2. Quality assessment criteria

Aspect	Criteria
Screening Paper	1. Is this paper a research article? 2. Are the paper objectives clearly defined? 3. Is the research context adequately described?
Rigor	4. Is the research design appropriate for addressing the research objectives and problems? 5. Are the strategies employed suitable for the research objectives? 6. Does the study collect data relevant to addressing the research problem? 7. Is the data analysis sufficiently reliable?
Reliability	8. Is the relationship between the researchers and the sample group clearly explained? 9. Are the findings clearly presented?
Relevance	10. Does the paper hold value for further research or practical application?

2.5. Data analysis and synthesis

This SLR employed an analytical approach and categorization method by Siemuri et al. (2022) and Petersen et al. (2008). EndNote was used to compile reference lists, which were then imported into Microsoft Excel to facilitate the research selection process and evaluate study quality.

3. RESEARCH RESULTS

Based on the SLR, the findings indicate that there are 10 categories of application/system controls in ERP systems, thereby answering RQ1. The first category is a software development process. To ensure that the software development process is accurate (Valdebenito & Quelopana, 2018), reliable, and of high quality, an appropriate method within the software development life cycle should be applied (Marques et al., 2023). Access control is a mechanism that ensures an organization establishes and frequently updates its relevant access policies (Iyer & Masoumzadeh, 2023). These policies should clearly define access rights, be officially approved through signed agreements, and undergo periodic reviews (Garrison et al., 2014). Input control ensures that data entered into the system is accurate, authorized by designated personnel, and compliant with predefined procedures (Meiryani et al., 2023). Process control ensures that all steps are accurate, complete, and reliable. Proper approval workflows and error-correction procedures should be in place, aligned with relevant regulations (Sun et al., 2023). Output control ensures the secure storage of data and any output generated by processes. Access permissions must be defined, with records maintained for data delivery and traceability. Outputs should align with the system's data and processes (Mamakou et al., 2024). Change control ensures that any system changes are planned, tested, approved, and implemented systematically (Fraga et al., 2024). Incident control ensures the continuous resolution of system issues. This includes tracking, summarizing, and preventing long-term problems (Manaf et al., 2021). Legal and ethical control ensures that an organization operates within legal standards and laws (Morales et al., 2022; Escher & Banovic, 2020), maintaining ethical practices and responsibility towards stakeholders. Information security risk management ensures that an organization evaluates and mitigates risks associated with its systems. This involves risk analysis and response planning to prevent business disruptions (Shaturaev, 2024). Lastly, Continuity control ensures that systems and data remain operational. This includes creating contingency plans, system recovery procedures, reliable backup architectures, and regular testing of these plans (Anshory et al., 2018).

Additionally, the findings indicate that 11 risks affect application controls in ERP systems, thereby answering RQ2. Physical and environmental risks encompass threats arising from natural disasters and human-made hazards (Costin & Dorian, 2019; Orosz et al., 2019). Human risks are those arising from personnel involved in IT and communication operations (Singh et al., 2023). This includes planning, task assignments, monitoring, and the delegation of roles and responsibilities among all stakeholders (Dong, 2023). Hardware and data communication risks refer to risks arising from equipment failures, improper relocation of devices, installation in unsuitable locations (Laadar et al., 2019), and threats such as computer viruses, malware, and trojans. Software risks refer to risks related to software operations, such as using outdated programs that are not updated to fix vulnerabilities. This could include exploitation of bugs by hackers or the use of unlicensed software, which could lead to lawsuits for copyright infringement (Handoko et al., 2023). Cyber risks refer to cyber threats involving activities that compromise IT systems or networks, resulting in harm to internal data or networks (Agarwal & Gupta, 2024). Database risks refer to risks associated with databases in IT systems

that could result in damage (Li et al., 2020). Strategic risks are those arising from changes in government policies or organizational leadership (Dantas et al., 2022). These changes can impact the formulation of strategies and IT-related tactics (Aniskina & Sorokin, 2020). Financial risks include insufficient budget allocation (Jørgensen, 2017) and delays in budget disbursement (Wang et al., 2020). Management risks refer to risks arising from inadequate management practices, such as a lack of well-structured operational plans and ineffective governance (Handoko & Amelia, 2021). Operational risks are risks affecting organizational operations (Anthony Jnr, 2019), stemming from human error, system failures, process inefficiencies, and natural disasters (Garg & Khurana, 2017; Deniswara et al., 2022). Lastly, fraud risks involve unethical or illegal practices, including bribery, offering or soliciting benefits, and the misuse of authority. Such activities contravene moral, ethical, and legal standards, as well as organizational rules and policies. Fraud poses a risk to the organization and the individuals involved (Schnepf et al., 2023).

4. APPLICATION CONTROLS AUDIT FRAMEWORK

Based on the answers to the RQs, an application controls audit framework for ERP systems is proposed. It consists of ten controls described as follows.

Control #1 Software Development Process: Effective supervision of the system development process ensures that the ERP system is error-free and meets organizational needs, without compromising its performance after implementation. Thus, all system development life cycle (SDLC) processes should be considered.

Control #2 Access Control: It is critical for organizations to clearly define roles and responsibilities and control system access through authorization. This prevents unauthorized access to data or unauthorized modifications, which could lead to operational errors or fraud. Thus, the following issues should be considered during an audit: clear policies on access rights, official signing, periodic review of access rights, alignment of granted rights with system configuration, and security policies.

Control #3 Input Control: This involves designing operational processes for data entry, ensuring a balance of checks and approvals between data input and verification. It helps mitigate data entry errors or unauthorized entries in ERP systems. Thus, the following issues should be considered during an audit, i.e., clear requirement elicitation processes, documentation verification between the development team and users, incorporation of regulatory requirements into documentation, continuous requirement review, system analysis and design using appropriate diagrams, business process flows with clear conditions and definition, use of standardized symbols, accurate data type definition, system approvals by authorized personnel, users accessing system within their privileges, system usage monitoring, prevention of incorrect data entry, proper database design and storage, and security design for input data.

Control #4 Process Control: This control focuses on verifying that those processes in the ERP system function correctly, particularly those involving calculations such as bill of materials, tax rates, interest rates, and penalties, by ensuring proper validation of formulas and source code. Thus, the following issues should be considered during an audit, i.e., clear assignment of approval rights, approvals with defined rights, processes complying with related regulations, processes aligning with business logic and facts, data management aligning with rights and business processes, written documentation for error corrections, system support for defined error corrections, robustness and fault-tolerance in error handling, and security design for processing data.

Control #5 Output Control: This process controls the system's outputs, such as reports on revenues and expenses, to ensure accuracy and prevent errors from incorrect data imports or faulty processing formulas. Thus, the following issues should be considered during an audit: consistency between actual data and results, traceable data and outputs, secure design for data output, proper data storage practices, documented access rights for data output, system rights aligned with policies, and output verification and validation.

Control #6 Change Control: ERP systems often need updates or changes in response to evolving organizational needs. The change control process ensures that any modifications to the system are tested, approved, and properly deployed to avoid errors that impact other business processes. Thus, the following issues should be considered during an audit, i.e., written change management process, process accessible to stakeholders, practices adherence to the process, bi-directional traceability matrix for impact analysis, risk assessment of scope, time, cost, and quality, formal approval for changes, separation of development and

production environments, comprehensive testing after updates, signed test documentation, version control, user training, and updated documentation.

Control #7 Incident Control: When issues or errors arise in the ERP system, it is crucial to document them and take corrective action. Incident management ensures that problems are addressed systematically, preventing future occurrences and helping improve system integrity. Thus, the following issues should be considered during an audit, i.e., reporting and resolving issues, tracking issues, issue summaries, and evaluation and review of preventive measures.

Control #8 Legal and Ethical Control: ERP systems must comply with relevant laws and regulations. This control also addresses the ethical aspects of handling personal and sensitive data, ensuring that the system adheres to privacy laws and governance standards. Thus, the following issues should be considered during an audit, i.e., validation of software licenses, adherence to intellectual property rights, compliance with legal procedures, and ethical and moral practices.

Control #9 Information Security Risk Management: This involves assessing and managing the security risks associated with the ERP system, including defining risk response strategies to ensure that the system supports the organization's operations effectively and securely. Thus, the following issues should be considered during an audit: risk analysis and responses to potential risks.

Control #10 Continuity Control: To prevent interruptions in business operations due to system failures, errors, or fraud, continuity control ensures the ERP system is prepared with disaster recovery plans and business continuity strategies, enabling it to recover and resume operations without disrupting organizational processes. Thus, the following issues should be considered during an audit, i.e., manuals or work instructions for operation, maintenance, and installation, suitable backup procedure and practice, reliable backup devices, regular backup plans, emergency response plans, periodic testing, and documented test results.

5. FRAMEWORK EVALUATION

The evaluation of the proposed application controls audit framework was conducted by three Information Technology (IT) auditors during Q4 of 2024 and Q1 of 2025. The framework was assessed for its applicability to auditing ERP (Enterprise Resource Planning) systems at two large-scale organizations. These included Organization A, a government agency, and Organization B, a private sector company. Both organizations had over 300 users using the ERP system. The audited ERP systems comprised 10 key modules, including general ledger, accounts payable, accounts receivable, fixed assets, cash management, budgeting, payroll, purchasing, sales, and inventory. Following the proposed framework guidance, IT auditors conducted audit reports, which were presented to the auditees, the relevant executive management, and the organization's audit committees. ERP usage data were collected through interviews based on five key questions: the purpose of ERP usage, the processes used within the ERP system, the benefits obtained from using the ERP system, problems and challenges in using the system, and risks or errors arising from ERP usage. Both risk and control criteria that influence risks and issues are divided into five levels, ranging from very low to extreme risk. The numbers shown in Table 3 represent the audit assessment scores for each control domain and risk category using a five-level scale ranging from 1 (very low) to 5 (very high). These scores reflect the auditors' evaluation of the effectiveness of the controls and the level of risk exposure identified in each organization.

Tab. 3. Comparison of audit results and risks found in the cases

Control	Org. A	Org. B	Risk Type	Org. A	Org. B
1. Software Development Process	3	3	1. Physical and Environmental Risk	2	3
2. Access Control	4	4	2. Human Risk	4	4
3. Input Control	3	4	3. Hardware and Data Communication Risk	4	3
4. Process Control	3	3	4. Software Risk	3	3
5. Output Control	3	3	5. Cyber Risk	4	4
6. Change Control	2	3	6. Database Risk	4	3
7. Incident Control	3	4	7. Strategic Risk	4	4
8. Legal and Ethical Control	4	5	8. Financial Risk	3	4
9. Information Security Risk Management	4	4	9. Management Risk	4	4
10. Continuity Control	4	4	10. Operational Risk	4	4
			11. Fraud Risk	3	4

After official auditing, a questionnaire was used to evaluate the utilization of the proposed framework. Feedback was gathered from participating auditors, auditees, executive management, and audit committee members from both organizations, with 20 respondents per organization, for a total of 40. The evaluation revealed that the proposed framework achieved an average accuracy of 91.19% in auditing applications. The audit results were also well received, with an average reliability score of 92.43%. The evaluation demonstrated that the framework enhanced the efficiency of application audits, achieving an average score of 95.24%. When applied to auditing applications with diverse processes, modules, and functions, the framework exhibited flexibility, enabling effective auditing across contexts. Moreover, the framework was found to be conducive to practical use, with an average usability score of 87.68%. Overall, the evaluation across all five aspects indicated that the framework was highly accepted and effective among its users.

6. DISCUSSION AND CONCLUSION

This research proposed an application controls audit framework for ERP systems, based on findings from a systematic literature review. The proposed framework consists of ten essential controls that must be implemented, including software development process control, access control, input control, process control, output control, change control, incident control, legal and ethical control, information security risk management, and continuity control. Compared with traditional application audits commonly performed by auditors and leading accounting firms such as the Big 4 CPA firms (Handoko et al., 2022), which typically focus on only four control domains—access control, input control, output control, and change control—the proposed framework provides broader coverage of application-level risks. These traditional domains do not sufficiently address the full range of IT and organizational risks that may arise in ERP environments. Within the proposed framework, the Software Development Process domain provides insight into ERP system development. A well-designed development process enhances system performance, whereas poorly designed development practices may introduce errors and increase fraud risk (Yadav et al., 2024). The Process Control domain helps ensure the accuracy of formulas, calculations, and coding used within ERP systems. This domain also contributes to preventing financial risks (Popchev et al., 2021) and ensuring compliance with organizational policies, regulations, and applicable laws (Fahrezy et al., 2025). The Incident Control domain plays a crucial role in identifying issues arising from human errors (Seidelin et al., 2022), operational mistakes (Cloete et al., 2020), and system bugs. The Legal and Ethical Control domain helps prevent database risks, protects personal data (Lucaj et al., 2023), and mitigates strategic and management risks (Wen et al., 2020). Furthermore, the Information Security Risk Management domain and the Continuity Control domain are critical for managing risks during ERP system disruptions (Zambon et al., 2007). These controls support organizations in planning and responding to incidents caused by physical and environmental threats, hardware or communication failures, and cyberattacks (Sabillon & Barr, 2024). In addition, the framework was evaluated using two case studies. The findings revealed that the framework demonstrated flexibility and could thoroughly cover the necessary areas of control and risk prevention in ERP system development and use.

The proposed framework also complements existing IT governance and audit frameworks, such as COBIT, as well as risk-based IT audit methodologies. While COBIT provides high-level governance and control objectives for enterprise IT management, the framework proposed in this study focuses specifically on application-level controls within ERP systems. The ten-control structure was derived from empirical evidence obtained through a systematic literature review and therefore provides a practical checklist for auditors when evaluating ERP applications. In this sense, the framework extends traditional application audit approaches by incorporating development, incident, legal, and continuity controls that are often overlooked in conventional audits.

While the framework provides a structured set of control domains for auditing ERP applications, the present study primarily focuses on the conceptual development of an application controls audit framework derived from a systematic literature review and validated through case studies. Quantitative metrics such as risk-reduction indices or control-coverage ratios were not formally implemented in the current research. Future studies may extend this work by incorporating quantitative evaluation models to measure audit effectiveness and risk mitigation capabilities in ERP environments.

In addition, although the evaluation was conducted in traditional ERP environments, the proposed framework is adaptable to modern ERP deployment models, including cloud-based ERP systems and highly customized ERP implementations. Because the framework focuses on fundamental application control

principles such as access management, process integrity, change control, and continuity planning, these controls remain applicable across different technological architectures. Therefore, the framework can potentially support auditing practices in contemporary enterprise systems where ERP solutions are increasingly integrated with cloud services and emerging technologies.

Funding

This research was funded by the Faculty of Applied Science, King Mongkut's University of Technology North Bangkok, Thailand, contract no. 673191

Conflict of Interest

The authors declare that they have no competing interests.

REFERENCES

Agarwal, P., & Gupta, A. (2024, May 3–4). *Cybersecurity strategies for safe ERP/CRM implementation* [Paper presentation]. 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT). https://doi.org/10.1109/AIIoT58432.2024.10574707

Aniskina, N. N., & Sorokin, A. V. (2020, September 7–11). *Risk management in running ERP-based process model of integrated group of companies* [Paper presentation]. 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). https://doi.org/10.1109/ITQMIS51053.2020.9322891

Anshory, B. J., Sfenrianto, S., Kaburuan, E. R., Peranginangin, E., & Fadhila, Q. (2018, October 23–26). *Information system audit in SaaS start-up company using COBIT 4.1 focus on deliver and support domain* [Paper presentation]. 2018 International Conference on Orange Technologies (ICOT). https://doi.org/10.1109/ICOT.2018.8705886

Anthony Jnr, B. (2019). Validating the usability attributes of AHP-software risk prioritization model using partial least square-structural equation modeling. *Journal of Science and Technology Policy Management, 10*(2), 404–430. https://doi.org/10.1108/JSTPM-06-2018-0060

Cloete, R., Norval, C., & Singh, J. (2020). A call for auditable virtual, augmented and mixed reality. In *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*. Association for Computing Machinery. https://doi.org/10.1145/3385956.3418960

Costin, B. V., & Dorian, C. (2019, October 9–11). *Global rollouts - risks and factors that affect ERP solutions in Romania - A case study in the sales and distribution area* [Paper presentation]. 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC). https://doi.org/10.1109/ICSTCC.2019.8885535

Dantas, E., Neto, A. S., Valadares, D., Perkusich, M., Ramos, F., Almeida, H., & Perkusich, A. (2022). Investigating technological risks and mitigation strategies in software projects. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*. Association for Computing Machinery. https://doi.org/10.1145/3477314.3507062

Deniswara, K., Prabowo, H., & Mulyawan, A. N. (2022). Digital business transformation: Exploration of the use of ERP based private cloud to improve managing system in the company (Case study on one of public company in Indonesia). In *Proceedings of the 7th International Conference on Industrial and Business Engineering*. Association for Computing Machinery. https://doi.org/10.1145/3494583.3494599

Dong, W. (2023). A study on the construction of human resources audit management platform based on big data. In *Proceedings of the 2022 6th International Conference on Software and e-Business*. Association for Computing Machinery. https://doi.org/10.1145/3578997.3579017

Dybå, T., & Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and Software Technology, 50*(9–10), 833–859. https://doi.org/10.1016/j.infsof.2008.01.006

Escher, N., & Banovic, N. (2020). Exposing error in poverty management technology: A method for auditing government benefits screening tools. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW1), Article 64. https://doi.org/10.1145/3392874

Fahrezy, M. D., Tjahyadi, R., & Kurniawati, H. (2025, February 3–4). *Blockchain adoption in financial audit: A review* [Paper presentation]. 2025 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS). https://doi.org/10.1109/ICADEIS65852.2025.10933126

Fraga, C., Abelém, A., Borges, V., Pinheiro, B., & Cordeiro, W. (2024, May 6–10). *A blockchain-based approach for continuous auditing in IT change management* [Paper presentation]. NOMS 2024-2024 IEEE Network Operations and Management Symposium. https://doi.org/10.1109/NOMS59830.2024.10575576

Garg, P., & Khurana, R. (2017). Applying structural equation model to study the critical risks in ERP implementation in Indian retail. *Benchmarking: An International Journal, 24*(1), 143–162. https://doi.org/10.1108/BIJ-12-2015-0122

Garrison, W. C., Lee, A. J., & Hinrichs, T. L. (2014). An actor-based, application-aware access control evaluation framework. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*. Association for Computing Machinery. https://doi.org/10.1145/2613087.2613099

Handoko, B. L., & Amelia, R. (2021). Implementation of good corporate governance, internal audit, whistle-blowing system for fraud prevention in state-owned enterprise. In *Proceedings of the 2021 12th International Conference on E-business, Management and Economics*. Association for Computing Machinery. https://doi.org/10.1145/3481127.3481144

Handoko, B. L., Gunawan, B. A., & Djati, M. F. P. (2022). Importance of blockchain within the Big 4 CPA firms: Cryptocurrency's existence. In *Proceedings of the 6th International Conference on E-Commerce, E-Business and E-Government*. Association for Computing Machinery. https://doi.org/10.1145/3537693.3537718

Handoko, B. L., Melisa, M., & Reinaldy, N. (2023). External auditors' perception of use of virtual reality in financial statement auditing process. In *Proceedings of the 2022 6th International Conference on Software and e-Business*. Association for Computing Machinery. https://doi.org/10.1145/3578997.3579002

Huang, L., & Huang, H. (2012, May 19–20). *ERP system architecture in the process of selection game* [Paper presentation]. 2012 International Conference on Systems and Informatics (ICSAI2012).

Imran, M., Hamid, S., & Ismail, M. A. (2023). Advancing process audits with process mining: A systematic review of trends, challenges, and opportunities. *IEEE Access, 11*, 68340–68357. https://doi.org/10.1109/ACCESS.2023.3292117

Iyer, P., & Masoumzadeh, A. (2023). Towards automated learning of access control policies enforced by web applications. In *Proceedings of the 28th ACM Symposium on Access Control Models and Technologies*. Association for Computing Machinery. https://doi.org/10.1145/3589608.3594743

Jørgensen, M. (2017). Software development contracts: The impact of the provider's risk of financial loss on project success. In *Proceedings of the 10th International Workshop on Cooperative and Human Aspects of Software Engineering*. IEEE. https://doi.org/10.1109/CHASE.2017.1

Khan, H. H., Mahrin, M. N. b., & Chuprat, S. b. (2013, December 2–4). *Situational requirement engineering: A systematic literature review protocol* [Paper presentation]. 2013 IEEE Conference on Open Systems (ICOS). https://doi.org/10.1109/ICOS.2013.6735060

Khemakhem, F., Ellouzi, H., Ltifi, H., & Ayed, M. B. (2022). Agent-based intelligent decision support systems: A systematic review. *IEEE Transactions on Cognitive and Developmental Systems, 14*(1), 20–34. https://doi.org/10.1109/TCDS.2020.3030571

Laadar, H. B., Cherti, I., & Bahaj, M. (2019). ERP systems in SMEs between a choice & an obligation. In *Proceedings of the 2019 8th International Conference on Educational and Information Technology*. Association for Computing Machinery. https://doi.org/10.1145/3318396.3318438

Li, X., Cao, C., & Yin, Y. (2020). Risk analysis of ERP in FY coal-fired power enterprises. In *Proceedings of the 2020 4th International Conference on Management Engineering, Software Engineering and Service Sciences*. Association for Computing Machinery. https://doi.org/10.1145/3380625.3380631

Lucaj, L., Smagt, P. v. d., & Benbouzid, D. (2023). AI regulation is (not) all you need. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. Association for Computing Machinery. https://doi.org/10.1145/3593013.3594079

Mamakou, X. J., Cohen, S., & Manolopoulos, D. (2024). Post-implementation evaluation of enterprise resource planning (ERP) systems: An internal auditors' perspective. *Journal of Systems and Information Technology, 26*(3), 363–394. https://doi.org/10.1108/JSIT-11-2023-0264

Manaf, K., Subaeki, B., Solihin, H. H., Pitara, S. W., Hidayat, S., & Laluma, R. H. (2021, November 18–19). *Digital report application audit using the COBIT 5 framework* [Paper presentation]. 2021 15th International Conference on Telecommunication Systems, Services, and Applications (TSSA). https://doi.org/10.1109/TSSA52866.2021.9768264

Marques, J., Yelisetty, S., Slavov, T., & Barros, L. (2023). Enhancing aviation software development: An experience report on conducting audits. In *Proceedings of the XXII Brazilian Symposium on Software Quality*. Association for Computing Machinery. https://doi.org/10.1145/3629479.3629505

Meiryani, M., Patricia, S., & Presillia, S. (2023). The effect of computerized accounting information systems, big data analysis, and internal audit in accounting fraud detection. In *Proceedings of the 2023 8th International Conference on Big Data and Computing*. Association for Computing Machinery. https://doi.org/10.1145/3624288.3624290

Morales, H. R., Porporato, M., & Epelbaum, N. (2022). Benford's law for integrity tests of high-volume databases: A case study of internal audit in a state-owned enterprise. *Journal of Economics, Finance and Administrative Science, 27*(53), 154–174. https://doi.org/10.1108/JEFAS-07-2021-0113

Orosz, I., Selmeci, A., & Orosz, T. (2019, January 24–26). *Software as a Service operation model in cloud based ERP systems* [Paper presentation]. 2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI). https://doi.org/10.1109/SAMI.2019.8782739

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). *Systematic mapping studies in software engineering* [Paper presentation]. 12th International Conference on Evaluation and Assessment in Software Engineering. https://doi.org/10.14236/ewic/EASE2008.8

Popchev, I., Radeva, I., & Velichkova, V. (2021, October 28–29). *The impact of blockchain on internal audit* [Paper presentation]. 2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE). https://doi.org/10.1109/BdKCSE53180.2021.9627276

Sabillon, R., & Barr, M. (2024, April 15–18). *Planning and conducting cybersecurity audits to assess the effectiveness of controls* [Paper presentation]. 2024 IEEE International Systems Conference (SysCon). https://doi.org/10.1109/SysCon61195.2024.10553588

Schnepf, J., Scheuermann, B., & Vetter, P. (2023, December 15–18). *Analyzing data sets for ML-driven fraud detection in SAP systems* [Paper presentation]. 2023 IEEE International Conference on Big Data (BigData). https://doi.org/10.1109/BigData59044.2023.10386379

Seidelin, C., Moreau, T., Shklovski, I., & Møller, N. H. (2022). Auditing risk prediction of long-term unemployment. *Proceedings of the ACM on Human-Computer Interaction, 6*(GROUP), Article 8. https://doi.org/10.1145/3492827

Shaturaev, J. (2024). Modeling the impact of information on audits on taxpayer risk profiles and evasions. In *Proceedings of the 7th International Conference on Future Networks and Distributed Systems*. Association for Computing Machinery. https://doi.org/10.1145/3644713.3644735

Siemuri, A., Selvan, K., Kuusniemi, H., Valisuo, P., & Elmusrati, M. S. (2022). A systematic review of machine learning techniques for GNSS use cases. *IEEE Transactions on Aerospace and Electronic Systems, 58*(6), 5043–5077. https://doi.org/10.1109/TAES.2022.3219366

Singh, S., Singh, S., & Misra, S. C. (2023). Post-implementation challenges of ERP system in pharmaceutical companies. *International Journal of Quality & Reliability Management, 40*(4), 889–921. https://doi.org/10.1108/IJQRM-10-2020-0333

Song, Y., Yin, M., Meng, F., & Ding, X. (2011, November 26–27). *Enterprise internal controlling risks and prevention within ERP system* [Paper presentation]. 2011 International Conference on Information Management, Innovation Management and Industrial Engineering.

Sun, Y., Zhang, X., & Han, M. (2023). Research on the application of blockchain technology in big data auditing. In *Proceedings of the 2023 3rd International Conference on Robotics and Control Engineering*. Association for Computing Machinery. https://doi.org/10.1145/3598151.3598160

Valdebenito, J., & Quelopana, A. (2018). Understanding the landscape of research in Enterprise Resource Planning (ERP) systems adoption. In *Proceedings of the 2018 International Conference on Computers in Management and Business*. Association for Computing Machinery. https://doi.org/10.1145/3232174.3232178

Wang, K., Zhang, Y., & Chang, E. (2020). A conceptual model for blockchain-based auditing information system. In *Proceedings of the 2nd International Electronics Communication Conference*. Association for Computing Machinery. https://doi.org/10.1145/3409934.3409949

Wen, C. Y., Ying, S. L. X., & Nair, R. K. (2020). The responsibility of internal auditors in preventing fraud in Malaysia listed companies. In *Proceedings of the 2019 2nd International Conference on E-Business, Information Management and Computer Science*. Association for Computing Machinery. https://doi.org/10.1145/3377817.3377831

Yadav, T., Kulkarni, P., Balaji, C. G., & Chirputkar, A. (2024, November 25). *Application of big data analytics in internal audit of banks* [Paper presentation]. 2024 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM). https://doi.org/10.1109/IIPEM62726.2024.10925684

Zambon, E., Bolzoni, D., Etalle, S., & Salvato, M. (2007, July 1–5). *A model supporting business continuity auditing and planning in information systems* [Paper presentation]. Second International Conference on Internet Monitoring and Protection (ICIMP 2007). https://doi.org/10.1109/ICIMP.2007.4