

Risk Management and Internal Controls in the Use of Generative Artificial Intelligence: An Integrated Framework for Organizations and Internal Audit

Abstract: *This paper examines the management of risks associated with the use of generative artificial intelligence (GenAI) within internal control systems and corporate governance. Based on a structured review of peer-reviewed literature, an integrated framework for risk management, internal controls, and internal audit is developed. Nine risk categories are linked to preventive and detective controls, responsible functions, and internal audit procedures. Internal audit is positioned as an independent function responsible for assessing the adequacy and effectiveness of the system, while accountability for risks and controls remains with management.*

Keywords: *generative artificial intelligence, internal controls, risk management, internal audit, AI governance*

¹ Ekspedicija, Belgrade, Serbia.

E-mail: milos@ekspedicija.rs

ORCID iD: <https://orcid.org/0009-0000-9537-4651>

² Office for Information Technologies and eGovernment, Belgrade, Serbia.

E-mail: sofija.vukmirovic@ite.gov.rs

ORCID iD: <https://orcid.org/0009-0003-7367-3230>

³ Faculty of Organizational Sciences, University of Belgrade, Serbia.

E-mail: rm20253253@student.fon.bg.ac.rs

ORCID iD: <https://orcid.org/0009-0008-5345-4168>

⁴ Faculty of Organizational Sciences, University of Belgrade, Serbia.

E-mail: dz20253254@student.fon.bg.ac.rs

ORCID iD: <https://orcid.org/0009-0008-5345-4168>

INTRODUCTION

Generative artificial intelligence (GenAI) has evolved from a highly specialized technology into a general-purpose interface used for writing, analysis, software development, customer support, finance, human resources, and the preparation of management decisions. Its organizational significance stems not only from the capabilities of the models themselves, but also from the fact that employees can integrate them into existing workflows without a formal redesign of business processes. A domestic academic foundation for understanding the principles and business applications of generative artificial intelligence is provided by Vukmirović and Jovanović-Milenković (22).

The key governance question, therefore, is not merely whether a model can generate a useful response, but whether an organization can use it repeatedly under clearly defined conditions, with an acceptable level of error, protected data, clear accountability, and an auditable decision trail. Research on human–AI collaboration indicates that automation and augmentation cannot be fully separated, because the introduction of AI changes the allocation of tasks, the need for verification, and the role of professional judgment (8, 18). A meta-analysis of human–AI systems further shows that combining humans and AI does not automatically produce better results than those achieved by the better-performing actor working independently; outcomes depend on the type of task and the relative capabilities of the human and the system (21).

The auditing literature presents a similarly balanced picture. Earlier studies highlighted the potential of AI to automate and expand audit procedures (12), while a large empirical study associates audit firms' investments in AI with higher audit quality and efficiency (4). More recent research, however, also identifies concerns regarding explainability, bias, data privacy, robustness, reliability, and auditors' overreliance on AI (11). Ethical analyses of AI use in auditing likewise emphasize accountability and governance rather than technical performance alone (17).

In the context of GenAI implementation itself, the control challenge extends beyond the question of how auditors use AI. Organizations may use public or embedded models, internal assistants, and AI-enabled functionalities across a wide range of processes. The scope of internal audit may therefore include assessing whether management has identified such uses, assigned appropriate owners, protected information, established validation and escalation rules, documented changes, and monitored outcomes. The literature on AI governance shows that accountability, life-cycle coverage, and organization-wide governance remain key issues (2), while research on how systems based on large language models should be evaluated and audited points to the need to consider simultaneously system governance, the characteristics and limitations of the model, and its specific application context (16).

The aim of this paper is to develop an integrated framework for risk management, internal controls, and internal audit in the organizational use of GenAI. The analysis is guided by four research questions: **RQ1:** What are the most significant risks when GenAI is integrated into business processes? **RQ2:** Which preventive and detective internal controls can mitigate

these risks? **RQ3:** How should responsibilities be allocated among management, process owners, technology and risk functions, and internal audit? **RQ4:** What evidence and procedures can internal audit use to assess the design and operating effectiveness of GenAI controls? The contribution of the paper is practical, while remaining grounded in the scientific literature: control objectives are translated into specific controls and verifiable audit evidence.

METHODOLOGY

The paper applies a structured integrative review and conceptual synthesis. The review focuses on peer-reviewed studies and academic books from five interrelated areas: AI governance and accountability; human–AI interaction and automation bias; data and model documentation; auditing of algorithms and large language models; and the application of AI in accounting, external audit, and internal audit. Priority was given to sources published between 2018 and 2026, while older studies were retained where they provide a relevant theoretical or methodological foundation.

The reference base deliberately excludes blogs, commercial white papers, and promotional materials produced by vendors. The sources used include systematic reviews and meta-analyses, conceptual papers published in leading journals, empirical studies in accounting and auditing, peer-reviewed research on AI governance, and two studies previously published in the journal *Revizor*. The systematic review of AI governance (2), the review of AI in auditing (1), and the meta-analysis of human–AI performance (21) served as key sources for the synthesis, while empirical findings were used to assess whether the proposed control approach is consistent with problems observed in real-world applications.

Table 1. Analytical Areas and Evidence Base

Analytical area	Key control question	Representative scientific evidence
AI governance and accountability	Who governs the AI system, what is subject to governance, and across which stages of the life cycle?	Reviews of AI governance and ethical auditing (2, 5, 15).
Human–AI interaction and oversight	Where must human judgment remain meaningful, and how can overreliance on AI be reduced?	Human–AI symbiosis, automation bias, augmentation, and human-centered AI (7, 8, 18, 20, 21).
Data and model documentation	Can data provenance, intended use, limitations, and model context be reconstructed?	Datasheets and model cards (6, 13).
AI/LLM auditing and independent audit assessment	Which levels of governance, model behavior, and specific applications require independent audit assessment?	Algorithm and LLM audits; internal audit research (15, 16, 23).
Applications in accounting and auditing	What benefits and risks of AI adoption have been documented in professional auditing practice?	Empirical, field-based, and review evidence (1, 4, 9, 11, 12, 17).

The analytical procedure consisted of three steps. First, the findings were coded according to key control questions: what potential errors may occur, why their consequences matter, who can influence the risk, what evidence demonstrates that a control has been performed, and how an independent auditor can test that evidence. Second, related findings were grouped into nine risk categories: output reliability, exposure of confidential data, bias and unfair outcomes, overreliance on AI, insufficient traceability, changes in models or configurations, third-party dependency, unclear accountability, and effects on work design and employee monitoring. Third, each category was translated into a control objective, preventive or detective controls, a responsible function, and a feasible audit test. The resulting framework represents a conceptual synthesis rather than an empirically validated control standard.

Table 1 presents the analytical areas and their role in the synthesis.

RESULTS AND DISCUSSION

Generative AI as an Internal Control Challenge

Conventional application controls generally assume that a system executes predefined logic on structured inputs. GenAI introduces a different control profile: outputs are probabilistic, the model may be used for purposes that were not precisely defined at the time of implementation, and interaction often takes place through natural language. The same model may support both the drafting of a low-risk text and a decision with serious consequences. Accordingly, intended use, context, and human accountability become fundamental control attributes.

The first implication is the need to distinguish technical capability from organizational reliability. Empirical research demonstrates significant productivity gains in clearly defined tasks; for example, a field study in customer support reports substantial productivity improvements, with particularly pronounced benefits among less experienced employees (3). At the same time, research on automation bias shows that system assistance may create new pathways to error when users uncritically accept a recommendation or fail to verify omitted information (7). Human-centered AI therefore requires visibility, the possibility of human intervention, and an appropriate level of control (20).

The second implication concerns accountability. An algorithm may recommend, classify, generate, or prioritize, but organizational accountability cannot be delegated to the model. Research on algorithmic management shows that digital systems redistribute managerial visibility and control, while also potentially creating problems of contestability and lack of transparency for employees (10). A meta-analysis of electronic monitoring finds no overall increase in performance, but does identify higher levels of stress, while more transparent and less intrusive systems are associated with more favorable employee attitudes (19). Control assessment must therefore also encompass the ways in which AI changes authority, oversight, and the ability to challenge a decision.

The third implication is that documentation becomes part of the control itself. *Data-sheets for Datasets* were proposed to improve visibility into data provenance, collection methods, limitations, and appropriate uses (6), while model cards formalize the intended use, evaluation conditions, and limitations of models (13). In the context of large language models, this logic extends to the governance, model, and application levels (16). Organizations therefore require an audit trail linking the approved use case, data-handling rules, model or service version, validation results, accountable owner, human review, and monitored outcomes.

Taxonomy of Risks in the Organizational Use of GenAI

The literature supports a broader risk taxonomy than the problem of “hallucinations” alone. Output reliability is the most visible risk, as a plausible response may contain factual, logical, or contextual errors. Research on the assessment and auditing of systems based on large language models emphasizes that performance should be evaluated in relation to the specific application rather than inferred from the model’s general capabilities (16). The second risk is the exposure of confidential data through prompts, attachments, retrieval documents, or generated outputs. The third is bias and unfair outcomes, particularly when AI influences decisions concerning individuals. Ethical frameworks consistently identify fairness, autonomy, beneficence, non-maleficence, and explainability as key principles (5), while ethical auditing requires these principles to be operationalized rather than merely accepted at a declarative level (15).

The fourth risk is overreliance on the model, a phenomenon known as automation bias. The literature on this phenomenon describes commission errors, in which users accept an incorrect automated recommendation, and omission errors, in which users fail to act because the system does not provide an appropriate signal (7). In the case of GenAI, this risk is amplified by fluent and persuasive language. The fifth risk is insufficient traceability: without the ability to reconstruct the data, instructions, system version, and human decision, it is difficult to investigate an incident or conduct a reliable independent audit assessment. The sixth risk concerns changes to the model or its configuration. Cloud-based models, system instructions, retrieval sources, and workflows may change over time, meaning that a control that was valid for one configuration may require revalidation following a material change.

The remaining risks are organizational in nature. Third-party dependency arises when a process depends on a vendor for availability, security, model behavior, or notification of changes. Unclear accountability occurs when the process owner, technology team, and end user each assume that responsibility lies with someone else. Finally, work design and monitoring risk arises when AI is used to intensify work, evaluate employees, or introduce non-transparent changes to performance criteria. The automation–augmentation paradox shows that AI can simultaneously automate certain activities while augmenting others, making the design of human and machine roles correspondingly important (18).

Integrated Framework for Risk Management, Internal Controls, and Internal Audit

Table 2 translates the nine risk categories into a control architecture. The underlying principle is proportionality of low risks. Nevertheless, every material use case should have a designated owner, rules governing permitted data, a defined validation method, and an escalation path for situations in which an output is uncertain or materially incorrect.

Table 2. Integrated Matrix of Risk Management, Internal Controls, and Internal Audit for GenAI

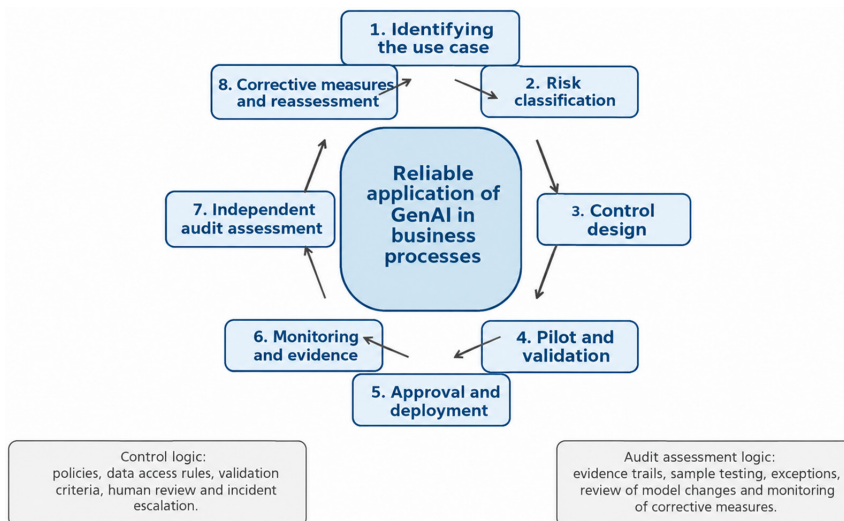
Risk	Control objective	Illustrative preventive/detective controls	Illustrative audit evidence and test
Output reliability	Keep material errors within an accepted tolerance.	Representative validation cases; mandatory expert review of material outputs; source requirements where feasible.	Reperform a sample of tests; compare outputs with approved evidence; review reviewer sign-offs and exceptions.
Exposure of confidential data	Prevent unauthorized disclosure or processing of sensitive information.	Approved tools; data classification; least-privilege access; rules for prompts and attachments; protected retrieval sources.	Review configurations and access rights; sample relevant logs and inputs; trace breaches through to corrective actions.
Bias and unfair outcomes	Detect and limit systematically adverse effects on relevant groups.	Pre-deployment testing; representative test cases; human review; escalation of disputed outcomes.	Review test design; compare outcomes across relevant groups where appropriate; review complaints and overrides.
Overreliance on AI	Preserve independent professional judgment.	Reviewer training; explicit verification criteria; override capability; independent review for high-impact applications.	Trace a sample of decisions to documented human rationale; review overrides; interview relevant personnel regarding escalation criteria.
Insufficient traceability	Enable reconstruction of an AI-supported process.	Recording of the use case, model/service version, key inputs, approvals, and final decision.	Reconstruct selected cases from end to end and test the completeness of the audit trail.
Model changes	Preserve the validity of controls following a material change.	Change register; risk-based revalidation; approval thresholds for changes to the model, prompt, retrieval process, or workflow.	Sample changes and verify approval, impact assessment, and revalidation.
Third-party dependency	Manage vendor, continuity, and service-change risks.	Due diligence; contractual requirements; change notifications; contingency procedures for material processes.	Review due diligence, contracts/SLAs, incident history, and evidence of vendor changes.
Unclear accountability	Ensure a designated human owner for each material application and decision.	Designated process owner; responsibility matrix; clear ownership of escalation and incident management.	Trace a sample of issues and decisions to accountable owners; review approvals and corrective actions.
Effects on work design/monitoring	Avoid non-transparent or disproportionate use of AI in employee monitoring and control.	Purpose limitation; transparent metrics; review of monitoring intensity; feedback and escalation channels.	Compare the stated purpose with actual data use; review monitoring outcomes, complaints, and actions taken.

Preventive controls can reduce exposure by restricting risky behavior before an output enters a business process. Examples include lists of approved tools, data classification, authorization of use cases, access rights, documented human review, and validation using representative cases. Detective controls are necessary because GenAI behavior cannot be fully specified in advance. Earlier research published in Revizor has already indicated that computerized environments can simultaneously strengthen certain controls and introduce new issues requiring adaptations to internal control systems (14).

The framework distinguishes between the control itself and evidence that the control has actually been performed. A policy requiring the review of AI outputs does not, by itself, demonstrate that the control is operating effectively, nor does it provide a sufficient basis for an independent audit assessment. For internal audit, it is essential that a selected case can be traced from its business purpose and AI use through human approval to the final outcome. The literature on algorithm auditing similarly emphasizes the need to translate broad objectives of accountability, fairness, and transparency into verifiable technical and organizational practices (15, 16).

Figure 1 synthesizes the proposed life cycle through which an organization can transform experimental GenAI use into a controlled and auditable application.

Figure 1. Cycle of Controlled Implementation and Independent Audit Assessment of Organizational GenAI Use



Allocation of Responsibilities and the Role of Internal Audit

The proposed framework assigns primary responsibility according to the business process rather than the technological label. The board of directors or senior management determines risk tolerance and requires visibility into material AI applications. The process

owner remains accountable for the business outcome, since only that function can assess the appropriateness of AI support and the acceptability of the consequences of error. Technology and data functions manage integration, access, configuration, logging, and technical changes, while risk, compliance, privacy, and security functions provide challenge and establish constraints within their respective areas of responsibility.

Figure 2 graphically presents the governance levels and boundaries of responsibility in the organizational use of GenAI.

Figure 2. Governance Structure and Allocation of Responsibilities for Organizational GenAI Use

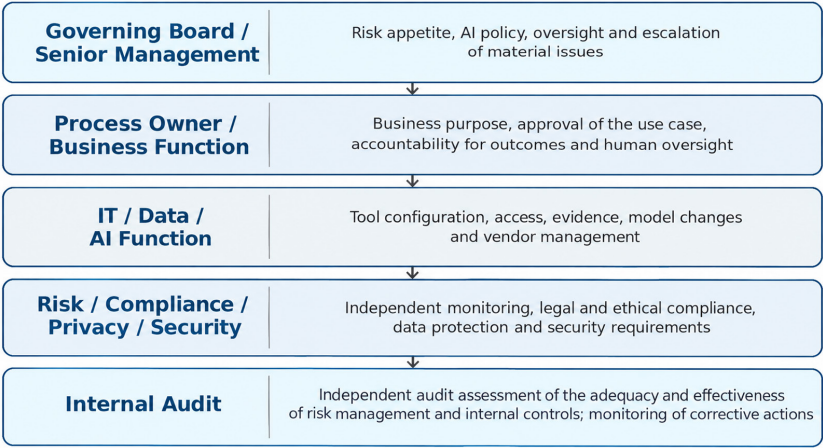


Table 3. Allocation of Responsibilities for Organizational GenAI Use

Organizational function	Primary responsibility for GenAI governance
Board of directors / senior management	Define risk tolerance; ensure visibility into material GenAI use; assign executive accountability; review unresolved high-risk issues.
Business function / process owner	Own the business purpose and outcome; define acceptable quality; approve the use case; ensure meaningful human decision-making and remediation of adverse consequences.
IT / data / AI function	Manage approved services, access, integration, configuration, logging, validation support, versions, and changes.
Risk / compliance / privacy / security	Define specialist requirements and independently challenge risk classification, data handling, fairness, security, and regulatory implications within their respective areas of responsibility.
Internal audit	Independently assess the adequacy and effectiveness of governance, risk management, and internal controls; report weaknesses and follow up on corrective actions; refrain from assuming management control responsibilities.

Internal audit occupies a different position. Its role is to independently assess whether governance, risk management, and internal controls are adequately designed and operating effectively, rather than to own the AI inventory, approve individual prompts, or perform

management validation. Research on the future of internal audit indicates that AI increases the need for new competencies and strategic oversight while preserving internal audit's role as an independent assurance function (23). An earlier study published in *Revizor* on AI in auditing also points to the tension between efficiency benefits and risks relating to human oversight and confidential information (9). The present paper extends this discussion from auditors' use of AI to the auditability of AI use across the entire organization.

Table 3 summarizes the proposed allocation of responsibilities. A practical rule is that every control weakness identified by internal audit should have a management owner capable of addressing it; otherwise, the independence of internal audit may be compromised.

Practical Internal Audit Program for GenAI Controls

An audit of GenAI should begin with assessing the completeness of the inventory rather than the sophistication of the model. If an organization does not know where GenAI is being used, it becomes difficult to define a reliable risk-based audit scope. The auditor may therefore compare the formal AI inventory with procurement records, business subscriptions, identity and access records, approved extensions, and the software inventory, supplemented by interviews with business units. The objective is not employee surveillance, but rather to assess whether management's inventory is reasonably complete and whether unauthorized use is detected and addressed.

The second step is to select material use cases and reconstruct them from end to end. For each sample, the auditor identifies the business objective, users, data classes, model or vendor, configuration, decision consequences, required human review, validation evidence, and monitoring metrics. Where a generated output influences a high-impact decision, the auditor assesses whether the human reviewer had sufficient information and authority to disagree with the AI. This directly reflects findings relating to automation bias and human-centered AI (7, 20).

The third step is to test operating effectiveness rather than merely the existence of documentation. Validation may be reperformed on a sample of representative cases; data protection may be tested by reviewing permitted categories of inputs and relevant logs; change control may be tested by selecting model or configuration changes and assessing the related risk evaluation and revalidation; and monitoring may be tested by tracing exceptions through to corrective action. Table 4 provides a concise illustrative audit program.

The scope should distinguish between "auditing AI" and "auditing with AI." A large-sample study in external auditing associates audit firms' investments in AI with higher audit quality and efficiency (4), while recent systematic reviews demonstrate the expanding scope and diversity of AI applications in auditing (1). These findings support the use of AI tools in internal audit work, but they do not eliminate the need to assess management's AI controls. If internal audit itself uses GenAI for sample selection, summarizing evidence, or drafting conclusions, such use should also comply with the same principles of data protection, validation, traceability, and human accountability.

Table 4. Illustrative Internal Audit Program for GenAI Controls

Audit objective	Illustrative audit procedure	Expected evidence
Inventory completeness	Reconcile the formal GenAI inventory with procurement records, business subscriptions, SSO/software records, and interviews with business units.	AI/use-case inventory, licenses, software/identity records, interviews.
Risk classification and approval	Sample material use cases and verify the owner, purpose, impact assessment, and approval prior to implementation.	Risk assessment, approval record, process map.
Data protection	Review permitted-data rules, access configurations, and a risk-based sample of relevant logs or inputs.	Data classification, access rights, configuration, logs, exceptions.
Validation	Reperform selected reference cases and compare outcomes with documented acceptance criteria.	Test set, expected results, validation report, reviewer sign-off.
Human oversight	Trace AI-supported high-impact decisions to the reviewer's identity, information available to the reviewer, authority to override, and final rationale.	Decision record, approval, evidence of override/escalation.
Change management	Sample changes to the model, prompt, retrieval process, or workflow and verify impact assessment and revalidation where changes are material.	Change register, approvals, test comparisons, updated risk assessment.
Monitoring and incidents	Trace errors, complaints, or threshold breaches from detection through root-cause analysis and corrective action.	Monitoring metrics, incident records, root-cause analysis, evidence of closure.
Third-party risk	Review vendor due diligence, contractual controls, change notifications, continuity arrangements, and exit/contingency arrangements for material services.	Vendor assessment, contract/SLA, notifications, business continuity plan.
User competencies	Sample training/authorization records and assess users' knowledge of verification requirements, prohibited data, and escalation procedures.	Training evidence, authorization, knowledge assessments/interviews.

Discussion, Applicability and Limitations

The proposed framework has three main advantages. First, it connects AI governance with established internal control concepts rather than creating a parallel bureaucracy. Second, the framework enables independent audit assessment based on verifiable evidence: each risk category is linked to a record or observable condition that an independent internal audit function can test. Third, it is technology-neutral and can be applied to public LLM services, enterprise copilots, retrieval-based assistants, or internal models, with the depth of control adjusted to the potential consequences, data sensitivity, and reversibility of the decision.

The framework also has limitations. It represents a conceptual synthesis of the scientific literature rather than empirical validation across a sample of organizations. The nine categories constitute a practical minimum set rather than an exhaustive taxonomy applicable to every sector. Technical controls may need to be more specific in regulated or safety-critical environments. The effectiveness of human review also depends on the reviewer's

competence: a formal sign-off may create only the appearance of control if the individual lacks domain expertise or is unable to independently assess the output. This is consistent with findings showing that human–AI combinations are not automatically synergistic (21).

An additional limitation concerns the boundary between auditing an organization's own use of AI and relying on vendor controls. Organizations using external models often do not have access to training data, internal parameters, or the vendor's development process. Mökander et al. therefore propose complementary auditing of governance, the model, and the application rather than assuming that the user can independently verify every layer (16). For internal audit, this means that vendor due diligence and contractual evidence are important, but cannot replace testing how the organization's own application is configured, used, and monitored.

Future empirical research should test the framework in organizations with different levels of AI maturity. It would be particularly useful to compare organizations that maintain a formal GenAI inventory and risk classification with those that rely predominantly on user discretion, while measuring incidents, rework, policy exceptions, and audit findings. In Serbia, further research should also examine whether limited specialist capacity affects the optimal allocation of control activities among process owners, centralized AI teams, and internal audit.

CONCLUSION

Generative AI creates value precisely because it is flexible, accessible, and applicable to a wide range of tasks. These same characteristics also make it a distinct internal control challenge. The objective of governance is not to eliminate uncertainty from a probabilistic technology, but to keep that uncertainty within an explicitly accepted risk boundary while preserving human accountability for consequential decisions.

The analysis addresses the four research questions by identifying nine recurring risk categories, translating them into preventive and detective controls, allocating responsibilities, and defining evidence that internal audit can test. Output reliability, data exposure, bias, overreliance, traceability, model changes, third-party dependency, accountability, and effects on work design should be viewed as elements of a single control system. The practical core of the paper is the integrated matrix of risk management, internal controls, and internal audit: every material GenAI use case should have an owner, data rules, a verification method, monitoring, and an escalation process, while internal audit should be capable of independently reconstructing and testing these elements.

Internal audit should not become the owner of AI governance. Its value lies in independently assessing whether management is aware of GenAI applications, understands the associated risks, has established proportionate controls, has retained meaningful human oversight, and responds appropriately to exceptions. The expansion of AI use will require collaboration with technology specialists and experts in data, privacy, and relevant business domains, but accountability remains with the organization and the people who make decisions.

REFERENCES

1. Alkhatib, E., Alkhatib, A., & Jarvis, R. (2026). Auditing using artificial intelligence: A systematic literature review with scientometric and topic modeling insights through a socio-technical systems (STS) perspective. *Journal of Financial Reporting and Accounting*, 1-28. <https://doi.org/10.1108/JFRA-07-2025-0518>
2. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics*, 5, 3265-3279. <https://doi.org/10.1007/s43681-024-00653-w>
3. Brynjolfsson, E., Li, D., & Raymond, L. R. (2025). Generative AI at work. *The Quarterly Journal of Economics*, 140(2), 889-942. <https://doi.org/10.1093/qje/qjae044>
4. Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*, 27, 938-985. <https://doi.org/10.1007/s11142-022-09697-x>
5. Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People-An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28, 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
6. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, 64(12), 86-92. <https://doi.org/10.1145/3458723>
7. Goddard, K., Roudsari, A., & Wyatt, J. C. (2012). Automation bias: A systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*, 19(1), 121-127. <https://doi.org/10.1136/amiajnl-2011-000089>
8. Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577-586. <https://doi.org/10.1016/j.bushor.2018.03.007>
9. Jeremić, N., & Luka, S. (2024). Veštačka inteligencija-izazovi upotrebe u reviziji. *Revizor*, 27(107), 29-55. <https://doi.org/10.56362/Rev24107043J>
10. Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, 14(1), 366-410. <https://doi.org/10.5465/annals.2018.0174>
11. Kokina, J., Blanchette, S., Davenport, T. H., & Pachamanova, D. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. *International Journal of Accounting Information Systems*, 56, Article 100734. <https://doi.org/10.1016/j.accinf.2025.100734>
12. Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115-122. <https://doi.org/10.2308/jeta-51730>
13. Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 220-229. <https://doi.org/10.1145/3287560.3287596>
14. Mitrović, A., Ognjanović, J., & Milašinović, M. (2022). Interna kontrola i računarsko okruženje. *Revizor*, 25(99), 65-80. <https://doi.org/10.56362/Rev2299065M>
15. Mökander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. *Minds and Machines*, 31, 323-327. <https://doi.org/10.1007/s11023-021-09557-8>
16. Mökander, J., Schuett, J., Kirk, H. R., & Floridi, L. (2024). Auditing large language models: A three-layered approach. *AI and Ethics*, 4, 1085-1115. <https://doi.org/10.1007/s43681-023-00289-2>
17. Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics*, 167, 209-234. <https://doi.org/10.1007/s10551-019-04407-1>
18. Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation-augmentation paradox. *Academy of Management Review*, 46(1), 192-210. <https://doi.org/10.5465/amr.2018.0072>

19. Ravid, D. M., White, J. C., Tomczak, D. L., Miles, A. F., & Behrend, T. S. (2023). A meta-analysis of the effects of electronic performance monitoring on work outcomes. *Personnel Psychology*, 76(1), 5-40. <https://doi.org/10.1111/peps.12514>
20. Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human-Computer Interaction*, 36(6), 495-504. <https://doi.org/10.1080/10447318.2020.1741118>
21. Vaccaro, M., Almaatouq, A., & Malone, T. W. (2024). When combinations of humans and AI are useful: A systematic review and meta-analysis. *Nature Human Behaviour*, 8, 2293-2303. <https://doi.org/10.1038/s41562-024-02024-1>
22. Vukmirović, D., & Jovanović-Milenković, M. (2025). Generativna veštačka inteligencija: Principi i primena u savremenom poslovanju. Univerzitet u Beogradu – Fakultet organizacionih nauka.
23. Wassie, F. A., & Lakatos, L. P. (2024). Artificial intelligence and the future of the internal audit function. *Humanities and Social Sciences Communications*, 11, Article 386. <https://doi.org/10.1057/s41599-024-02905-w>

Upravljanje rizicima i interne kontrole pri primeni generativne veštačke inteligencije: Integrirani okvir za organizacije i internu reviziju

Apstrakt: U radu se analizira upravljanje rizicima primene generativne veštačke inteligencije (GenAI) u sistemu internih kontrola i korporativnog upravljanja. Strukturisanim pregledom recenzirane literature razvijen je integrirani okvir upravljanja rizicima, internih kontrola i interne revizije. Devet kategorija rizika povezano je sa preventivnim i kontrolama detekcije, odgovornim funkcijama i postupcima interne revizije. Interna revizija se pozicionira kao nezavisna funkcija koja ocenjuje adekvatnost i efektivnost sistema, dok odgovornost za rizike i kontrole ostaje na rukovodstvu.

Ključne reči: generativna veštačka inteligencija, interne kontrole, upravljanje rizicima, interna revizija, upravljanje veštačkom inteligencijom.