Journal of Accounting Innovation
Homepage : https://ijai.antispublisher.or.id/index.php/IJAI
Email : admin@antispublisher.com

e-ISSN : 3089-5383
IJAI, Vol. 3, No. 1, October 2025
Page 241-254

Integrating Accounting Information Systems and Enterprise Risk Management for Real-Time Financial Risk Monitoring

Munkashir Hossen
Bangladesh Open University, Bangladesh

DOI : https://doi.org/10.61796/ijai.v1i3.28

Sections Info

Article history:
Submitted: September 05, 2025
Final Revised: October 13, 2025
Accepted: November 08, 2025
Published: December 20, 2025

Keywords:
Accounting Information Systems
Enterprise Risk Management
Financial Risk Monitoring
Real-Time Reporting
Organizational Resilience

ABSTRACT

Objective: *This study aims to examine the strategic integration of Accounting Information Systems (AIS) and Enterprise Risk Management (ERM) as a mechanism for strengthening real-time financial risk monitoring and improving organizational decision-making in dynamic financial environments.* ***Method:*** *The study adopts a conceptual and analytical review approach by synthesizing relevant literature on AIS functionality, ERM frameworks, cybersecurity risks, and digital risk governance. Key themes related to system integration challenges, risk control mechanisms, and governance practices are systematically analyzed to develop an integrated perspective.* ***Results:*** *The findings indicate that AIS–ERM integration enables organizations to shift from reactive financial management toward proactive and predictive risk identification through accurate data processing, real-time monitoring, and advanced analytics. However, implementation challenges persist, including legacy system incompatibility, cybersecurity threats, human error, and organizational resistance. The adoption of best practices – such as encryption, access control, continuous monitoring, incident response planning, and leadership-driven change management – significantly enhances system reliability and risk mitigation effectiveness.* ***Novelty:*** *This study highlights the strategic value of aligning transactional accuracy with enterprise-wide risk governance by emphasizing predictive analytics, customizable dashboards, and risk-aware organizational culture as critical enablers of modern financial governance.*

INTRODUCTION

In today's fast-paced and unpredictable financial world, companies recognize that integrating Accounting Information Systems (AIS) with Enterprise Risk Management (ERM) is crucial for improving their ability to monitor financial risks in real time. The capability to quickly access and analyze accurate data has become essential for making informed decisions and managing risks effectively. This integration not only streamlines reporting processes but also equips organizations with the necessary tools to spot, evaluate, and address various risks such as technological failures, operational hiccups, and compliance issues before they evolve into serious problems [1]. By adopting this proactive strategy, companies can maintain financial stability and build long-term resilience. Traditionally, financial reporting relied on manual processes that were often slow, prone to errors, and reactive. This isolation of accounting practices made it challenging for organizations to respond quickly to financial challenges, leaving them exposed during crises. For instance, accounting information was often confined to specific departments, preventing effective communication across the organization and

complicating comprehensive risk analysis. This fragmentation led to delayed decision-making and a sluggish response to emerging risks. Technology has dramatically changed this scenario. The introduction of computerized accounting systems, automated data processing, and cloud-based financial platforms has revolutionized how financial reporting and control are conducted. Real-time accounting, in particular, has been a game-changer, allowing for immediate insights into a company's financial well-being. With access to real-time data, managers can respond to risks as they arise instead of relying on outdated information [2]. This shift from static reporting to dynamic monitoring has fostered stronger alignment between AIS and ERM, paving the way for a more integrated and strategic approach to risk management. Moreover, ERM frameworks contribute structure and methodology for identifying, assessing, and addressing risks throughout the organization. When combined with AIS, ERM enables the creation of comprehensive risk registers that not only capture financial risks but also account for operational, technological, and compliance aspects. This integration allows for smooth data flow, from detailed transaction records to high-level strategic planning, making it easier to meet regulatory requirements and align risk management with the company's overall goals. However, integrating AIS and ERM does come with its challenges. Many organizations still rely on outdated legacy systems that may not work well with modern platforms, and upgrading these systems requires significant investment, technical know-how, and good change management practices. Resistance from employees towards new technologies, especially when they disrupt established workflows, can delay the integration process. Therefore, strong leadership and support from senior management are vital in effectively implementing both the technical upgrades and the cultural shifts required [3]. Overcoming these obstacles is crucial for organizations to fully appreciate the benefits of harnessing the synergy between AIS and ERM, including better resource allocation, enhanced data integrity, and improved predictive analytics [4]. At its core, an AIS serves as the technological foundation for this integration. It is a structured system designed to manage and process financial data, facilitating its collection, storage, and sharing across the organization. An effective AIS hinges on six key components: people, procedures, data, software, IT infrastructure, and internal controls. Together, these elements ensure that financial information is gathered accurately, processed efficiently, and distributed appropriately to all relevant stakeholders. An AIS primarily fulfills three roles: it collects and stores essential financial data, applies controls to maintain its integrity, and presents actionable information that aids in managerial decision-making. By delivering reliable and timely financial insights, AIS significantly enhances the quality of data available for ERM, making risk assessments more precise and actionable. Ultimately, AIS provides the essential data needed, while ERM offers the framework to analyze and act upon that information [5]. Together, they elevate accounting from a routine record-keeping role into a strategic tool for enhancing organizational resilience. As businesses navigate the uncertainties of a volatile global economy filled with financial challenges, cyber threats, and regulatory complexities integrating AIS and ERM stands out as a vital strategy. This combination not only equips

organizations to respond effectively to risks but also empowers them to anticipate potential threats, thereby fortifying their financial resilience and ensuring lasting success.

RESEARCH METHOD

This study employed a qualitative conceptual review approach to examine the integration of Accounting Information Systems (AIS) and Enterprise Risk Management (ERM) in supporting real-time financial risk monitoring. Relevant scholarly articles, standards, and empirical studies were identified through a structured literature search of reputable databases, including Google Scholar, Scopus-indexed journals, and peer-reviewed accounting and risk management publications. The selection criteria focused on studies discussing AIS architecture, ERM frameworks, cybersecurity vulnerabilities, real-time reporting, and organizational governance. The collected literature was systematically analyzed using thematic analysis to identify key patterns related to system functions, integration mechanisms, common vulnerabilities, mitigation strategies, and implementation challenges. Conceptual synthesis was then applied to integrate findings into a coherent analytical framework explaining how AIS and ERM jointly enhance proactive risk identification, decision-making quality, and organizational resilience. This method allows for an in-depth understanding of contemporary practices and challenges in AIS–ERM integration without relying on primary empirical data.

RESULTS AND DISCUSSION

Result

Functions, Integration, and Vulnerabilities of AIS and ERM

In today's business world, Accounting Information Systems (AIS) and Enterprise Risk Management (ERM) work hand in hand. They form the backbone of effective financial management, providing both oversight and a strategy for navigating risks. Together, they shift financial management from merely responding to problems to actively preparing for them. At its heart, an AIS manages essential financial tasks—like recording transactions, handling accounts payable and receivable, and producing on-time financial reports [6]. It not only supports everyday operations but also ensures that the data available for deeper analysis is accurate and trustworthy. AIS falls into three categories: manual systems that rely heavily on human effort (and are becoming a thing of the past), legacy systems that still exist in some organizations but often face inefficiencies, and modern computerized systems that represent the best practice today. These modern systems automate key tasks such as posting journal entries and reconciling accounts, significantly reducing human error, boosting efficiency, and providing real-time access to vital financial information needed for sound decision-making. On the flip side, ERM offers a comprehensive approach to spotting, evaluating, and managing the risks that might jeopardize an organization's goals [7]. It focuses on anticipating risks before they escalate into serious problems. By considering a wide array of risks financial, operational, technological, and environmental ERM helps organizations be ready for whatever uncertainty comes their way. A solid ERM strategy not only helps prevent

unexpected losses but also encourages smarter decision-making by weaving risk awareness into the fabric of everyday operations and strategic planning. When AIS and ERM work together, they elevate one another's effectiveness. AIS provides the structured financial data that ERM needs to monitor and assess Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) in real-time. This synergy enables organizations to create dynamic dashboards that give decision-makers access to the most relevant and current financial metrics. As a result, financial management aligns closely with organizational strategies, allowing managers to allocate resources more effectively, engage stakeholders, and ensure compliance with regulations. This combination also strengthens financial forecasting, improves reserving practices, and enhances adaptability to changing market conditions. ERM tackles a variety of risks that can directly impact financial stability [8]. For example, technological risks like system failures or cyberattacks can disrupt operations and jeopardize sensitive data. Human capital risks might arise from issues related to workforce shortages or skill gaps. Environmental risks, which can include natural disasters and sustainability challenges, may also influence long-term success. Legal risks, such as disputes or regulatory noncompliance, highlight the need for thorough monitoring and reporting. By integrating data from AIS into the ERM process, organizations can better predict these risks, measure their potential effects, and develop effective strategies to address them. However, it's important to note that AIS itself isn't without vulnerabilities, and these weaknesses can weaken even the best ERM strategies. Common issues include human errors in data entry, weak password practices that could allow unauthorized access, and outdated software without necessary security updates. Moreover, the threat of phishing and social engineering attacks continues to loom, preying on human behavior to access sensitive financial data. If not addressed, these vulnerabilities can compromise the integrity and confidentiality of financial information, damage stakeholder trust, and expose organizations to significant losses [9]. To counter this, it's essential to strengthen internal controls, invest in cybersecurity, and cultivate a culture of digital awareness. AIS provides the technology and procedures needed to manage financial data, while ERM offers a strategic framework for identifying and addressing risks. Their integration creates a strong synergy that enhances transparency, boosts financial resilience, and promotes sustainable growth. Yet, achieving this integration requires vigilance in addressing the vulnerabilities within AIS to protect the accuracy, integrity, and security of financial information. Organizations that find this balance are better equipped to thrive in today's complex landscape.

Common Vulnerabilities in Accounting Information Systems

Accounting Information Systems (AIS) play a crucial role in managing finances, but they can have their fair share of weaknesses that put sensitive financial data at risk. It's important for organizations to recognize and tackle these vulnerabilities to protect their information and stay resilient in today's digital age (Table 1).

Table 1. Common Vulnerabilities in Accounting Information Systems (AIS) and Their Implications

Vulnerability	Description	Implications	Reference
Outdated software and hardware	Use of legacy systems without timely updates and patches	Increases exposure to cyberattacks exploiting known flaws	[1]
Human error	Mistakes in data entry, miscalculations, or negligence in handling information	Leads to inaccurate financial reporting, possible fraud	[2]
Weak/reused passwords	Employees using simple or repeated passwords	Enables unauthorized access to sensitive financial data	[4]
Phishing and social engineering attacks	Deceptive emails or calls tricking employees into revealing credentials	Data breaches, financial losses, reputational damage	[5]
Lack of incident response planning	Absence of structured procedures to handle breaches	Prolonged downtime, loss of trust, regulatory penalties	[5],[6]

One major vulnerability stems from using outdated software and hardware. Cybercriminals often take advantage of known flaws in systems that haven't been properly updated. Organizations that lag in keeping their software and hardware up to date become easy targets for attacks [10]. To help minimize the chances of unauthorized access or data breaches, regular updates, timely patches, and hardware upgrades are essential. Ignoring these practices can leave financial systems vulnerable to threats that are already recognized and exploited by bad actors. Another significant source of vulnerability in AIS is human error. Despite technological advancements, financial systems still heavily depend on human input, which opens the door for mistakes like data entry errors or miscalculations. These seemingly minor blunders can lead to serious consequences, such as distorted financial reports or even fraud. Providing training for employees on careful data handling and using automated error-checking tools can greatly lessen the impact of these mistakes. Weak or reused passwords also contribute to system vulnerabilities. When employees choose simple or obvious passwords—or use the same password across multiple accounts—cybercriminals can gain unauthorized access with ease. Establishing strict password policies that mandate complex and unique combinations is a vital protective measure. Adding two-factor authentication (2FA) can also provide an extra layer of security, making it much harder for intruders to breach sensitive accounts, even if they manage to steal passwords [11]. Phishing attacks, whether through misleading emails or phone calls, pose a persistent threat as well. These scams trick employees into revealing confidential details, like login information or financial

data, often through convincing but fake communications. To combat these tactics, it's essential to raise employee awareness and provide ongoing cybersecurity training. Organizations should also implement email filters and verification processes to reduce the risk of being exposed to harmful messages and calls. In addition to preventing vulnerabilities, organizations need to be prepared to react effectively when incidents occur. Having a solid incident response plan is crucial; it helps ensure that breaches are detected, contained, and addressed swiftly. This plan should outline communication methods, assign responsibilities, and detail the steps to restore system integrity. Regular security audits and penetration testing can further bolster defenses by identifying weaknesses before they can be exploited by attackers [12]. Ultimately, AIS vulnerabilities involve both technical and human elements ranging from old software and poor authentication practices to human mistakes and social engineering tactics. By blending preventative measures like patch management, strong password policies, and employee training with comprehensive incident response strategies, organizations can greatly enhance their security. Addressing these vulnerabilities goes beyond just protecting data; it's about building trust, ensuring compliance, and maintaining the financial stability of the organization in a digital-first business world.

Securing and Integrating AIS for Effective Enterprise Risk Management

To truly get the most out of Accounting Information Systems (AIS) in the context of Enterprise Risk Management (ERM), organizations need to prioritize two key goals: protecting financial data and using system integration to boost resilience and improve decision-making (Figure 2).

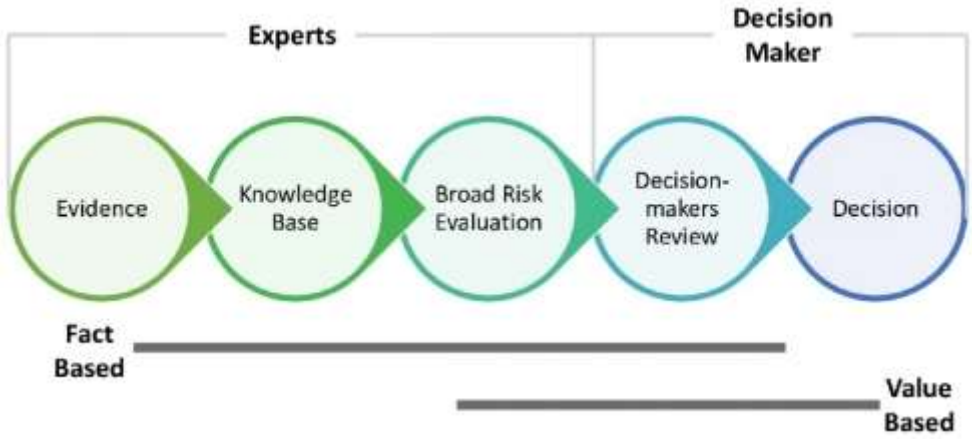

Figure 2. The links between facts and values in risk decision-making [29]

First and foremost, it's crucial to safeguard sensitive information, like employee records and financial details. Implementing strong encryption protocols, including end-to-end encryption for communications and transfers, is essential. Additionally, utilizing robust authentication methods such as multi-factor authentication and password managers can significantly decrease the risks of unauthorized access. Regular audits of encryption practices and user permissions are also important, as they help create a

culture of security awareness among employees. Training staff on security best practices can further strengthen this culture [13]. Moreover, having a solid disaster recovery plan in place is vital for getting operations back on track in case of a breach or disruption. Following the 3-2-1 backup rule which involves maintaining three copies of data, on two different types of media, with one copy stored offsite helps ensure data integrity. Automated backups can minimize human error and speed up recovery, reducing downtime for the organization. Investing in AI-driven monitoring tools allows for the early detection of unusual activities, enabling a proactive approach to security. Documenting security practices and ensuring compliance not only aligns with regulations but also demonstrates accountability during audits (Table 2)[14].

Table 2. Best Practices for Securing and Integrating AIS with Enterprise Risk Management (ERM)

Best Practice	Key Actions	Benefits	Reference
Strong encryption protocols	Implement end-to-end encryption, regular audits of practices	Protects sensitive data during transfer and storage	[8]
Multi-factor authentication (MFA)	Use MFA and password managers	Reduces risk of unauthorized system access	[12]
3-2-1 backup rule	Keep 3 copies of data, on 2 media types, with 1 offsite	Ensures data recovery during breaches or disasters	[13]
AI-driven monitoring tools	Detect anomalies in real-time	Enables proactive threat detection and mitigation	[15]
Vendor risk management	Evaluate third-party vendors' compliance and security standards	Minimizes external risks and ensures accountability	[18]
Change management and training	Continuous staff training and awareness programs	Builds a risk-aware organizational culture	[21]

It's also important to assess third-party vendors scrupulously, making sure they meet defined security standards through audits, authentication protocols, and preparedness for incident responses. Including these requirements in service level agreements (SLAs) can enhance accountability and mitigate external vulnerabilities. When organizations integrate secured AIS with ERM, they unlock significant benefits. Real-time processing improves both accuracy and responsiveness, while predictive analytics provide better insight into risk assessments. Centralized data governance enhances the quality and integrity of information, allowing for more effective resource

allocation based on trustworthy insights. Role-based dashboards can promote accountability among teams, and strategic planning can be enhanced with a comprehensive and continuously updated overview of key metrics [15]. This integrated approach not only helps mitigate potential issues by encouraging proactive risk management but also boosts the organization's adaptability to changing market conditions and regulatory requirements. By aligning security best practices with ERM, organizations can build trust and agility—two cornerstones of sustainable financial success.

Challenges and Implementation Strategies for Integrating AIS with ERM

The integration of Accounting Information Systems (AIS) and Enterprise Risk Management (ERM) for real-time monitoring of financial risks presents both exciting opportunities and considerable challenges. For organizations looking to adopt this integrated approach, it's crucial to understand the obstacles and implement strategies to navigate them effectively (Figure 1).

Figure 1. Several techniques and strategies are used to mitigate risks [28]

One major hurdle is the difficulty of aligning older systems with new, predictive tools [16]. Many organizations struggle to standardize data across various platforms and ensure that everything stays updated in real time. Additionally, inconsistent security protocols can compromise data integrity and compliance, creating potential vulnerabilities that need to be addressed. To tackle these issues, it's essential to build a strong, multidisciplinary technical team. This team should include experts in data governance, quality control, and access management to oversee the complexities involved in integration. By establishing a robust data governance framework, organizations can ensure clarity in data ownership, support regular audits, and enhance compliance adherence [17]. Another challenge is the resistance from employees when it

comes to adopting new technologies. Many professionals in accounting may be hesitant to embrace automation and AI-driven analytics, fearing that these advancements could disrupt their established workflows. Overcoming this resistance requires a thoughtful change management strategy that incorporates comprehensive training programs and ongoing learning opportunities. By creating a culture that values adaptability and innovation, organizations can encourage employees to welcome technological advancements instead of fighting against them. In addition to employee buy-in, the involvement of senior management is crucial for successful integration. When executives are not engaged—often due to competing priorities or lack of awareness about ERM's significance—it can stall efforts. Aligning risk management initiatives with the organization's broader goals and fostering a risk-aware culture can help in securing leadership support and ensuring necessary resources are allocated [18]. Choosing the right systems is also vital. Organizations should look for platforms that easily integrate with their existing infrastructure, are scalable, cost-effective, user-friendly, and comply with industry regulations. Customizing dashboards and system features to meet specific business needs can maximize integration benefits, ensuring decision-makers have access to the relevant and timely information they need. Once the systems are in place, continuous monitoring and optimization are essential for maintaining effectiveness. Regular feedback from users can highlight areas for improvement, and periodic reviews of system performance and security help strengthen data protection while reducing vulnerabilities. Automated compliance systems can further reduce human error and keep organizations aligned with changing regulations. Collaboration across departments is crucial for overcoming integration barriers like data standardization and synchronization [19]. Open communication and coordination among teams ensure transparency and promote a unified approach to governance and risk management. Additionally, cultivating a risk-aware culture through ongoing education and awareness programs keeps employees informed about emerging risks and regulatory changes, ultimately enhancing the organization's risk management framework. By understanding these challenges and implementing targeted strategies, organizations can effectively integrate AIS with ERM. This leads to greater resilience, real-time risk monitoring, and improved financial risk management—benefits that are well worth the effort.

Discussion

The integration of Accounting Information Systems (AIS) and Enterprise Risk Management (ERM) is more important than ever for organizations aiming to strengthen their resilience and monitor financial risks in real-time. In today's fast-paced business environment, companies must strike a balance between operational efficiency and proactive risk management. This discussion delves into how AIS and ERM work together, the vulnerabilities that could hinder their effectiveness, best practices to mitigate those risks, and the strategies needed to overcome challenges in integration [20]. AIS is essential for managing financial data, handling everything from transaction recording and accounts payable and receivable to generating reports. Over the years, these systems have transformed from manual processes to sophisticated computerized

platforms that automate routine tasks. This shift not only minimizes human errors but also boosts efficiency, accuracy, and the timeliness of financial reporting [21]. However, relying solely on AIS isn't enough to navigate the complex risk landscape that businesses face today. This is where ERM adds real value by providing a structured approach to identifying, assessing, and managing risks that could affect the organization's goals. By proactively surfacing potential threats—from tech disruptions to compliance issues—ERM enhances decision-making and safeguards long-term sustainability. The real magic happens when AIS and ERM are integrated. This synergy allows organizations to shift from static reporting to dynamic, real-time financial risk monitoring. AIS supplies the raw data, while ERM offers an analytical framework, enabling the creation of dashboards that track both Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) [22]. These metrics are crucial for understanding financial risks and ensuring that resources are allocated efficiently, all while keeping daily operations aligned with broader strategic goals. With this integration, organizations can proactively respond to changing market conditions and emerging threats. Yet, the path to integration isn't without its challenges. AIS itself faces various risks, including outdated software, human errors, weak passwords, and phishing attacks. Older systems pose a significant risk; cybercriminals can exploit vulnerabilities if they remain unpatched. Human mistakes such as data entry errors or negligence, can undermine the reliability of these systems. Additionally, weak or reused passwords create easy access points for malicious actors, while phishing attacks exploit human psychology to glean sensitive information. These vulnerabilities show that the effectiveness of AIS relies on both the technology used and the behavior of the users within the organization. If safeguards aren't in place, the integration of AIS and ERM could potentially increase risks instead of mitigating them. To tackle these vulnerabilities, organizations can adopt a set of best practices that strengthen both technological defenses and user awareness. Implementing strong data protection measures, especially through comprehensive encryption protocols, is key to keeping sensitive information secure [23]. Ensuring end-to-end encryption during data transfers, along with regular audits of these practices, significantly reduces the risk of breaches. Robust access controls, accompanied by multi-factor authentication and effective password management systems, further limit unauthorized access. It's equally vital to have incident response plans and backup strategies, like following the 3-2-1 rule for data backups, which ensures multiple secure copies of critical data are retained. Continuous monitoring of system activity, supported by AI-driven anomaly detection, adds another layer of security by enabling early identification of suspicious behavior [24]. At the organizational level, staying compliant with evolving regulations helps maintain accountability while meeting external expectations. When organizations adopt such practices, the benefits of integrating AIS and ERM become clearer. These integrated systems offer improved flexibility and performance, allowing businesses to swiftly adapt to unpredictable environments. Decision-makers gain access to real-time performance metrics, which helps them allocate resources more effectively and address inefficiencies. Moreover, governance frameworks enhance data integrity and quality by establishing clear ownership roles and quality

control mechanisms. Looking beyond immediate advantages, incorporating predictive analytics within these integrated systems enhances foresight, enabling organizations to anticipate risks and devise robust mitigation strategies. Integration fosters a sense of accountability across teams through role-based dashboards and performance tracking. Ultimately, aligning financial management with risk oversight strengthens the organization's ability to navigate challenges while pursuing its goals. Integrating Enterprise Risk Management (ERM) into an organization isn't just about technology; it's a vital part of creating a resilient, agile business [25]. Without clear support and resource allocation from leadership, these efforts can easily lose momentum. Often, executives don't fully grasp the value of ERM or think it's too complicated, which can lead to a lack of engagement. To turn this around, it's crucial to show them how integration can enhance resilience, lower risk, and promote sustained growth. Making ERM a core part of the organizational strategy and nurturing a risk-aware culture helps ensure leaders understand its importance and stay involved. Choosing the right technology is also essential for overcoming integration hurdles. Organizations should look for platforms that are scalable, user-friendly, and compliant with industry standards, while also fitting into their current systems. Features like customizable dashboards and analytical tools are key—they help decision-makers focus on what's most important. Once the systems are in place, ongoing monitoring and optimization are vital for maintaining their effectiveness. This involves regular performance reviews, gathering user feedback, and keeping the technology updated to meet changing business needs. Also, security audits and periodic reviews help to identify and address any vulnerabilities quickly. To make all this work, collaboration between departments is crucial. Open communication and shared responsibilities can help tackle challenges like data standardization and synchronization more effectively [26]. Skilled tech professionals are important in this process, but it's equally important to foster a culture of risk awareness across the organization. Regular training and awareness programs keep everyone informed about new threats and regulatory changes, reinforcing the need for vigilance at every level. Overall, integrating Accounting Information Systems (AIS) with ERM is a complex transformation that goes beyond just technical implementation. It requires attention to potential vulnerabilities, embracing best practices, and navigating the intricacies of organizational dynamics. When done successfully, the benefits are substantial: better financial oversight, improved decision-making, increased resilience, and real-time risk monitoring. Yet, reaching these goals involves overcoming considerable challenges [27]. This calls for a thoughtful mix of technical expertise, strong governance, leadership commitment, and cultural evolution. The discussions around integrating AIS and ERM are part of a larger trend in the digital transformation of financial management. As organizations face increasingly complex and uncertain environments, the combination of accurate financial data and robust risk management frameworks will be vital for maintaining growth and stability. Those that strategically invest in overcoming integration challenges and embedding risk awareness will be in the best position to harness the power of real-time financial risk monitoring.

CONCLUSION

Fundamental Finding : This study finds that the integration of Accounting Information Systems (AIS) and Enterprise Risk Management (ERM) constitutes a robust and strategic framework for real-time financial risk monitoring, enabling organizations to enhance transactional accuracy, anticipate emerging risks, and strengthen overall financial resilience. **Implication :** The findings imply that organizations adopting an integrated AIS–ERM approach can improve governance quality, regulatory compliance, transparency, and strategic decision-making, while fostering investor confidence and reducing exposure to unexpected financial losses in volatile environments. **Limitation :** Despite these contributions, this study is limited by its conceptual and literature-based nature, as it does not incorporate empirical data or sector-specific case evidence that could further validate the practical effectiveness of AIS–ERM integration across different organizational contexts. **Future Research :** Future studies are therefore encouraged to employ empirical methods, such as surveys or case studies, to examine implementation outcomes across industries, explore the role of organizational culture and leadership in integration success, and assess the impact of emerging technologies—such as artificial intelligence and advanced analytics—on enhancing real-time financial risk management capabilities.

REFERENCES

[1] M. Abdullah, Z. A. Shukor, Z. M. Mohamed, and A. Ahmad, "Risk management disclosure," *Journal of Applied Accounting Research*, vol. 16, no. 3, pp. 400–432, 2015, doi: 10.1108/JAAR-10-2014-0106.

[2] M. Akter and M. R. Haque, "Innovative quantitative models for enhancing financial resilience in U.S. capital markets," Business and Social Sciences, vol. 2, no. 1, pp. 1–6, 2024, doi: 10.25163/business.2110488.

[3] K. Al-Amri and Y. Davydov, "Testing the effectiveness of enterprise risk management: Evidence from operational losses," *Journal of Economics and Business*, vol. 87, pp. 70–82, 2016, doi: 10.1016/j.jeconbus.2016.07.002.

[4] M. R. Haque and P. Choudhury, "Exploring financial risk management approaches, challenges, and their effects on organizational performance outcomes," Journal of Primeasia, vol. 1, no. 3, pp. 1–8, 2020, doi: 10.25163/primeasia.1110486.

[5] A. Ara, M. A. A. Maraj, M. A. Rahman, and M. H. Bari, "The impact of machine learning on prescriptive analytics for optimized business decision-making," *International Journal of Management Information Systems and Data Science*, vol. 1, no. 1, pp. 7–18, 2024.

[6] M. J. Diba, M. R. Haque, and M. Akter, "Artificial intelligence enabled auditing for real-time financial reporting enhancing precision and regulatory compliance," Business and Social Sciences, vol. 2, no. 1, pp. 1–8, 2024, doi: 10.25163/business.2110492.

[7] A. Derbali and A. Lamouchi, "Global financial crisis, foreign portfolio investment and volatility: Impact analysis on select Southeast Asian markets," *Pacific Accounting Review*, vol. 32, no. 2, pp. 177–195, 2020, doi: 10.1108/PAR-07-2019-0090.

[8] M. R. Haque, "Resilient supply chain and adaptive marketing strategies: A post-pandemic framework for business sustainability," Journal of Primeasia, vol. 2, no. 1, pp. 1–7, 2021, doi: 10.25163/primeasia.2110437.

[9] C. Florio and G. Leoni, "Enterprise risk management and firm performance: The Italian case," *The British Accounting Review*, vol. 49, no. 1, pp. 56–74, 2017, doi: 10.1016/j.bar.2016.08.003.

[10] K. M. Hasan and M. S. Mia, "A project management model for deploying AI-based healthcare infrastructure," Journal of AI, ML & DL, vol. 1, no. 1, pp. 1–8, 2025, doi: 10.25163/ai.1110514.

[11] I. Iswajuni, A. Manasikana, and S. Soetedjo, "The effect of enterprise risk management on firm value in manufacturing companies listed on the Indonesian Stock Exchange," *Asian Journal of Accounting Research*, vol. 3, no. 2, pp. 224–235, 2018, doi: 10.1108/AJAR-06-2018-0006.

[12] M. J. Diba, "Integrating artificial intelligence into sustainability and ESG accounting: Enhancing environmental and social performance," Applied IT & Engineering, vol. 1, no. 1, pp. 1–8, 2023, doi: 10.25163/engineering.1110490.

[13] H. Khalfaoui and A. Derbali, "The determinants of foreign direct investment: Evidence from the Arab Maghreb countries," *Journal of Investment Compliance*, vol. 22, no. 4, pp. 295–308, 2021, doi: 10.1108/JOIC-04-2021-0010.

[14] M. Akter and M. R. Haque, "Optimizing risk assessment frameworks to support sustainable economic development in the United States," Journal of Primeasia, vol. 4, no. 1, pp. 1–7, 2023, doi: 10.25163/primeasia.4110433.

[15] Y. Li, J. He, and M. Xiao, "Risk disclosure in annual reports and corporate investment efficiency," *International Review of Economics & Finance*, vol. 63, pp. 138–151, 2019, doi: 10.1016/j.iref.2018.08.021.

[16] K. M. Hasan and M. R. Haque, "Leadership competencies for managing AI and IT modernization projects," Applied IT & Engineering, vol. 2, no. 1, pp. 1–8, 2024, doi: 10.25163/engineering.2110532.

[17] R. Mahi, "Optimizing supply chain efficiency in the manufacturing sector through AI-powered analytics," *International Journal of Management Information Systems and Data Science*, vol. 1, no. 1, pp. 41–50, 2024.

[18] M. R. Haque and M. Akter, "Crisis prevention and early-warning systems in financial risk management for U.S. market stability," Journal of Primeasia, vol. 4, no. 1, pp. 1–8, 2023, doi: 10.25163/primeasia.4110489.

[19] M. F. Malik, M. Zaman, and S. Buckby, "Enterprise risk management and firm performance: Role of the risk committee," *Journal of Contemporary Accounting & Economics*, vol. 16, no. 1, Art. no. 100178, 2020, doi: 10.1016/j.jcae.2019.100178.

[20] M. Sharfuddin and S. K. Papia, "Management information systems driven green marketing intelligence for sustainable consumer engagement," Journal of Primeasia, vol. 4, no. 1, pp. 1–7, 2023, doi: 10.25163/primeasia.4110496.

[21] B. W. Nocco and R. M. Stulz, "Enterprise risk management: Theory and practice," *Journal of Applied Corporate Finance*, vol. 18, no. 4, pp. 8–20, 2006, doi: 10.1111/j.1745-6622.2006.00106.x.

[22] M. N. M. Khan, "Artificial intelligence driven big data and business analytics: A comprehensive review of multi-sectoral applications in healthcare, finance, supply chain, and organizational innovation," *PJBIS*, vol. 2, no. 4, pp. 122–137, Nov. 2025, doi: 10.70818/pjbis.v02i04.0130.

[23] M. J. Diba and F. Zannat, "The artificial intelligence (AI) era's evident effect on accounting careers and skills," Business and Social Sciences, vol. 1, no. 1, pp. 1–9, 2023, doi: 10.25163/business.1110390.

[24] M. Akter, M. R. Haque, and M. I. Hossain, "Integrating artificial intelligence and machine learning into U.S. financial risk management systems," Journal of Primeasia, vol. 6, no. 1, pp. 1–8, 2025, doi: 10.25163/primeasia.6110430.

[25] M. Rahaman and M. Bari, "Predictive analytics for strategic workforce planning: A cross-industry perspective from energy and telecommunications," *International Journal of Business Diplomacy and Economy*, vol. 3, no. 2, pp. 14–25, 2024.

[26] M. Akter, M. R. Haque, and M. I. Hossain, "Integrating artificial intelligence and machine learning into U.S. financial risk management systems," *Journal of Primeasia*, vol. 6, no. 1, pp. 1–8, 2025, doi: 10.25163/primeasia.6110430.

[27] M. Sharfuddin and P. Choudhury, "Enhancing data reliability in management information systems through artificial intelligence driven validation and error detection models," Journal of AI, ML & DL, vol. 1, no. 1, pp. 1–8, 2025, article no. 10442.

[28] D. M. Sprčić, A. Kožul, and E. Pecina, "State and perspectives of enterprise risk management system development: The case of Croatian companies," *Procedia Economics and Finance*, vol. 30, pp. 768–779, 2015, doi: 10.1016/S2212-5671(15)01326-X.

[29] M. Shamim, "Digital leadership in project management in the emerging digital era," *Global Mainstream Journal of Business, Economics, Development & Project Management*, vol. 1, no. 1, pp. 1–14, 2022, doi: 10.62304/JBEDPM.V1I1.1.

*** Munkashir Hossen (Corresponding Author)**
Bangladesh Open University, Bangladesh
Email: munkashir@gmail.com