ЭКОНОМИКА
ECONOMY
ЭКОНОМИКА

ISO 31000 IN DIGITAL PUBLIC GOVERNANCE: A SYSTEMATIC REVIEW OF APPLICATIONS AND IMPLEMENTATION PATTERNS

Marzhan SEMBINOVA * *Doctoral student Astana IT University, Astana city, Kazakhstan, marzhansembinova@gmail.com, ORCID ID: https://orcid.org/0009-0005-9966-0723*

Leila SALYKOVA *PhD in economics Astana IT University, Astana city, Kazakhstan, leila.salykova@astanait.edu.kz, ORCID ID: https://orcid.org/ 0000-0003-0766-4363*

Nadeem KHALID *PhD Management, Anglia Ruskin University, United Kingdom, nadeem.khalid.phd@gmail.com, ORCID ID: https://orcid.org/ 0000-0001-9544-3741, Scopus ID: 57190303279*

Дата поступления рукописи в редакцию: 30/09/2025
Доработано: 01/12/2025
Принято: 08/12/2025

DOI: 10.52123/1994-2370-2025-1631
УДК 2964
МРНТИ 11.07.75

Annotation. Digital transformation in public administration has generated complex risks that require systematic approaches. This review analyzes the application of ISO 31000 in digital governance, focusing on e-government and electronic human resource management (E-HRM) systems. Following PRISMA guidelines, 54 studies published between 2009 and 2024 were examined from an initial pool of 228 publications.
Findings indicate that ISO 31000 provides a flexible, principle-based framework for identifying, assessing, and mitigating risks, enhancing service reliability and accountability. However, adoption in the public sector is limited by political turnover and fragmented resources. Complementary frameworks such as ISO 27005 and COBIT strengthen ISO 31000, yet research on emerging technologies (AI, blockchain, predictive HR analytics) remains insufficient.
Keywords: ISO 31000, risk management, digital governance, e-government, systematic literature review

Аңдатпа. Мемлекеттік басқарудағы цифрлық трансформация күрделі тәуекелдердің туындауына себеп болып, оларды жүйелі басқару қажеттігін арттырды. Бұл шолу ISO 31000 қағидаттарының электрондық үкімет пен электрондық адами ресурстарды басқару (E-HRM) жүйелерінде қолданылуын қарастырады. PRISMA әдіснамасына сәйкес 2009–2024 жылдар аралығындағы 228 жарияланымның ішінен 54 зерттеу таңдалып, талдау жүргізілді.
Нәтижелер ISO 31000-ның тәуекелдерді айқындауға, бағалауға және азайтуға мүмкіндік беретін бейімделгіш құрылым екенін көрсетті. Ол мемлекеттік қызметтердің сенімділігі мен есеп берушілігін арттыра алады. Алайда саяси тұрақсыздық пен ресурстардың жеткіліксіздігі енгізу тиімділігін шектейді. ISO 27005 пен COBIT сияқты қосымша стандарттар тиімділікті күшейте алады, бірақ жаңа технологияларға қатысты (жасанды интеллект, блокчейн, болжамалы HR-талдау) деректер жеткіліксіз.
Түйінді сөздер: ISO 31000, тәуекелдерді басқару, цифрлық басқару, электрондық үкімет, жүйелі әдеби шолу

Аннотация. Цифровая трансформация в государственном управлении сопровождается появлением новых рисков, требующих системных методов управления. В обзоре анализируется применение ISO 31000 в цифровом государственном управлении, в том числе в электронном правительстве и системах управления персоналом (E-HRM). В соответствии с PRISMA было рассмотрено 54 исследования, отобранные из 228 публикаций за 2009–2024 гг.
Результаты показывают, что ISO 31000 является гибкой структурой для идентификации, оценки и снижения рисков, повышающей надёжность услуг и подотчётность организаций. Однако внедрение ограничивается политической сменяемостью и фрагментированным распределением ресурсов. Дополнительные стандарты, такие как ISO 27005 и COBIT, усиливают эффективность применения, но исследований по новым технологиям (ИИ, блокчейн, предиктивная HR-аналитика) недостаточно.

* *Corresponding author: M. Sembinova, marzhansembinova@gmail.com*

Ключевые слова: ISO 31000, управление рисками, цифровое управление, электронное правительство, систематический обзор литературы

Introduction

Digital transformation of public administration has fundamentally reshaped service delivery models, creating new opportunities for citizen engagement, operational efficiency, and transparent governance. Modern e-government platforms, electronic human resource management (e-HRM) systems, and digital identity services have transformed how public organizations interact with citizens and manage internal operations. At the same time, this transformation has introduced complex risk landscapes, including cybersecurity threats, data privacy breaches, system reliability failures, and governance accountability challenges. As public organizations increasingly depend on digital platforms for critical services, from healthcare delivery to tax administration, the potential impact of system failures extends far beyond technical disruptions, affecting public trust, service continuity, and democratic processes (Weerakkody et.al., 2015; Xie et.al., 2022). The growing complexity of global risk environments has highlighted the limitations of traditional, fragmented approaches to risk management. Interconnected risks, spanning technological, environmental, social, and institutional dimensions, require comprehensive frameworks capable of addressing both immediate operational threats and long-term strategic implications. In this context, ISO 31000:2018 Risk Management Guidelines have emerged as one of the leading frameworks for systematic risk governance. The standard provides a principle-based, adaptable approach designed to help organizations identify, analyze, evaluate, and treat risks while embedding risk awareness into decision-making and organizational culture. Its versatility has made it increasingly relevant in the public sector, where digital transformation requires balancing innovation with accountability and resilience.

This systematic review addresses these gaps by synthesizing available evidence on ISO 31000 applications in digital governance, with a particular focus on E-HRM systems. The review aims to:

(a) assess how the framework has been operationalized in digital public administration;

(b) identify institutional barriers and contextual enablers of its adoption;

(c) propose research directions for strengthening its application in the context of ongoing digital transformation.

Literature Review

2.1 Early Foundations and Framework Development

The evolution of ISO 31000 can be traced to broader developments in risk governance and management standards at the beginning of the 21st century. The publication of ISO 31000:2009 responded to increasing recognition that risks in organizations are interconnected, cutting across sectors and functions. Scholars emphasize that ISO 31000 differs from prescriptive frameworks such as COSO by focusing on principles and guidelines that can be flexibly adapted to various contexts (Ernawati et.al., 2012; Olechowsk et.al., 2016; Barafort et.al., 2018). The 2018 revision reinforced its emphasis on integration into decision-making and culture, clarifying definitions and stressing leadership and stakeholder engagement as core principles. This shift has been interpreted as recognition that risks in digital governance cannot be addressed solely by technical tools but require cultural and organizational alignment (Olechowsk et.al., 2016; Nurdin, 2024).

2.2 Framework Integration and Comparative Analysis

ISO 31000 is not a stand-alone instrument; it has been increasingly combined with complementary standards. For instance, integration with ISO 27001/27005 has been widely applied in contexts of information security and cybersecurity (Akinrolabu et.al., 2019; Putra et.al., 2023). The standard's flexibility allows it to be applied even to organizational IT infrastructure risks, as demonstrated by Elly et al. (2022), underscoring ISO 31000's broad applicability beyond core government services. Barafort et al., demonstrated the adaptability of ISO 31000 in multi-standard environments where quality, continuity, and security certifications coexist. Comparative analyses also highlight contrasts: while COSO-ERM is stronger on financial controls, ISO 31000 provides broader applicability across strategic, operational, and compliance risks (Nurdin, 2024). These findings suggest that in digital public governance, ISO 31000 is most effective when aligned with

sector-specific regulations and accountability frameworks, such as data protection laws (GDPR) or government audit standards (Sinulingga et.al., 2024). This formal integration of ISO 31000 into public policy is evident in Brazil, where international risk management standards have been incorporated into federal regulations, exemplifying how regulatory pressures can drive adoption (Souza et.al., 2023).

2.3 Applications in Digital Governance

A growing body of empirical studies (Twizeyimana & Andersson, 2019; Nugraha, 2019; Arif et.al., 2024) documents how ISO 31000 has been adopted in digital transformation initiatives. In e-government, adoption has supported structured approaches to risk assessment, particularly in procurement, service continuity, and IT modernization projects. Researchers in Brazil and Indonesia (Twizeyimana & Andersson, 2019; Alves et.al., 2020; Arif et.al., 2024) provide extensive case studies illustrating how ISO 31000 shaped the design of monitoring systems, guided prioritization of risks, and informed governance structures. One such study applied ISO 31000 to a local government information system (SIOLGA), where Mamuaja and Cahyono (2024) detail how the framework was used to systematically identify and mitigate IT risks in an e-government platform. Reported barriers, however, are recurrent: frequent political turnover undermines continuity, fragmented budgeting prevents systematic risk treatment, and absence of performance indicators limits accountability (Twizeyimana and Andersson, 2019; Lubis, 2023). At the same time, innovative tools such as the Enterprise Risk Management Agile Canvas (Alves et.al., 2020) have been introduced to foster stakeholder dialogue and enhance risk visualization in the public sector. For instance, Anindya (2023) presents a case study of a regional public hospital that implemented an ISO 31000-based risk management design, demonstrating the framework's adaptability in improving operational resilience.

2.4 E-HRM as an Emerging Domain

Electronic Human Resource Management (E-HRM) represents one of the less explored but critical areas for ISO 31000 application. Risks in this domain include data protection breaches, system usability issues, change management failures, and compliance with evolving regulations. Studies (Kempeneer and Heylen, 2023; Sattlegger and Bharosa, 2024) show that ISO 31000 has been applied to design HR risk registers, structure monitoring processes, and inform training of HR staff. Integration with ISO 27005 has proven valuable for addressing cybersecurity risks in employee data management (Akinrolabu et.al., 2019; Nugraha, 2019). Yet, existing evidence remains fragmented, often descriptive, and limited to individual case studies. There is still insufficient knowledge on how ISO 31000 can be institutionalized across public HR systems, particularly in transitional economies.

2.5 Emerging Technology Challenges

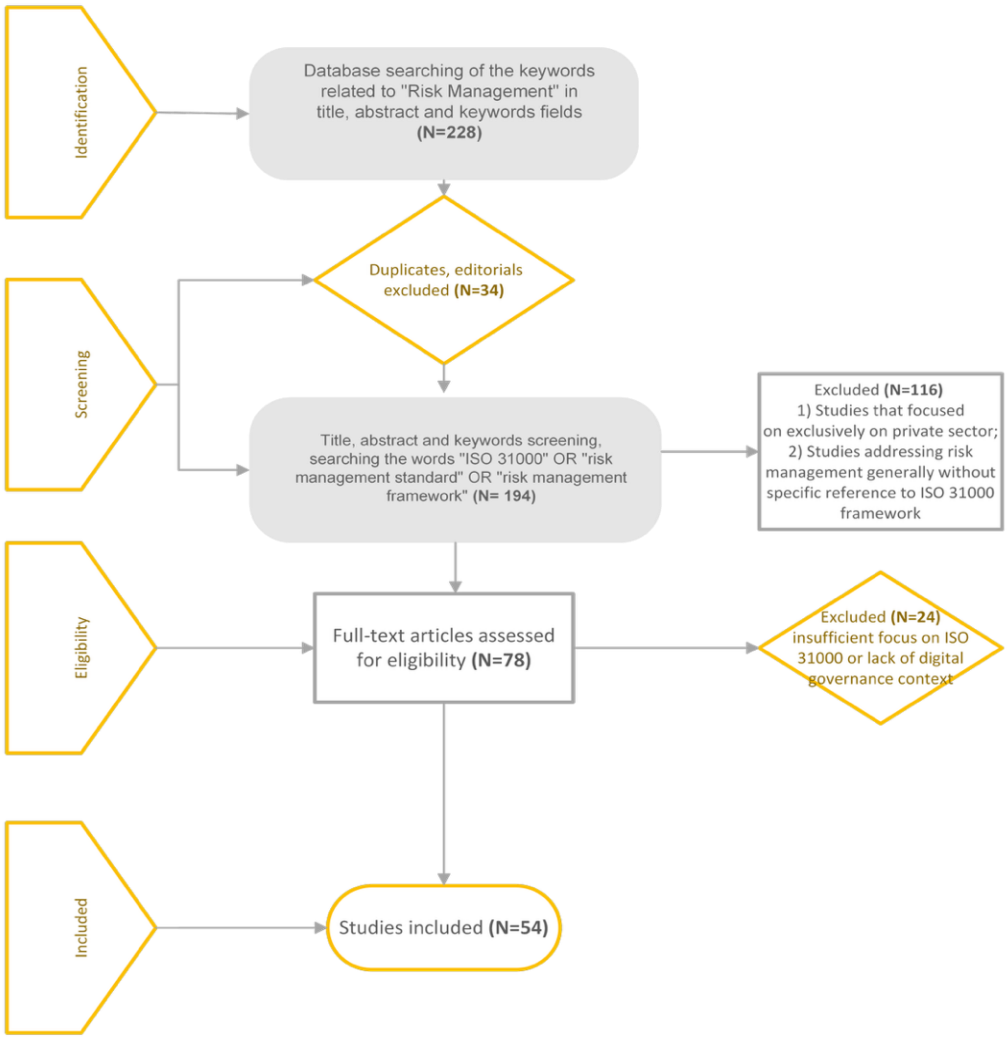
The acceleration of AI, blockchain, and IoT in the public sector raises novel risks that cut across technical, ethical, and societal dimensions. Scholars argue (Park, 2018; Akinrolabu et.al., 2019; Putra and Soewito, 2023) that while ISO 31000 offers a broad principle-based approach, its operationalization in these domains remains under-theorized. For example, ethical risks in AI adoption - bias, opacity, accountability gaps - require embedding risk considerations into design and oversight, going beyond compliance (Putra and Soewito, 2023). Smart city literature (Park, 2018; Morozova and Yatsechko, 2022) similarly highlights interconnected risks such as privacy, interoperability, and sustainability. These works indicate that while ISO 31000 provides a starting framework, it needs complementary guidance and sector-specific adaptation to remain relevant for emerging digital ecosystems.

Moreover, Taherdoost (2022) provides a comprehensive review of cybersecurity frameworks and standards, positioning ISO 31000 as a high-level risk governance guideline that complements more specialized information security frameworks.

Methodology

This systematic literature review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines to ensure transparency and comprehensiveness (Page et.al., 2020). The review was designed to identify, analyze, and synthesize peer-reviewed research on ISO 31000 applications in digital governance.

Fig.1. PRISMA Flow diagram



Source: Created by authors (based on review data)

3.1 Search Strategy

A comprehensive search was conducted in January 2025 across Scopus, Web of Science, IEEE Xplore, and Google Scholar. The timeframe covered publications from January 2009 (the year of ISO 31000's first edition) to January 2025. Search strings combined three main concept groups using Boolean operators:

– Risk management terms: "ISO 31000" OR "risk management framework" OR "enterprise risk management" OR "risk assessment" OR "risk governance";

– Digital governance terms: "digital governance" OR "e-government" OR "digital transformation" OR "e-HRM" OR "electronic human resource management" OR "digital public services" OR "smart cities" OR "digital administration";

– Technology terms: "information technology" OR "cybersecurity" OR "data security" OR "digital platform" OR "artificial intelligence" OR "blockchain" OR "IoT" OR "Internet of Things".

3.2 Inclusion and Exclusion Criteria

Inclusion Criteria: (1) peer-reviewed journal articles, conference proceedings, and book chapters; (2) publications in English language; (3) studies focusing on ISO 31000 applications in public sector or digital governance contexts; (4) research examining risk management in e-government, e-HRM, or related digital public services; (5) publications from 2009-2025.

Exclusion Criteria: (1) non-peer-reviewed publications (reports, white papers, dissertations); (2) studies focusing solely on private sector applications without public sector relevance; (3) publications not directly addressing ISO 31000 or systematic risk management approaches; (4) duplicate publications or conference papers subsequently published as journal articles.

3.3 Selection Process

The initial search yielded 228 records. After removing duplicates (n = 34), 194 articles underwent title and abstract screening by two independent reviewers. Agreement was measured with Cohen's kappa (κ = 0.82), indicating substantial consistency. Discrepancies were resolved through discussion with a third reviewer. From this stage, 78 articles proceeded to full-text assessment. Following exclusions (n = 24) for insufficient relevance, the final dataset comprised 54 studies. A PRISMA flow diagram (Figure 1) illustrates the process.

3.4 Quality Assessment

Study quality was assessed using an adapted Critical Appraisal Skills Programme (CASP) checklist suitable for case studies, empirical surveys, and conceptual frameworks. Assessment criteria included: clarity of methodology, appropriateness of research design, rigor of data collection, transparency of analysis, and validity of conclusions.

Of the 54 included studies, 22 were rated high quality, 25 moderate, and 7 low. All studies were retained to ensure comprehensiveness; however, findings from high- and moderate-quality studies were given greater interpretive weight in the synthesis, while insights from low-quality studies were treated cautiously and used primarily for contextual illustration.

3.5 Data Extraction and Analysis

For each study we extracted: application domain, methods, key findings, reported outcomes, challenges, and recommendations. We used inductive thematic coding aligned deductively with our research questions to surface common implementation patterns and context-specific differences.

Following PRISMA guidelines, 54 studies were included in the synthesis. The reference list, however, is shorter, as it reports only those sources explicitly cited in the text. Additional studies contributed to the coding and contextual analysis but are not listed individually.

4. Results

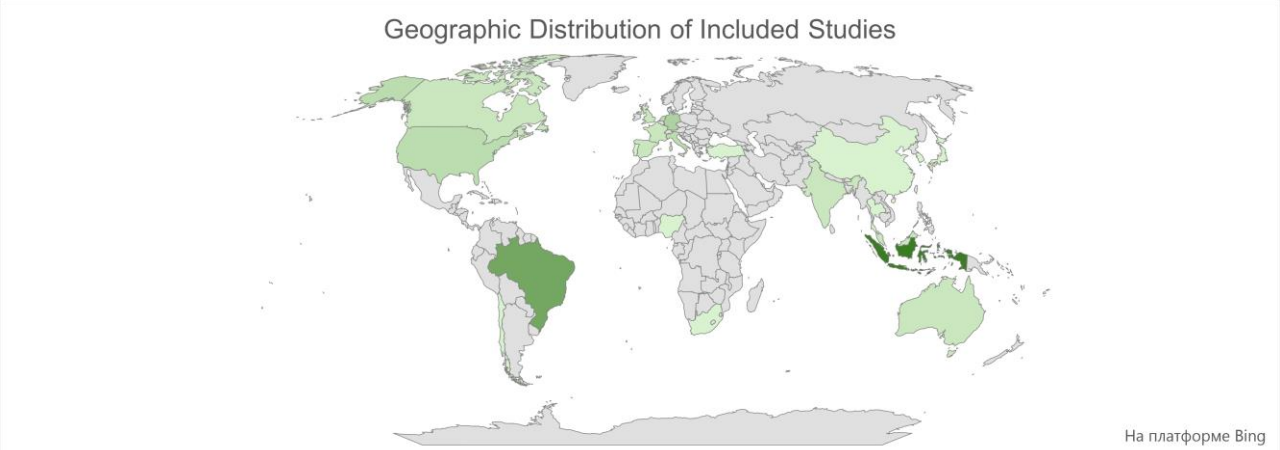
4.1 Study Characteristics

The final dataset comprised 54 studies published between 2009 and 2024, with notable growth after the ISO 31000:2018 revision. Geographic distribution was diverse, covering 23 countries, with concentrations in Indonesia (n = 12), Brazil (n = 8), and the European Union (n = 15).

Indonesian studies (Oliveira et.al., 2017; Nugraha, 2019; Alves et.al., 2020; Rahman et.al., 2024) provided extensive evidence of ISO 31000 adoption at local government and agency levels, illustrating how the framework was applied to strengthen accountability and compliance in public administration. Brazilian research (Donaldson, 2001; Alves et.al., 2020; Xie et.al., 2022), in turn, emphasized IT- and cybersecurity-oriented applications, frequently linking ISO 31000 with COBIT or ISO 27005 to reinforce digital infrastructure governance These regional patterns suggest that local institutional capacity and policy drivers shaped the form of implementation.

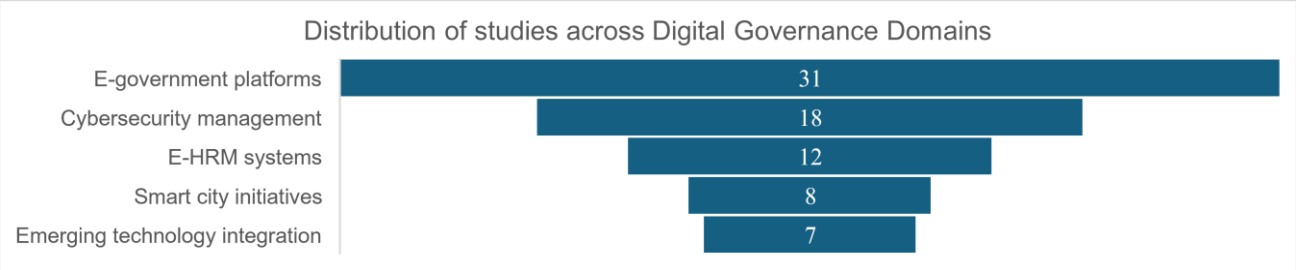
Overall, 34 studies focused exclusively on public-sector contexts, while 20 examined mixed public–private settings.

Fig.2. Spatial Distribution of the 54 Included Studies Across 23 Countries



Source: Created by authors (based on review data)

Fig.3. Digital Governance Domains



Source: Created by authors (based on review data)

4.2 Key Findings by Theme

Table 1. Thematic Analysis of ISO 31000 Implementation in Digital Governance

Theme	Key Insights	Main Challenges
Versatility and Adaptation	Flexible, principle-driven; adaptable to diverse contexts; well-suited for e-government.	Balancing stakeholders and regulatory requirements
Public Sector Implementation	Approaches: phased deployment (67%, 36/54); pilot testing (45%, 24/54); integration with governance frameworks (78%, 42/54). Success factors: training (89%, 48/54); governance structures (82%, 44/54); senior leadership support (95%, 51/54).	Political volatility, budget fragmentation, unclear performance indicators
Technology Integration	Complements cybersecurity standards; supports IT and digital risk management.	Aligning vocabularies, multi-stakeholder coordination, evolving threats
Effectiveness and Outcomes	Reported benefits: risk awareness (85%, 46/54); decision-making (72%, 39/54); stakeholder communication (68%, 37/54); reduced incidents (43%, 23/54). Cost–benefit analyses (11%, 6/54).	Limited quantitative evidence, reliance on self-reports
Implementation Challenges	Persistent barriers: resources (78%, 42/54); cultural resistance (65%, 35/54); IT integration (58%, 31/54); data quality (52%, 28/54); risk quantification (47%, 25/54); unclear roles (43%, 23/54); limited leadership support (38%, 20/54); competing priorities (62%, 33/54).	Persistent barriers to adoption and maturity

Source: Created by authors (based on review data)

The majority of studies highlighted ISO 31000's adaptability, especially in e-government platforms, where its principles aligned with stakeholder communication and accountability needs.

Public-sector adoption often followed a phased or pilot-based approach, with success depending heavily on leadership support and staff training.

Effectiveness evidence remains limited: while many studies reported improved awareness and communication, only a handful (6/54) provided cost–benefit analysis.

Implementation barriers were consistent across contexts: resource constraints, fragmented governance, and resistance to cultural change.

4.3 Sector-Specific Findings

Table 2. Sector-Specific Applications of ISO 31000 in Digital Governance

Domain	Key Success Factors	Main Challenges
E-Government (31 studies)	Transparency, accountability, citizen engagement	Managing expectations, inter-agency coordination, privacy protection
E-HRM (12 studies)	Compliance, data protection, system reliability	HR engagement, policy clarity, integration with legacy processes
Smart City (8 studies)	Structured ISO 31000 adaptation, cross-sector coordination	Data governance, privacy concerns, interdepartmental fragmentation

Source: Created by authors (based on review data)

Applications in e-government were the most common (n = 31). These studies (Twizeyimana and Andersson, 2019; Nugraha, 2019; Alves et.al., 2020; Sinulingga et.al., 2024) demonstrated how ISO 31000 principles were applied to enhance transparency, accountability, and risk communication across government agencies, although challenges such as inter-agency coordination and data privacy remained persistent.

Research on E-HRM (n = 12) focused mainly on compliance and data protection, with several works describing ISO 31000's role in structuring HR-related risk registers and integrating monitoring mechanisms into broader organizational reforms (Kempeneer and Heylen, 2023; Sattlegger and Bharosa, 2024).

Finally, smart city initiatives (n = 8) illustrated the complexity of cross-sectoral risk governance. Studies highlighted IT-governance integration, with ISO 31000 serving as a bridge between municipal administration and private technology providers (Park, 2018; Morozova and Yatsechko, 2022)

Discussion

The systematic synthesis of 54 studies demonstrates that ISO 31000 operates as a flexible governance instrument in digital public-sector contexts, including electronic human resource management (E-HRM). The evidence from the results section indicates that adoption is concentrated geographically (Indonesia, Brazil, selected EU countries) and topically (e-government, E-HRM, smart cities, cybersecurity). This discussion interprets the results in light of broader theoretical and practical debates.

First, the distribution of ISO 31000 adoption across diverse public-sector contexts underscores the explanatory value of institutional theory: adoption appears shaped not only by technical rationales but also by legitimacy and normative pressures. In Indonesia and Brazil, (Twizeyimana and Andersson, 2019; Alves et.al., 2020; Arif et.al., 2024) for example, ISO 31000 uptake was often linked to regulatory requirements or alignment with international donor expectations.

Second, the recurring preference for phased rollouts and pilot testing strengthens socio-technical systems perspectives. E-HRM systems are not merely IT installations but socio-technical interventions reshaping organizational routines, roles, and practices. High emphasis on staff training (89%) and governance structures (82%) suggests that practitioners treat social and technical elements as co-constitutive (Moynihan, 2008). ISO 31000's emphasis on context and stakeholder engagement aligns with socio-technical design principles.

Third, variation in implementation success reflects contingency theory: effectiveness depends on political stability, administrative capacity, and inter-organisational coordination. In E-HRM, success was most likely when risk management was integrated with broader HR reforms and adequately resourced. This supports the contingency perspective that organizational outcomes are shaped by contextual moderators (Barraza et.al., 2023).

Fourth, the lack of measurable outcomes highlights a gap in performance management theory. Only 28% of studies reported quantifiable improvements. Most focused on process indicators (training, registers, awareness), while evidence on outcomes (reduced breaches, improved trust) remains scarce. Linking ISO 31000 to performance management frameworks could clarify causal mechanisms (Rumba et.al., 2022).

Taken together, these findings suggest that ISO 31000 in E-HRM is best conceptualised as an interaction of institutional drivers, socio-technical alignment, contextual contingencies, and measurable performance outcomes. This interpretation also aligns with socio-technical systems theory, which cautions that many failures in digital projects stem not only from technical or procedural gaps but from limited integration of social and technical dimensions. Embedding ISO 31000 principles into a socio-technical perspective encourages joint optimization of efficiency and quality of working life, ensuring that risk controls support autonomy, learning, and sustainable behavioral change (Bostrom & Heinen, 1977).The findings of this review suggest that public-sector organizations are more likely to succeed with ISO 31000 when adoption is phased, anchored in senior leadership commitment, supported by comprehensive staff training, and embedded within clear governance structures. Evidence from e-government and E-HRM cases shows that pilot implementations help tailor risk processes to organizational realities and reduce disruption before

scaling. Such staged approaches proved particularly salient where cross-departmental coordination and role clarity were prerequisites for consistent risk practices (Oliveira et.al., 2017; Arif et.al., 2024).

Effectiveness is further enhanced when ISO 31000 is integrated with complementary standards and managerial frameworks rather than deployed as a stand-alone instrument. Aligning organizational risk assessment with information-security guidance strengthened controls over sensitive data, especially in HR contexts, by coupling ISO 31000 with ISO 27005 and related methods for threat identification and treatment (Akinrolabu et.al., 2019; Kempeneer and Heylen, 2023). Where IT governance considerations were prominent, combinations with COBIT clarified responsibilities, interfaces, and control ownership across business and technology functions (Arif et.al., 2024; Sattlegger and Bharosa, 2024).

Technical capacity remains a decisive condition for credible implementation. Studies underscore the need for cybersecurity, interoperability, and data-privacy expertise within public agencies, and point to partnerships with universities and private providers as a pragmatic way to access advanced competencies, including analytics for HR and other mission-critical domains (Xie et.al., 2022; Sattlegger and Bharosa, 2024). At the same time, the literature cautions that reported benefits are still rarely quantified and that stronger evaluation designs are required to demonstrate value beyond process compliance (Donaldson, 2001).Contextual constraints continue to shape outcomes. Political volatility, fragmented budgets, and multi-stakeholder complexity frequently limited continuity and depth of adoption; visual and participatory instruments such as the ERM Agile Canvas helped sustain cross-agency dialogue about risks and treatments under such conditions (Lubis, 2023). Consistent with socio-technical insights, effective ISO 31000 implementation also requires participatory design, timely feedback loops, and behavioral incentives that enhance both efficiency and quality of working life, reducing resistance and fostering shared ownership of risk practices (Bostrom & Heinen, 1977).Comparative insights indicate that ISO 31000 travels best when adapted to prevailing governance traditions: for example, balancing central steering with departmental autonomy in mature public administrations improved alignment between enterprise-level risk policies and operational practices (Xie et.al., 2022).

Taken together, these implications argue for viewing ISO 31000 not merely as a technical framework but as a strategic, context-sensitive scaffolding that gains effectiveness through phased adoption, integration with security and IT-governance standards, purposeful capability building, and systematic evaluation.

Research Limitations

Despite the breadth of this review, several limitations constrain the conclusions that can be drawn. These limitations are methodological, contextual, and conceptual.

Methodologically, the majority of the included studies relied on qualitative designs such as case studies or descriptive analyses, which provide valuable insights but offer limited opportunities for quantitative validation (Oliveira et.al., 2017; Alves et.al., 2020; Kempeneer and Heylen, 2023; Arif et.al., 2024; Sattlegger & Bharosa, 2024). This reliance on self-reported evidence constrains the generalizability of results and leaves important outcome dimensions underexplored.The evidence base is also geographically imbalanced, with the bulk of studies originating from Indonesia, Brazil, and selected European Union countries (Donaldson, 2001; Twizeyimana & Andersson, 2019; Nugraha, 2019), while other regions such as Central Asia or Sub-Saharan Africa remain largely absent from the literature.In topical terms, only a small subset of studies (n = 12) directly examined E-HRM systems, reducing the ability to draw broader conclusions about risk governance in this critical domain (Kempeneer & Heylen, 2023; Sattlegger & Bharosa, 2024).Conceptually, many studies treated ISO 31000 as a prescriptive checklist or compliance tool rather than unpacking the mechanisms through which it influences organizational behavior and governance outcomes (Twizeyimana and Andersson, 2019; Kempeneer & Heylen, 2023; Sattlegger & Bharosa, 2024).

Together, these limitations suggest that current knowledge about ISO 31000 in digital governance, particularly in E-HRM contexts, remains partial and requires cautious interpretation.

Future Research Directions

Addressing these limitations will require a more diverse and rigorous research agenda. Longitudinal studies tracking the adoption of ISO 31000 across different phases of E-HRM implementation would provide clearer evidence of its sustained impact on risk mitigation and organizational resilience (Kempeneer & Heylen, 2023; Sattlegger & Bharosa, 2024). Comparative

research between adopters and non-adopters, ideally using quantitative indicators such as data breach rates, employee trust, or service continuity metrics, could enhance the evidence base on tangible outcomes (Akinrolabu et.al., 2019).Future studies should also engage more systematically with emerging technologies, particularly artificial intelligence, blockchain, and predictive HR analytics, to assess whether ISO 31000 remains adequate for governing these novel risks (Park, 2018; Akinrolabu et.al., 2019; Putra & Soewito, 2023). Expanding the geographical scope of research to underrepresented regions, including Central Asia and Africa, would also improve the generalizability of findings and highlight context-specific adaptations.

Finally, theoretical work is needed to integrate ISO 31000 with complementary frameworks such as COBIT, ISO 27005, and GDPR, and to examine how these combinations can strengthen digital risk governance in both e-government and E-HRM settings (Alves et.al., 2020; Lubis, 2023; Arif et.al., 2024). Advancing along these lines would significantly enhance understanding of ISO 31000's role as both a practical tool and a theoretical construct in the evolving field of digital public governance.

Conclusion

This systematic review compiled 54 studies regarding the implementation of ISO 31000 in digital public governance, emphasizing electronic human resource management (E-HRM).

According to the study's results, ISO 31000 serves as a complex, principle-oriented structure that improves accountability, communication, and resilience in online settings, despite the minimal quantitative evidence about its influence. Continual obstacles – political fluctuations, dispersed resources, and inadequate performance metrics – remain a significant impediment to the methodical implementation. Integration with complementary frameworks such as ISO 27005, COBIT, and GDPR strengthens its relevance, suggesting that ISO 31000 serves most effectively as an integrating backbone rather than as an isolated tool.

In order to augment its functional applicability within the domain of human resource management, entities should incorporate the tenets of ISO 31000 into their human resource policies and procedures, maintain risk registers that are specifically oriented towards human resources, develop the competencies of personnel for making decisions that are informed by risk considerations, and engage in collaborative efforts with information technology, legal, and audit divisions. Regular audits and pilot implementations can further entrench a risk culture and boost adaptability. Initiatives like these would promote the advancement of Human Resources divisions from a reactive, compliance-driven oversight style to a proactive, analytics-based governance arrangement.

In conclusion, ISO 31000 remains a vital yet frequently underutilised framework within digital public governance. The extensive implementation of this concept will be contingent upon contextual adaptation, the integration with alternative frameworks, and the development of quantifiable metrics for evaluating the maturity of risk governance across human resources and various administrative sectors.

References

Anindya, S. R. (2023). Potential risk management design based on ISO 31000:2018: A case study of RSUD BLUD X. InCAF, 1(1). https://doi.org/10.20885/InCAF.vol1.art1

Akinrolabu, O., Nurse, J. R. C., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. Computers & Security, 87, 101600. https://doi.org/10.1016/j.cose.2019.101600

Alves, G. F., Martins, M. A. F., Brito, R. L., & Santos, W. O. (2020). Enterprise Risk Management Agile Canvas: A framework for risk management on public administration. Revista do Serviço Público, 71(4), 245–268. https://doi.org/10.21874/RSP.V71IC.4363

Arif, G. S., Erliani, Y., & Ratnasari, A. (2024). Analysis of risk management using E-Office application with ISO 31000:2018 in National Public Procurement Agency (NPPA/LKPP). Airlangga Journal of Innovation Management, 5(2), 260–277. https://doi.org/10.20473/ajim.v5i2.56656

Barafort, B., Mesquida, A.-L., & Mas, A. (2018). Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. Computer Standards & Interfaces, 60, 57–66. https://doi.org/10.1016/j.csi.2018.04.010

Barraza, J., Rodríguez-Picón, L., Morales-Rocha, V., & Torres, V. (2023). A systematic review of risk management methodologies for complex organizations in Industry 4.0 and 5.0. Systems, 11(5), 218. https://doi.org/10.3390/systems11050218

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. MIS Quarterly, 1(3), 17–32. https://doi.org/10.2307/248710

Donaldson, L. (2001). The contingency theory of organizations. Sage Publications. https://doi.org/10.4135/9781452229249

Elly, R., Chen, K., Hanes, D., & Joosten, S. (2022). ISO 31000:2018-based IT infrastructure risk management study (case study: Universitas Mikroskil). Jurnal Riset Informatika, 5(1), 469–480. https://doi.org/10.34288/jri.v5i1.448

Ernawati, T., Suhardi, & Nugroho, D. R. (2012). IT risk management framework based on ISO 31000:2009. In Proceedings of the International Conference on System Engineering and Technology (pp. 233–238). IEEE. https://doi.org/10.1109/ICSENGT.2012.6339352

Kempeneer, S., & Heylen, F. (2023). Virtual state, where are you? A literature review, framework and agenda for failed digital transformation. Big Data & Society. https://doi.org/10.1177/20539517231160528

Lubis, F. S. (2023). IT risk analysis based on risk management using ISO 31000: Case study registration application at University XYZ. In Proceedings of the International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS'23). ACM. https://doi.org/10.1145/3629378.3629464

Mamuaja, H. B., & Cahyono, A. (2024). SIOLGA information technology risk management analysis using ISO 31000. Journal of Information Systems and Informatics, 6(1), 57–67. https://doi.org/10.51519/journalisi.v6i1.641

Morozova, I. A., & Yatsechko, S. S. (2022). The risks of smart cities and the perspectives of their management based on corporate social responsibility in the interests of sustainable development. Risks, 10(2), 34. https://doi.org/10.3390/risks10020034

Moynihan, D. P. (2008). The dynamics of performance management: Constructing information and reform. Georgetown University Press.

Nugraha, U. (2019). Implementation of ISO 31000 for information technology risk management in the government environment. International Journal of Advanced Science and Technology, 28(19).

Nurdin, I. (2024). Development of an integrated IT risk management framework for electronic-based government systems: A case study of the XYZ ministry. Indonesian Interdisciplinary Journal of Sharia Economics, 7(1), 1331–1353. https://doi.org/10.31538/iijse.v7i1.4322

Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? International Journal of Project Management, 34(8), 1568–1578. https://doi.org/10.1016/j.ijproman.2016.08.002

Oliveira, U. R. de, Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. Journal of Cleaner Production, 151, 616–633. https://doi.org/10.1016/j.jclepro.2017.03.054

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Park, K. J. (2018). A risk management model for sustainable smart city. International Journal of Advanced Science and Technology, 110, 23–32. https://doi.org/10.14257/ijast.2018.110.03

Putra, A. P., & Soewito, B. (2023). Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/IJACSA.2023.0140468

Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). Assess ITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and cybersecurity risk assessment. arXiv. https://doi.org/10.48550/arXiv.2410.01750

Rumba, M. F., Mirsel, R., & Sabu, F. X. (2022). Risk management information technology based on ISO 31000:2018 at Institute of Philosophy and Creative Technology, Ledalero. American Journal of Computer Science and Technology, 5(3), 170–177. https://doi.org/10.11648/j.ajcst.20220503.13

Sattlegger, A., & Bharosa, N. (2024). Beyond principles: Embedding ethical AI risks in public sector risk management practice. In Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT) (pp. 657–663). https://doi.org/10.1145/3657054.3657063

Sinulingga, R., Raharjo, T., & Trisnawaty, N. W. (2024). Risk management design and analysis on agile development project using ISO 31000 integrated with ISO 27005: A case study of SiREV application. Jurnal Informatika Ekonomi Bisnis, 6(4), 815–821. https://doi.org/10.37034/infeb.v6i4.1053

Souza, F. S. R. N., Braga, M. V. A., & Cunha, A. S. M. (2023). Incorporation of international risk management standards into federal regulations. Revista de Administração Pública, 57(3), 245–262. https://doi.org/10.1590/0034-761220180117x

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview. Electronics, 11(14), 2181. https://doi.org/10.3390/electronics11142181

Twizeyimana, J. D., & Andersson, A. (2019). The public value of e-government: A literature review. Government Information Quarterly, 36(2). https://doi.org/10.1016/j.giq.2019.01.001

Weerakkody, V., Irani, Z., Lee, H., Osman, I. H., & Hindi, N. (2015). E-government deployment: A bird's eye view of issues relating to costs, opportunities, benefits and risks. Information Systems Frontiers, 17(4), 889–915. https://doi.org/10.1007/s10796-013-9472-3

Xie, Z. (2022). ICT governance and management macroprocesses of a Brazilian federal government agency. Information, 13(5), 231. https://doi.org/10.3390/info13050231

ISO 31000 ЦИФРЛЫҚ МЕМЛЕКЕТТІК БАСҚАРУДА: ҚОЛДАНУ ТӘЖІРИБЕЛЕРІ МЕН ІСКЕ АСЫРУ ҮЛГІЛЕРІНІҢ ЖҮЙЕЛІ ТАЛДАУЫ

Маржан СЕМБИНОВА*, докторант, Astana IT University, Астана, Қазақстан, marzhansembinova@gmail.com, ORCID ID: 0009-0005-9966-0723*

***Лейла САЛЫКОВА**, экономика ғылымдарының кандидаты, PhD докторы, Astana IT University, Астана, Қазақстан,leila.salykova@astanait.edu.kz, ORCID ID: 0000-0003-0766-4363*

***Надим КХАЛИД,** менеджмент саласында PhD докторы, Anglia Ruskin University, Ұлыбритания, nadeem.khalid.phd@gmail.com , ORCID ID: 0000-0001-9544-3741 Scopus ID: 57190303279*

ISO 31000 В ЦИФРОВОМ ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: СИСТЕМАТИЧЕСКИЙ АНАЛИЗ ПРАКТИК ПРИМЕНЕНИЯ И МОДЕЛЕЙ РЕАЛИЗАЦИИ

Маржан СЕМБИНОВА*, Докторант Astana IT University, Астана, Казахстан, marzhansembinova@gmail.com, ORCID ID: 0009-0005-9966-0723*

***Лейла САЛЫКОВА**, Кандидат экономических наук, доктор PhD, Astana IT University Астана, Казахстан,leila.salykova@astanait.edu.kz, ORCID ID 0000-0003-0766-4363*

***Надим КХАЛИД**, доктор PhD в области менеджмента, Anglia Ruskin University, Великобритания, nadeem.khalid.phd@gmail.com, ORCID ID 0000-0001-9544-374, Scopus ID: 57190303279*