https://doi.org/10.34074/rere.00604

Literature Review

# Managing Professional Liability Risks from Digitalisation in New Zealand Accounting Firms

Imeshika Wickramaratne, Indrapriya Kularatne, and Jishuo (Jimmy) Sun

AIC OTAGO POLYTECHNIC

## ABSTRACT

Digitalisation is transforming accounting practice in New Zealand through the adoption of cloud accounting, artificial intelligence (AI), and data analytics, while simultaneously introducing new professional liability risks. Although previous studies have examined cybersecurity, digital competencies, and ethical issues associated with digital technologies, these risks have largely been investigated in isolation, providing a limited understanding of how they collectively shape professional liability in New Zealand accounting firms. To address this gap, this study has identified 74 sources of literature, ranging from academic studies to industry reports and professional guidelines, in a systematic literature review. Our review identifies three interconnected themes: (1) cybersecurity and data governance, (2) digital competency and skills gaps, and (3) ethical and professional responsibility. The findings suggest that managing professional liability requires an integrated approach that combines robust cybersecurity practices, continuous development of digital capabilities, effective governance, and professional judgement. By synthesising these interconnected risk dimensions, this study provides a conceptual understanding of professional liability management and offers practical recommendations to support secure, ethical, and sustainable digital transformation in New Zealand accounting firms.

*Keywords: Digitalisation, Accounting Profession, Professional Liability Risk, Cybersecurity, Artificial Intelligence (AI), Ethical Governance, Digital Skills Gap*

## INTRODUCTION

Digitalisation has fundamentally reshaped the accounting profession by enabling the widespread adoption of cloud accounting, artificial intelligence (AI), business intelligence, and data analytics to automate routine tasks, improve decision-making, and enhance advisory services (Mai, 2025). These technologies have transformed the role of accountants from traditional record keepers to strategic business advisors capable of delivering effective data-driven and value-added services. However, these services increase the risk of professional liability, including cybersecurity breaches, data inaccuracies, ineffective governance, and ultimately, financial, regulatory and reputational impacts (Nurwanah, 2024). Consequently, managing professional liability has become an increasingly important strategic issue as accounting firms seek to balance technological innovation with professional responsibility. Professional liability is defined as exposure to law, regulations, finances, or discipline due to failure to meet the professional responsibilities for confidentiality, competence, due care, judgement, or oversight (Faruque et al., 2024).

The accounting industry in New Zealand is changing rapidly with cloud-based accounting software such as Xero, MYOB and QuickBooks and the development of artificial intelligence, business intelligence and data analytics. These technologies improve the efficiency of operations, real-time reporting and better service delivery to clients (Sahni, 2021). New Zealand accounting firms, many of which are small and medium-sized practices, face increasing reliance

on remote collaboration, third-party cloud service providers, and AI-supported decision-making while at the same time remaining responsible for protecting highly sensitive financial and personal information under the Privacy Act 2020, and relevant professional standards issued by Chartered Accountants Australia and New Zealand. This combination of rapid digital adoption, regulatory obligations, and resource constraints creates unique professional liability challenges that warrant closer examination (Kafi & Akter, 2023).

Although previous studies have examined individual issues like cybersecurity, digital competencies, AI adoption, or ethical governance in accounting, these topics have largely been investigated independently. Existing research provides limited understanding of how these interconnected risks collectively influence professional liability within accounting firms, particularly in the New Zealand context. As digital technologies become increasingly integrated into accounting practice, cybersecurity vulnerabilities, capability gaps, governance weaknesses, and ethical responsibilities are no longer isolated challenges but mutually reinforcing factors that require an integrated risk management perspective.

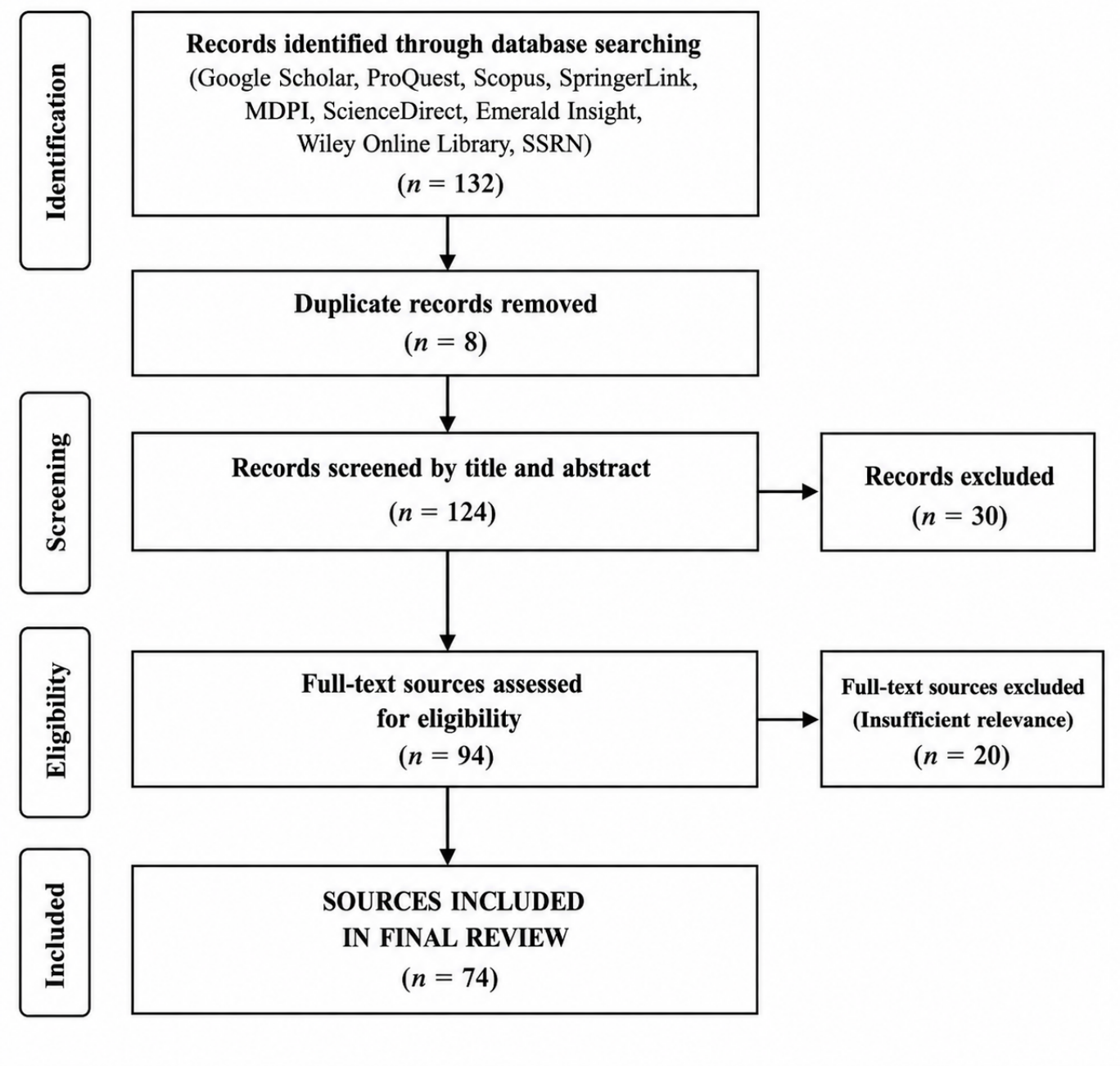
To address this gap, this study examines how New Zealand accounting firms can manage professional liability risks arising from increasing digitalisation by employing a systematic literature review. This study contributes to the literature by providing a more holistic understanding of professional liability risks in digital accounting while offering practical recommendations to support secure, ethical, and sustainable digital transformation within New Zealand accounting firms.

## METHODOLOGY

This study adopted a systematic literature review to examine how digitalisation contributes to professional liability risks in New Zealand accounting firms and to identify practical strategies for managing these risks. A systematic literature review was considered appropriate because it enables a structured synthesis of existing academic and professional knowledge of an emerging topic (Snyder, 2019). The literature search was conducted from 15th February to 20th March 2026 in the databases Google Scholar, ProQuest, Scopus, SpringerLink, MDPI, ScienceDirect, Emerald Insight, Wiley Online Library, and SSRN, from 1st January 2016 to 15th March 2026. These were done through the use of a range of key Boolean search strings, incorporating the terms: (“accounting profession” OR “accounting firm”) AND (“digitalisation”OR “digital transformation”) AND “professional liability”; ( “accounting profession” OR accountant) AND (cybersecurity OR “data governance”); ( “accounting profession” OR accountant) AND (digital competency OR “digital skills gap”); and ( “artificial intelligence” OR AI) AND (ethics OR “professional responsibility”); with “New Zealand” and “Aotearoa” included where appropriate. Sources examining digitalisation and professional liability in accounting in English were included; however, irrelevant, non-English, and duplicate texts were excluded. An assessment of relevant grey literature from Chartered Accountants Australia and New Zealand (CA ANZ), the Association of Chartered Certified Accountants, the New Zealand National Cyber Security Centre, the Office of the Privacy Commissioner (2025, 2026), Netsafe NZ and the Privacy Act 2020 was also undertaken. Duplicates were found using the title, authors, year of publication and DOIs. The 132 records identified yielded eight duplicate records that were deleted, leaving 124 records to be screened for title/abstract review. Post screening, 30 records were excluded and 94 full-text sources were evaluated for eligibility. Twenty other sources were deemed irrelevant and/or did not meet the inclusion criteria, leaving 74 sources for the final review. The quality and relevance of the included literature were assessed by considering source credibility, the clarity and evidential support of its findings or recommendations, and its applicability to digitalisation and professional liability in New Zealand accounting practice. Thematic analysis involved coding recurring risks and mitigation strategies, comparing codes across sources, and grouping related codes

into three overarching themes: cybersecurity and data governance, digital competency and skills gaps, and ethical and professional responsibility. The screening process is explained by a flow diagram in the PRISMA format shown in Figure 1:

**Figure 1: Methodology for Examining Explainable Artificial Intelligence and Trust in New Zealand Digital Media**



## FINDINGS AND DISCUSSION

### Cybersecurity and Data Protection Governance

Cybersecurity is the set of protective measures implemented to defend digital systems, networks, and data against unauthorised access and cyber threats in the accounting profession (Nurwanah, 2024). Accounting firms are facing increasing threats to their cybersecurity due to digitalisation. They are highly targeted by cyber criminals because accounting firms deal with highly sensitive financial data and their presence in client networks, which enhance the risk of data exfiltration, accounting record manipulation, operational impairment, and subsequent adverse legal and reputational damage (Hasan et al., 2024; Legenchuk et al., 2022). Threats such as phishing, ransomware, insider attacks, and unauthorised access are commonly witnessed, and thus, cybersecurity emerges as a significant professional liability issue instead of a technical one (Nyombi et al., 2024; Rajib et al., 2024). In New Zealand, cyber security issues can lead to a breach of obligations under privacy, confidentiality and data protection in the Privacy Act 2020, and professional standards, creating professional liability.

### Multi-Layered Cybersecurity Measures and AI-driven Cybersecurity Measures

This mitigation strategy installs a set of measures such as an encryption system, firewalls, intrusion detection models, and multi-factor authentication tools (Nurwanah, 2024). Deloitte, PwC, and EY have taken it further by adopting AI-driven monitoring, blockchain-based security and automated fraud detection devices, thus making it possible to identify such threats in real time, and to enlarge data integrity (Deloitte, 2024). However, these solutions require massive resources, constant improvements, and specialised knowledge. Although they provide a competitive edge to large organisations, smaller practices are facing limitations in finances and capabilities (Hasan et al., 2024).

### Governance Structure on Cybersecurity

This offers another avenue for risk management by incorporating security-related notions into the organisational decision-making process. Collaboration among accountants, auditors, management and IT specialists is essential, but the effectiveness of the governance structure depends on the implementation reliability (Almaqtari, 2024). Poor enforcement and limited awareness will often relegate such frameworks to compliance processes rather than to realistic risk management, which needs to be considered in both their design and in how they have been incorporated into organisational behaviour (Australia & Zealand, 2022; Hasan et al., 2024).

### Employee Awareness Programmes and Training

The objective of the awareness programmes is to mitigate the threat of human error. Well-informed staff are better placed to identify phishing attacks and comply with safe rules, thereby enhancing organisational resilience and fostering a security-minded culture(Ugbebor et al., 2024). This is particularly applicable in accountancy, where employees work with very sensitive financial information. However, the fast-changing threat to the digital environment may require a regular updates of the curriculum, increasing the cost and complexity (Abrahams et al., 2024). Small companies tend not to have the funds to carry proper programmes, and training becomes a need rather than a reality unless investing continuously and supported by the sector (Saeed et al., 2023).

### Innovative Risk Management Systems

Risk management systems allow resilience and increased efficiency (Saeed et al., 2023). However, it is a common

practice for organisations to focus more on innovation than on security when they are in the initial stages of development, which exposes them to vulnerabilities (Zadorozhnyi et al., 2020).

### Regular Insight Tests and Security Audits

This approach helps to detect vulnerabilities, authenticate controls, and deliver data-specific decisions, mainly for large firms. These demand particular capabilities and high investment, which few smaller firms can afford (Amodu, 2024). Furthermore, due to the scheduling of audits, they may fail to detect any emergent threats, so it is important to monitor them continuously along with periodic evaluations.

### Cybersecurity Governance and Compliance

The number of cyber incidents with possible systemic consequences is high, and professional service providers can be targeted since they deal with confidential financial information ((NCSC), 2025). Measures to combat this problem should include better governance systems, improved industry standards, and cooperative work by the governmental authority, professional associations, and individual corporations themselves (Hollingworth, 2024; Ncubukezi, 2022).The report demonstrates a significant gap between large and small firms when adopting measures against cybersecurity threats. Large organisation strategies include AI-based monitoring, special security units, and in-built forms of governance that are implemented. Smaller companies depend on using disconnected security measures such as basic cloud security services, multi-factor authentication, a firewall, and basic training (Kendyala, 2020). Overall, there is no specific solution for all of these threats; however, the indication is that multilayered and combined strategies are the most effective in reducing the risk of cybersecurity and professional liability.

### Digital Competency and Skills Gap

The accounting profession has rapidly digitised, leading to the creation of a digital skills gap, which could lead to a professional liability risk. Artificial and business intelligence, data analytics, and cloud accounting are also changing the role of the accounting profession (Karim et al., 2025). Cloud accounting, AI, Business Intelligence dashboards and sophisticated data analysis help accountants process vast amounts of data, uncover trends and anomalies, and provide valuable insights to assist in better decision-making, operational efficiency and financial advice (Elo, 2025; Imjai et al., 2025). Although these tools support more efficient, data-informed decision-making, gaps remain in accountants' ability to use them effectively (Busulwa et al., 2025; Jain & Mitra, 2025). This misalignment demonstrates the need for integrated solutions. Insufficient digital competence can therefore result in liability in that the error or over-reliance on the output of an automated system can interfere with the attainment of professional liability, due care or client advice.

### Development of Digital Competencies

Continuous professional development is a crucial factor in reducing capability gaps. Digital competence increases the ability of accountants to interpret data and detect anomalies in order to support strategic decisions, thus supporting the shift towards an advisory role (Yigitbasioglu et al., 2022). However, rapid technological change can quickly render skills outdated, creating a need for ongoing training (Kim & Park, 2020). Resources constraints causes greater challenges to smaller firms aiming at maintaining constant learning. Without training, organisational behaviour will not change. Therefore, it is essential to incorporate continuous learning into the firm's strategy and to be supported by professional bodies (Konstantinidou et al., 2023).

### Adoption of New Digital Technologies

Implementation of AI, cloud systems, Power BI, and analytics applications leads to process efficiency and abilities development (Talakola, 2022). Companies adopting such technologies achieve real-time knowledge, improved service provision and a competitive edge. However, employees can use these capabilities only if companies incorporate digital technology into their firms. Some risks are also present, including expensive implementation, vulnerability to cybersecurity, and over-reliance on automated outputs (Imjai et al., 2025). Excessive use of AI can destroy professional scepticism and increase the number of decision errors. These issues are especially critical in SMEs that have limited resources. A gradual adoption plan supported by training and a human supervision method will help to ensure professional judgement is supported by technology, as opposed to being replaced (Williamson & Prybutok, 2024).

### Technology Governance and Risk Management

Governance structures can address the risks relating to the use of digital technologies. These risks include automation bias, data integrity concerns, and cybersecurity risks. Good governance can improve accountability and can guarantee the observance of regulatory and professional standards (Australia & Zealand, 2022; Coman et al., 2022). However, this may increase complexity in the organisation and require expertise. Incorporating governance into the organisational culture should guarantee its practical effectiveness (Coman et al., 2022).

### Industry-Education Collaboration

Some firms focus on the partnership of universities, professional organisations and companies as a long-term solution to the digital skills gap. Matching education to industry needs will improve graduate preparedness, reduce training investments by organisations, and support the effectiveness of industry-based programmes and internships, therefore narrowing the gaps in capabilities. However, the implementation is slow due to the constraints of the curriculum and the different expectations of the stakeholders (Jackson et al., 2023).

Deloitte, PwC, and KPMG spend millions on advanced digital tools and well-structured training and governance (Abboud, 2025). Conversely, small firms adapt moderately and face financial and capacity constraints. This unbalanced digital maturity creates a competitive imbalance, where more technologically advanced companies gain efficiency and advisory benefits, while small companies face an increased risk of errors and professional liability (Coman et al., 2022; Faruque et al., 2024). The capability gap is reduced through the above solutions. Technology adoption improves efficiency but creates new risks; governance raises accountability, but little behavioural change occurs, and collaboration in education brings long-term benefits but is slow (Satjawisate et al., 2025). Therefore, an integrated approach to continuous learning, the use of scalable technology, and embedded governance is necessary to reduce the digital skills gap and provide the resilience and competitiveness of the accountancy profession in the long term.

### Ethical and Professional Responsibility in Digital Practice

Digitalisation in accounting has revolutionised accounting activities; however, it has also generated ethical and professional misconduct with the potential to result in regulatory penalties, negative publicity, and malpractices (Awang et al., 2022; Tiron-Tudor et al., 2025). Digitalisation in the accounting sector requires proper ethical governance, and poor ethical governance can result in legal liability, tarnished reputation, and loss of customer trust. Ethical governance is a strategic priority (Cheong, 2024; Ramachandran, 2025). Similarly, using AI solely without human judgement and oversight could lead to liability as it may deliver precise or biased outputs that lead to mistakes or biased strands. The following are suggested solutions for managing professional liability risk arising from ethical concerns.

### AI Governance Frameworks

AI governance models can be used to define responsibility, ethical principles, and establish risk management regarding the use of AI. These frameworks ease any uncertainty over automated output responsibility, since the designation of legal accountability still rests with professional practitioners (Ogunmokun et al., 2021). However, these models often become compliance-oriented tools that have little impact on the behaviour of practitioners. Statistics in New Zealand have shown that increased regulatory complexity has not increased ethical performance (Puchakayala, 2022). The effectiveness of governance could be determined by how it is executed and not merely designed. When large accounting firms use integrated systems of oversight, smaller companies usually rely on informal systems, thus increasing their vulnerability to risk (Ladley, 2019). The standardised, resource-effective models of governance are more efficient; SMEs require the uniformity of ethical practices, which is possible only through the means of the standardised governance models (Riso & Morrone, 2023).

### Automated Decision-Making Transparency

Automated decision making can provide transparency to AI outputs, which can then be interpretable, auditable and ethical. Lack of transparency will increase bias, error, and accountability gaps, while explainability increases trust and professional scepticism (Cheong, 2024; Saputro et al., 2025). Transparency increases the effectiveness of communicating with clients, providing a solution to the liability risks. However, AI systems are typically deployed as black boxes, and attempts to increase transparency can contradict privacy and economic concerns as well as intellectual property limitations (Saputro et al., 2025; Wang et al., 2025). Large companies use AI tools, but small companies often have no similar options which increases their dependence on automated results (Odonkor et al., 2024).

### The Human-in-the-Loop Model

The human-in-the-loop model has been deemed to be effective than entirely autonomous AI systems, specifically in tasks requiring professional judgement and oversight. Research has shown that within this paradigm, there is less automation bias as well as increased accuracy in decision-making compared with fully automated systems. At the end of the process, humans can use their professional judgements, avoid errors and improve their output (Agyepong et al., 2024; Carnat, 2024).

### Ethical Guidelines for Digital Advisory Services and Continuous Professional Development

Professional competence, confidentiality, and due care are vulnerable to breaches in digital environments that are supported by ethical guidelines. As solutions, Australia and Zealand (2022) promotes the view that AI can support professional judgement but not replace it, thus increasing accountability. Some accountants have limited familiarity with new technologies, thereby limiting the proper application of these ethical guidelines. Continuous professional education and training in digital ethics is necessary, as it has been proven that any deficiencies in capabilities will also increase the chances of making ethical mistakes and misusing digital tools in an indirect proportion (Australia & Zealand, 2022; Carnat, 2024). Unethical conduct may lead to breaches of data, bias in algorithms and undermining the integrity of financial reporting. Global audit failures are examples that show that over-reliance on electronic programmes reduces professional scepticism and increases error risk (Zhang et al., 2023).

Overall, AI governance, transparency, and ethical regulations are essential but unstable, and ineffective when implemented standalone instead of in an integrated model. Large firms such as Deloitte, PwC, EY, and KPMG adopt a combined governance structure and advanced digital systems, thus obtaining enhanced control and reducing li-

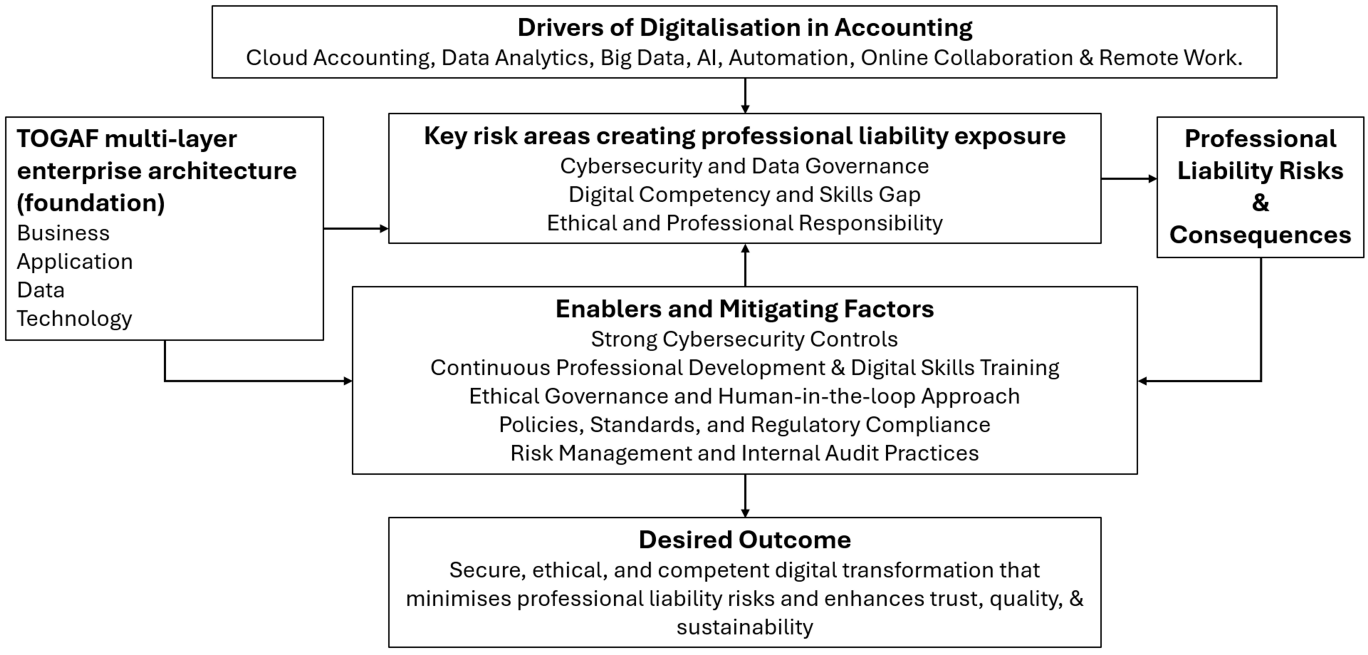
ability (Bibi, 2024). Smaller firms have resource and capability constraints that will hinder their successful implementation, and professional bodies need to support them (Odonkor et al., 2024). A combination of solutions will address the gaps and will reduce the risks of professional liability. The literature shows that digitalisation increases professional liability risks relating to cybersecurity, digital competency, and ethical responsibility. However, limited research has examined how these three interconnected areas can be managed collectively within New Zealand accounting firms. This research gap justifies the present study and the selection of these three themes to investigate how accounting firms can effectively manage professional liability risks arising from increasing digitalisation.

## Conceptual Framework for Managing Professional Liability Risks

The results of the review are presented in a conceptual framework provided in Figure 2, which has three key strands: (1) cybersecurity and data governance, (2) digital competency and skills gaps, and (3) ethical and professional responsibility. TOGAF was used as a lens for integrating into the structured enterprise architecture, following the themes that surfaced in the literature review. TOGAF was chosen because it is organised into business, application, data, and technology layers, which allows for a systematic structure in aligning digital practices, governance, and responsibilities.

To integrate these capabilities into organisational practice, the framework adopts the Open Group Architecture Framework (TOGAF) as an enterprise architecture model (Josey & Hornford, 2022). TOGAF provides a structured approach for aligning business processes, applications, data, and technology during digital transformation. Within this framework, cybersecurity and data governance support secure and compliant technology and data management. Digital competency enables the effective adoption and use of digital technologies across business processes, and ethical and professional responsibility provides the governance principles that guide responsible decision-making throughout the organisation. These three capabilities contribute to a more secure, ethical, and sustainable approach to digital transformation while reducing professional liability risks in New Zealand accounting firms.

**Figure 2: The Proposed Conceptual Framework Derived from the Review**



## RECOMMENDATION AND CONCLUSIONS

The recommendations are organised around the three themes identified in the review and are based on the evidence synthesised in the study.

### Cybersecurity and Data Governance

Accounting firms should adopt multilayered cybersecurity practices, including multi-factor authentication, encryption, secure backups, employee awareness, and appropriate governance (Nurwanah, 2024; Zadorozhnyi et al., 2020). Smaller firms with limited internal expertise may consider secure cloud services and external specialist support while maintaining appropriate oversight and accountability. Continuous cybersecurity awareness and training can further reduce risks associated with human error (Iqbal & Yusof, 2024; Santos, 2018). Cybersecurity insurance policy is also viable if the company can manage the cost (Ejeofobiri et al., 2025; Moore et al., 2016). Accounting firms should integrate cybersecurity policies into their long-term strategies and allocate management-approved budgets for their implementation (Ejeofobiri et al., 2025). Furthermore, sophisticated strategies such as Zero-Trust architecture and AI-driven threat detection could enhance cybersecurity resilience. Along with that, investment in cybersecurity within organisations should be directed towards the priorities of the organisation and available resources (Moore et al., 2016) and recognised information-security standards can also contribute to facilitating cybersecurity governance and resilience (Folorunso et al., 2024).

### Digital Competency and Skills Gaps

Continuous training, professional development and progressive adoption of digital technologies can strengthen accountants' digital capabilities and support effective technology use (Ali & Hasanah, 2024; Kim & Park, 2020). Recruitment based on strong digital skills and professional experience will fill the digital skills gap. The integration of digital skills into training programs, internship programs, and integrating digital skill competency should be included in performance appraisal (Musa & Nurhayati, 2025). Hiring dedicated digital support also gives an opportunity to attain the knowledge at a relatively lower price. Limited funding and technical skills represent the basic challenges; these could be mitigated by means of joint external collaboration, interaction with certified suppliers, and adoption stages (Grant, 2025; Noor, 2024) Collaboration among professional bodies like CA ANZ, education providers, and industry can help align accounting education and training with changing technological requirements (Duzguncınar, 2025; Herbert et al., 2021; Jackson et al., 2023).

### Ethical and Professional Responsibility

Accounting firms should maintain human oversight and critically evaluate AI-supported outputs to preserve professional judgement and reduce risks associated with automation (Schweitzer, 2024). Ethical governance and continuing professional development can further support responsible technology use, professional competence, and accountability. Professional bodies can support these practices through flexible, principle-based guidance as digital technologies evolve (Sillaber et al., 2021). Employees are recommended to evaluate AI outputs critically instead of mindlessly accepting them in order to strengthen their professional judgement and limit ethical hazards. However, time limitations and overdependence on automated systems are barriers. Realistic training can be used to address these by displaying real-world risks. Also, the ethical digital behaviour incorporated into the performance appraisals strengthens professional responsibility (Rajib et al., 2024). Subsidised training and funding helps smaller business organisations to implement ethical behaviours despite the difficulties of coordination. This is alleviated through the

collaboration between the government and professional organisations (Turyakira, 2018).

## Proposed Integrated Approach and Conclusion

Building on the evidence-supported recommendations above, the authors propose the TOGAF-based conceptual framework presented in Figure 2. The framework integrates cybersecurity and data governance, digital competency and skills, and ethical and professional responsibility across the business, application, data, and technology layers to provide a structured approach to professional liability risk management in New Zealand accounting firms.

In conclusion, digitalisation provides significant opportunities for New Zealand accounting firms but also creates professional liability risks. Effective risk management requires an integrated approach combining cybersecurity and data governance, continuous digital capability development, and professional judgement and ethical oversight. Together, these capabilities can support secure and responsible digital transformation while maintaining professional accountability and client trust.

## REFERENCES


Abboud, E. (2025). *The role of artificial intelligence in the financial industry: Enhancing financial analysis, early warning detection, and strategic recommendations (ssrn scholarly paper no. 5389089)*. Social Science Research Network. https://doi.org/10.2139/ssrn.5389089

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Samuel, O. D. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal*, *5*(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708

Agyepong, V., Cattoen, C., Adusei-Fosu, K., Buelow, F. A., Wilson, T. K., Qasim, M., Grimshaw, G. M., & Godsoe, W. (2024). *AI feedback loops in Aotearoa New Zealand: A human-centered creative problem-solving approach*. SocArXiv. https://doi.org/10.31235/osf.io/m5ehj

Ali, A. U., & Hasanah, U. (2024). Adaption of organisational culture in supporting digital transformation in accounting. *Journal Mutiara Management*, *9*(2), 167–178. https://doi.org/10.51544/jmm.v9i2.5580

Almaqtari, F. A. (2024). The role of IT governance in the integration of AI in accounting and auditing operations. *Economies*, *12*(8), 199. https://doi.org/10.3390/economies12080199

Amodu, O. (2024). Security auditors' perspective in tackling cyber-threats. *Journal of Multidisciplinary Engineering Science and Technology*, *11*(5), 16868–16875.

Australia, C. A., & Zealand, N. (2022, July). *CA cyber security playbook*. *CA ANZ cyber security*. https://www.charteredaccountantsanz.com/tools-and-resources/client-service-essentials/business-mindset/ca-cyber-security-playbook

Awang, Y., Shuhidan, S. M., Taib, A., Rashid, N., & Hasan, M. S. (2022). Digitalization of accounting profession: An opportunity or a risk for future accountants? *Proceedings*, *82*(1), 93. https://doi.org/10.3390/proceedings2022082093

Bibi, P. (2024). *Establishing transparency and accountability in AI: Ethical standards for data governance and automated systems*. https://www.researchgate.net/profile/Palwasha-Bibi-2/publication/384967741_Establishing_Transparency_and_Accountability_in_AI_Ethical_Standards_for_Data_Governance_and_Automated_Systems/links/670fc38224a01038d0f04435/Establishing-Transparency-and-Accountability-in-AI-Ethical-Standards-for-Data-Governance-and-Automated-Systems.pdf

Busulwa, R., Birt, J., Gepp, A., & Oates, G. (2025). Current state of accountants' knowledge of digital technologies: Evidence from Australia and New Zealand. *Accounting & Finance*, *65*(3), 2649–2664. https://doi.org/10.1111/acfi.70010

Carnat, I. (2024). Human, all too human: Accounting for automation bias in generative large language models. *International Data Privacy Law*, *14*(4), 299–314. https://doi.org/10.1093/idpl/ipae018

Cheong, B. C. (2024). Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, *6*. https://doi.org/10.3389/fhumd.2024.1421273

Coman, D. M., Ionescu, C. A., Coman, M. D., Uzlau, M. C., Stanescu, S. G., & State, V. (2022). Digitization of accounting: The premise of the paradigm shift of role of the professional accountant. *Applied Sciences*, *12*(7), 3359. https://doi.org/10.3390/app12073359

Deloitte. (2024). *Future of Cyber Survey 2024*. https://www.deloitte.com/global/en/about/press-room/deloitte-global-future-cyber-survey.html

Duzguncınar, T. (2025). Bridging the gap between industry needs and vocational training curricula. *Journal of Information Systems Engineering & Management*, *10*(44s), 693–707. https://doi.org/10.52783/jisem.v10i44s.8649

Ejeofobiri, C. K., Adelere, M., & Shonubi, J. A. (2025). Developing adaptive cybersecurity architectures using zero trust models and ai-powered threat detection algorithms. *International Journal of Computer Applications Technology and Research*, *11*(12), 607–621. https://doi.org/10.7753/IJCATR1112.1024

Elo, T. (2025). *An evolving landscape and skill requirements of the accounting profession: A Multistakeholder perspective*. https://lutpub.lut.fi/handle/10024/169644

Faruque, M. O., Chowdhury, S. N., Rabbani, M. G., & Khan, N. A. (2024). Technology adoption and digital transformation in small businesses: Trends, challenges, and opportunities. *International Journal for Multidisciplinary Research*, *6*(5), 1–21.

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582–2595. https://doi.org/10.30574/wjarr.2024.24.1.3169

Grant, O. (2025). *A Qualitative study on the impact of advanced technologies on supplier collaboration. Business, economics and management*. https://doi.org/10.20944/preprints202501.1730.v1

Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. *European Journal of Applied Science, Engineering and Technology*, *2*(6), 64–80. https://doi.org/10.59324/ejaset.2024.2(6).06

Herbert, I. P., Rothwell, A. T., Glover, J. L., & Lambert, S. A. (2021). Does the changing world of professional work need a new approach to accounting education? *Accounting Education*, *30*(2), 188–212. https://doi.org/10.1080/09639284.2020.1827446

Hollingworth, D. H. (2024, October 10). *Exclusive: New Zealand accounting firm confirms Sarcoma ransomware attack*. Retrieved October 10, 2024, from https://www.cyberdaily.au/security/11225-exclusive-new-zealand-accounting-firm-confirms-sarcoma-ransomware-attack

Imjai, N., Promma, W., Visedsun, N., Usman, B., & Aujirapongpan, S. (2025). Fraud detection skills of Thai Gen Z accountants: The roles of digital competency, data science literacy and diagnostic skills. *International Journal of Information Management Data Insights*, *5*(1), 100308. https://doi.org/10.1016/j.jjimei.2024.100308

Iqbal, F., & Yusof, Z. B. (2024). Efficacy of cybersecurity awareness training in reducing phishing vulnerabilities in organizations. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *8*(12), 10–21.

Jackson, D., Michelson, G., & Munir, R. (2023). Developing accountants for the future: New technology, skills, and the role of stakeholders. *Accounting Education*, *32*(2), 150–177. https://doi.org/10.1080/09639284.2022.2057195

Jain, V., & Mitra, A. (2025). Bridging the digital literacy gap: Effective collaboration between institutes of higher education and the workforce for technology integration. In *Institutes of higher education (ihe) and workforce collaboration for digital literacy* (pp. 71–90). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0004-7.ch003

Josey, A., & Hornford, D. (2022). *The TOGAF standard: A pocket guide*. Van Haren Publishing.

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15–26. https://doi.org/10.18034/ajtp.v10i1.659

Karim, D., Ahmad, K., & Ali, A. (2025). Artificial intelligence and the evolution of accounting: Transforming roles, skills, and professional practices. *Journal for Social Studies*, *2*(1).

Kendyala, S. H. (2020). *The role of multifactor authentication in securing cloud based enterprise applications (SSRN Scholarly Paper No. 5074876)*. Social Science Research Network. https://doi.org/10.2139/ssrn.5074876

Kim, J., & Park, C.-Y. (2020). Education, skill training, and lifelong learning in the era of technological revolution: A review. *Asian-Pacific Economic Literature*, *34*(2), 3–19. https://doi.org/10.1111/apel.12299

Konstantinidou, I., Dillenburger, K., & Ramey, D. (2023). Positive behaviour support: A systematic literature review of the effect of staff training and organisational behaviour management. *International Journal of Developmental Disabilities*, *69*(1), 29–44. https://doi.org/10.1080/20473869.2022.2123199

Ladley, J. (2019). *Data governance: How to design, deploy, and sustain an effective data governance program*. Academic Press.

Legenchuk, . O., Vyhivska, I. M., & Hryhorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security. *Problems of the Theory and Methodology of Accounting, Control, and Analysis*, *2*(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46

Mai, L. P. (2025). *Changes in competencies, capabilities, and decision-making in the accounting profession as a result of information digitalization and big data analytics/artificial intelligence*. https://unitesi.unive.it/handle/20.500.14247/7630

Moore, T., Dynes, S., & Chang, F. R. (2016). Identifying how firms manage cybersecurity investment. *Workshop on the Economics of Information Security University of California, Berkeley, 2016*.

Musa, S., & Nurhayati, S. (2025). The effect of internships on graduates' employability, soft skills, and digital competence. *Educational Process: International Journal (EDUPIJ)*, *17*(4), 1–31.

(NCSC), N. C. S. C. (2025). *CyberReport 2025*. https://www.ncsc.govt.nz/assets/insights/cyber-threat-report/NCSC-CyberReport2025-FINAL.pdf

Ncubukezi, T. (2022). Human errors: A cybersecurity concern and the weakest link to small businesses. *International Conference on Cyber Warfare and Security*, *17*, 395–403. https://doi.org/10.34190/iccws.17.1.51

Noor, N. H. (2024). *Affordable Cloud Empowerment: Revolutionizing small business operations with cost-effective cloud solutions: Revolutionizing small business operations with cost-effective cloud solutions* [Master's thesis, Metropolia University of Applied Sciences]. Theseus]. http://www.theseus.fi/handle/10024/861790

Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. *Advances in Applied Accounting Research*, *2*(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

Nyombi, A., Sekinobe, M., Happy, B., Nagalila, W., & Ampe, J. (2024). *Enhancing cybersecurity protocols in tax accounting practices: Strategies for protecting taxpayer information (ssrn scholarly paper no. 5225445)*. Social Science Research Network. https://papers.ssrn.com/abstract=5225445

Odonkor, B., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Farayola, O. A. (2024). The impact of AI on accounting practices: A review: Exploring how artificial intelligence is transforming traditional accounting methods and financial reporting. *World Journal of Advanced Research and Reviews*, *21*(1), 172–188. https://doi.org/10.30574/wjarr.2024.21.1.2721

Ogunmokun, A. S., Balogun, E. D., & Ogunsola, K. O. (2021). A conceptual framework for AI-driven financial risk management and corporate governance optimization. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(1), 772–780. https://doi.org/10.54660/.IJMRGE.2021.2.1.772-780

Puchakayala, P. R. A. (2022). Responsible AI ensuring ethical, transparent, and accountable artificial intelligence systems. *Journal of Computational Analysis and Applications*, *30*(1), 208–221.

Rajib, H., Sarkar, N. I., Alani, N. H. S., & Lutui, R. (2024). *Cyber edge: Current state of cyber security in Aotearoa-New Zealand, opportunities, and challenges. Current state of cyber security in aotearoa-new zealand, opportunities, and challenges*. Computer Science; Mathematics. https://doi.org/10.20944/preprints202409.2174.v1

Ramachandran, D. R. (2025). *Ethics and Corporate Governance*. Academic Guru Publishing House.

Riso, T., & Morrone, C. (2023). To align technological advancement and ethical conduct: An analysis of the relationship between digital technologies and sustainable decision-making processes. *Sustainability*, *15*(3), 1911. https://doi.org/10.3390/su15031911

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses' resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Sahni, K. N. (2021). *A systematic analysis of SAP enterprise resource planning (ERP) software implementation as accounting software in New Zealand organisations [Master of Applied Management, Otago Polytechnic]*. https://doi.org/10.34074/thes.5496

Santos, O. (2018). *Developing cybersecurity programs and policies*. Pearson IT Certification.

Saputro, M. E., Widhiatuti, R., & Arief, S. (2025). Accountants and AI: The ethical boundaries of adoption. *Proceedings of International Conference on Economics, Business, and Economic Education*, 112–121.

Satjawisate, S., Suriyapaiboonwattana, K., Saramolee, A., & Hone, K. (2025). Digital competencies for a fintech-driven accounting profession: A systematic literature review. *Informatics*, *12*(4), 121. https://doi.org/10.3390/informatics12040121

Schweitzer, B. (2024). Artificial intelligence (AI) ethics in accounting. *Journal of Accounting, Ethics & Public Policy, JAEPP*, *25*(1), 67–67. https://doi.org/10.60154/jaepp.2024.v25n1p67

Sillaber, C., Waltl, B., Treiblmaier, H., Gallersdörfer, U., & Felderer, M. (2021). Laying the foundation for smart contract development: An integrated engineering process model. *Information Systems and E-Business Management*, *19*(3), 863–882. https://doi.org/10.1007/s10257-020-00465-5

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Talakola, S. (2022). Analytics and reporting with Google cloud platform and Microsoft power BI. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(2), 43–52. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I2P106

Tiron-Tudor, A., Rodgers, W., & Deliu, D. (2025). The accounting profession in the twilight zone: Navigating digitalisation's sided challenges through ethical pathways for decision-making. *Accounting, Auditing & Accountability Journal*, *38*(3), 990–1018. https://doi.org/10.1108/AAAJ-12-2022-6173

Turyakira, P. K. (2018). Ethical practices of small and medium-sized enterprises in developing countries: Literature analysis. *South African Journal of Economic and Management Sciences*, *21*(1), 1–7. https://doi.org/10.4102/sajems.v21i1.1756

Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). Employee Cybersecurity awareness programs customised for sme contexts to reduce human-error related security incidents. *Journal of Knowledge Learning and Science Technology*, *3*(3), 382–409. https://doi.org/10.60087/jklst.vol3.n3.p382-409

Wang, M., Zhang, X., & Han, X. (2025). AI driven systems for improving accounting accuracy fraud detection and financial transparency. *Frontiers in Artificial Intelligence Research*, *2*(3), 403–421. https://doi.org/10.71465/fair398

Williamson, S. M., & Prybutok, V. (2024). The era of artificial intelligence deception: Unraveling the complexities of false realities and emerging threats of misinformation. *Information*, *15*(6), 299. https://doi.org/10.3390/info15060299

Yigitbasioglu, O., Green, P., & Cheung, M.-Y. D. (2022). Digital transformation and accountants as advisors. *Accounting, Auditing & Accountability Journal*, *36*(1), 209–237. https://doi.org/10.1108/AAAJ-02-2019-3894

Zadorozhnyi, Z.-M., Muravskyi, V. V., Shevchuk, ., & Muravskyi, V. (2020). The accounting systems as the basis for organising enterprise cybersecurity. *Financial and Credit Activity Problems of Theory and Practice*, *3*(34), 149–157. https://doi.org/10.18371/fcaptp.v3i34.215462

Zhang, C., Zhu, W., Dai, J., Wu, Y., & Chen, X. (2023). Ethical impact of artificial intelligence in managerial accounting. *International Journal of Accounting Information Systems*, *49*, 100619. https://doi.org/10.1016/j.accinf.2023.100619