# The Effect of Emerging Technological Risks on Insurance Companies' Performance: Challenges and Solutions in the Era of Digital Transformation

**Ghazi Ayed Alghathian**[1] **& Ahmad Abdalla Alahmad**[2,*]

**Abstract: Purpose/Objectives**: This study examines how digital transformation and emerging technologies have reshaped the global economy and affected the risk management strategies of insurance companies, particularly in adapting to technological risks. **Methods**: The study explores the impact of advancements in information and communication technologies, focusing on how insurance firms must evolve from traditional risk coverage to addressing technological and cybersecurity risks. **Results**: The study found that emerging technologies like AI, machine learning, blockchain, and the Internet of Things (IoT), present both opportunities and challenges for the insurance sector, particularly due to the heightened risk of cyberattacks on sensitive customer data. **Conclusion/Implications**: The study concludes that traditional risk management strategies are inadequate for addressing the new technological risks. It calls for the development of updated strategies to improve operational efficiency, reduce costs, and ensure the security of personal data. The study also advocates for mandatory insurance for risks related to personal data processing to support the sustainability of the industry.

**Keywords**: Digitization, Operational, Efficiency, Insurance Strategies, Insurance Risk, Law.

## تأثير المخاطر التكنولوجية الناشئة في أداء شركات التأمين: التحديات والحلول في عصر التحول الرقمي

**غازي عايد الغثيان**[1,*]، **وأحمد عبدالله الأحمد**[2*]

**الملخص: الهدف:** تتناول هذه الدراسة كيفية إعادة تشكيل التحول الرقمي والتقنيات الناشئة للاقتصاد العالمي، وتأثير ذلك في استراتيجيات إدارة المخاطر في شركات التأمين، لا سيما في التكيّف مع المخاطر التكنولوجية. **المنهجية:** تعتمد الدراسة منهجية وصفية تحليلية بُغية استكشاف تأثير تطوّر تكنولوجيا المعلومات والاتصالات في أداء شركات التأمين على نحو عام مع التركيز على كيفية انتقال شركات التأمين من التغطية التقليدية للمخاطر إلى التعامل مع المخاطر التكنولوجية ومخاطر الأمن السيبراني على نحو خاص. **النتائج:** توصلت الدراسة إلى أن التقنيات الناشئة مثل الذكاء الاصطناعي، وتعلم الآلة، وإنترنت الأشياء (IoT)، تُشكّل فرصًا وتحديات في آنٍ واحد لقطاع التأمين، خاصةً بسبب ارتقاع خطر الهجمات السيبرانية على البيانات الحساسة للعملاء. **الاستنتاجات:** خلُصت الدراسة إلى أن استراتيجيات إدارة المخاطر التقليدية لم تعد كافية لمواجهة المخاطر التكنولوجية الجديدة. **التوصيات:** تدعو الدراسة إلى تطوير استراتيجيات محدّثة تهدف إلى تحسين الكفاءة التشغيلية، وتقليل التكاليف، وضمان أمن البيانات الشخصية، كما توصي الدراسة بفرض التأمين الإلزامي ضد المخاطر المتعلقة بمعالجة البيانات الشخصية، لدعم استدامة القطاع.

**الكلمات المفتاحية:** الرقمنة، الكفاءة التشغيلية، استراتيجيات التأمين، مخاطر التأمين، القانون.

1 School of Law, The University of Jordan, Jordan. g_alghathian@ju.edu.jo
2 Information Technology Center, The University of Jordan, Jordan.
*Corresponding author: mal@ju.edu.jo

1 كلية الحقوق، الجامعة الأردنية، الأردن. g_alghathian@ju.edu.jo
2 مركز تكنولوجيا المعلومات، الجامعة الأردنية، الأردن.
* الباحث المرسل: mal@ju.edu.jo

## Introduction

Technology has become an integral part of daily life, transforming the world into a "small village" through rapid advancements, which have led to fundamental changes in various sectors, including the global economy (Soboh, 2025), significantly impacted by the information revolution and technological progress (Ortiz & Acosta, 2020). Today, humanity relies heavily on information, ensuring this trend extends into the future due to the close connection with accelerating technological development, making data protection against risks crucial (Volosovych, et al., 2021). These technological advancements have introduced new and unforeseen risks affecting all aspects of life, including the insurance sector, which has undergone significant changes in work methods and insurance concepts. This requires the redesign of processes to align with current progress, creating a balance in addressing the needs of modern transactions. The insurance sector plays a vital role in supporting stability, investment, and work environments, with profitability being key to the continued operation and stability of insurance companies (Czerwińska, 2017; Hilkevics & Semakina, 2019).

Emerging technologies refer to a group of technological innovations that are not yet fully developed but hold great potential to transform various fields in the near future. These technologies include Artificial Intelligence (AI), Machine Learning (ML), Blockchain, and the Internet of Things (IoT), along with other advanced technological solutions (Stark, 2020). These technologies are not limited to one sector; they impact numerous industries, including the insurance sector. For example, AI can enhance insurance companies' ability to predict risks, while Blockchain helps improve security and transparency in transactions, and IoT enables the collection of accurate customer behavior data, contributing to the development of innovative insurance solutions. Despite the opportunities these technologies offer, they also carry risks that could affect the sustainability and competitiveness of businesses, such as security risks and cyberattacks that could lead to the loss or theft of sensitive data (Pisoni, 2021). Additionally, regulatory and privacy risks exist that may compromise the integrity of operational transactions.

The question arises: Can insurance, in its current form, address modern technological risks and ensure high security in the face of rapid technological advancements? Insurance companies struggle to provide protection against these global, complex risks, leading to significant digital transformations within the sector. This shift impacts operations and competition, requiring effective risk management methods to improve efficiency and reduce costs. Automation plays a key role in this, alongside the need to enhance customer experience and offer innovative solutions. Regular assessments of technological risks are essential to keep pace with fast-paced developments. (Kadtke & Wells, 2014; Taherdoost, 2024).

Laws and regulations play a crucial role in regulating the use of emerging technologies within companies (Isleem, 2025). Amid the rapid advancement of technology, insurance companies are facing a growing need for updated legislation that can keep pace with emerging developments (Romanosky, et al., 2019). Many countries have begun to develop laws focused on the use of artificial intelligence and personal data protection, creating a regulatory framework that protects consumers and reduces security risks (Ullah, 2019). Companies that comply with these laws can avoid legal risks and gain customer trust. Therefore, it is necessary to reconsider traditional insurance foundations to cover

damages resulting from modern technological uses. In this context, technical and legal foundations can be modified to address these new risks in collaboration with reinsurance companies. Insurance contributes to transferring technology to markets and creating new industries, requiring the development of effective methods to assess emerging technological risks (Eckert & Osterrieder, 2020). Amid the digital transformation, insurance companies must invest more in technology to provide innovative services while addressing the new risks arising from these digital shifts (Eckert & Osterrieder, 2020).

Therefore, this study aims to outline a framework for an effective insurance strategy within a renewed concept and philosophy of risk coverage, shifting from traditional risk insurance to addressing real technological risks due to rapid technological advancements. Poor risk management is considered a multifaceted issue that increases insurance costs and undermines the effectiveness of insurance strategies.

## Research Problem

Rapid technological developments have significantly impacted the insurance sector in many aspects, bringing with them new and unexpected risks, particularly regarding cybersecurity, data protection, and the integration of emerging technologies such as artificial intelligence, blockchain, and the Internet of Things. Despite the positive benefits they have provided to the sector, they have also posed new challenges. This study addresses the problem of increasing reliance on technology and the transformation of the sector. Conversely, current insurance frameworks focus largely on traditional risks and have not been sufficiently updated to address the unique threats posed by rapid technological change. This study seeks to explore how the insurance

sector can adapt to these emerging technological risks, develop effective risk management strategies, and implement insurance solutions that meet the needs of modern transactions. The findings aim to contribute to the theoretical understanding and practical application of insurance strategies in the face of technological advancements.

## Significance of the Study

The study discusses traditional risk management to include challenges resulting from technological transformations, such as cybersecurity threats and data breaches, with the aim of expanding insurance coverage to include new and important areas such as privacy and data protection. Also, it focuses on developing new conceptual frameworks aimed at effectively assessing technological risks, enhancing academic research in the field of risk management in the era of digital transformation.

The study offers valuable insights for insurance companies, emphasizing the practical importance of adapting risk management strategies to tackle the growing technological threats. By doing so, it helps enhance operational efficiency, reduce costs, and safeguard sensitive customer data. Additionally, the study underscores the crucial role of technology developers in partnering with the insurance sector to create secure technologies that mitigate risks, ultimately fostering innovative and secure solutions that are well-suited to the digital landscape.

## Methodology

The study adopts a descriptive-analytical methodology to examine how different companies use emerging technologies and manage technological risks. It focuses on describing and analyzing the evolution and impact of technological risks in the insurance sector, and evaluating current strategies for addressing these risks. The collected data is

analyzed through a comparative analysis, comparing the risks and benefits of implementing emerging technologies with traditional risk management practices, while addressing the legal and technical frameworks that regulate the insurability of these risks. Data for this study was collected from various sources, including academic literature, industry reports, and insurance company case studies, focusing on major insurance companies that have successfully integrated emerging technologies, such as artificial intelligence, the Internet of Things, and blockchain, into their operations. Companies such as MetLife, Allianz, Lemonade, and Progressive serve as case studies to illustrate the practical application of these technologies in the insurance sector.

## Literature review

### Forms of Risks of Technological Uses

While technology provides immense benefits and has become essential in modern society, it also carries significant risks that must not be overlooked. The potential dangers associated with technological use affect both humans and the environment, with some risks having far-reaching consequences (Zhang et al., 2022). Contemporary legal scholars argue for the implementation of mandatory insurance to address liabilities resulting from technological risks, such as system failures, fraud, or environmental harm caused by technological activities (Eckert & Osterrieder, 2020). Such insurance systems would provide adequate protection and compensation for damages, particularly in complex fields like information technology and environmental pollution. As emerging technologies continue to evolve, these risks will only increase, requiring new insurance mechanisms to manage the liabilities associated with them.

This section is divided into three subsections: the first addresses the risks linked to information systems, the second examines the technological risks associated with personal data processing, and the third focuses on the emerging technology risks faced by insurance companies.

### Information Systems Risks

Information system errors, such as software malfunctions, fraud, or the introduction of malicious viruses, pose a significant threat to the integrity of technological infrastructures. These issues can impact various components of the system, including the physical hardware, logical structures, data integrity, and the operational systems that support these programs (Wilkinson et al., 2023). Because of the technical complexity involved, civil liability in the context of information systems is often based on the concept of "strict liability," which holds parties accountable for damages regardless of fault (Al-Sadeeq, 1999). This approach ensures that victims of information system failures receive compensation, even when it is difficult to pinpoint the exact cause of the breach. Legal scholars suggest that mandatory insurance should be implemented to address the liabilities arising from information systems, as traditional methods of risk management are inadequate for such complex technological risks (Volosovych et al., 2021). Given the widespread and unpredictable nature of these risks, similar to those associated with radioactive materials, insurance is necessary to ensure that damages can be covered, and affected parties adequately compensated (Eling et al., 2022).

The application of strict liability to information systems ensures that victims are compensated, but this approach raises challenges in attributing fault, particularly in cases involving complex technological failures or malicious attacks. Moreover, implementing mandatory insurance requires developing new

frameworks that go beyond traditional regulatory principles (Wilkinson et al., 2023).

## Technological Risks in Personal Data Processing.

The increasing use of technology to process personal data exposes individuals to various risks, including breaches of confidentiality, unauthorized alterations, and destruction of data (Al-Balooshi, 2017). Protecting this data requires balancing security measures with the practical demands of modern transactions. In addition to technical threats, risks to personal data include human errors, such as accidental access by unauthorized individuals, as well as natural risks, such as fire or other environmental factors that can compromise data integrity (Abu Hassan, 2022).

These risks are generally categorized into five key types. First, data confidentiality risks involve the threat of unauthorized access to personal information, which remains one of the most critical concerns (Abu Hassan, 2022). Second, data integrity risks focus on ensuring that data remains accurate, complete, and unaltered during both storage and transmission (Abu Hassan, 2022). Third, availability risks pertain to the need for data to be accessible to authorized users when required, supporting the continuity of services (Abu Hassan, 2022). Fourth, accountability risks emphasize the importance of traceability in data handling activities, allowing actions to be linked to specific individuals or entities to maintain transparency (Abu Hassan, 2022). Finally, data authentication risks highlight the necessity of verifying the identity of users or systems interacting with data, which is essential for upholding overall data security (Abu Hassan, 2022).

These risks can stem from external attacks, like hacking, or internal failures, such as human error or system flaws, and they pose significant challenges to data protection. Effective risk management strategies must account for both technical and human factors to safeguard the integrity, accuracy, and confidentiality of personal data.

While regulatory frameworks like data protection laws and risk assessments help address data security challenges, high-profile breaches, such as the 2013 Home Depot incident, reveal the persistent vulnerability of personal data. Additionally, as technologies like artificial intelligence and big data evolve, new risks emerge that require ongoing adaptation of security measures (Abu Hassan, 2022).

## Emerging Technology Risks for Insurance Companies

Emerging technologies present both opportunities and risks for insurance companies. As these technologies evolve, insurance companies are increasingly reliant on digital tools, which exposes them to new risks in several areas, including security, regulation, and data privacy. The following sections outline the key risks insurance companies face due to technological advancements:

1. **Security Risks**: The rise of emerging technologies increases the vulnerability of insurance companies to cyberattacks, which could result in the theft or loss of sensitive customer data. Cybersecurity breaches, such as viruses or malware, can disrupt operations, damage reputations, and lead to significant financial losses. Additionally, the integration of artificial intelligence and machine learning in data processing can create new security gaps if these systems are not adequately protected, potentially leading to inaccurate outcomes or security failures (Ahmed et al., 2024).

2. **Regulatory Risks**: As technology continues to evolve, insurance companies must navigate a constantly changing regulatory environment. Different countries impose

varying laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union, which imposes strict rules on how personal data is collected and processed. These regulatory challenges become more complicated as technologies like artificial intelligence require large datasets for analysis, which may conflict with privacy laws. Insurance companies also face the risk that existing regulations may be outdated, failing to address the unique risks posed by new technologies (Cappiello, 2018).

3. **Data and Privacy Risks**: Technologies like the Internet of Things (IoT) and artificial intelligence provide insurance companies with valuable insights into customer behavior and risk profiles. However, these advancements raise significant concerns about data security and privacy. If customer data is mishandled, misused, or exposed in a data breach, it could result in a loss of customer trust, financial penalties, and reputational damage. Managing the data collected by smart devices and ensuring privacy protection requires robust security measures to prevent hacking and data exploitation (Ahmed et al., 2024).

4. **Risks to Customer Relationships**: While automation and digital technologies offer increased convenience, they can also reduce the level of personal interaction between insurance companies and their customers. Some clients may value direct, human engagement and could feel alienated by the shift towards AI-driven services. Additionally, as AI and big data analytics become more widespread, customers may have higher expectations for personalized services, and companies that fail to meet these expectations risk losing customer loyalty (Cappiello, 2018).

5. **Operational Risks**: The heavy reliance on digital systems in insurance companies exposes them to operational risks, including technological downtime, data management challenges, and the high costs of system maintenance and upgrades. System failures, such as server crashes or cyberattacks, could halt essential insurance operations, while inaccurate or incomplete data may undermine decision-making. Additionally, the rapid pace of technological advancement requires constant investment in infrastructure and employee training, which can strain resources (Ahmed et al., 2024).

6. **Changing Business Models**: Technologies such as AI and blockchain are driving the emergence of new business models that could disrupt traditional insurance markets. Startups offering digital insurance solutions may threaten the dominance of established companies by offering more flexible, data-driven services (Cappiello, 2018). Insurance companies must adapt to these changes by integrating innovative technologies into their business models and focusing on maintaining strong relationships with customers.

Despite these risks, insurance companies can capitalize on emerging technologies by developing flexible strategies that address these challenges and enhance their competitiveness. Embracing innovation while maintaining high-quality customer service and operational efficiency will allow companies to remain resilient in a rapidly changing market (Eling & Lehmann, 2018).

Although emerging technologies present significant opportunities for insurance companies, they also introduce new risks that must be managed strategically. Companies that fail to adapt to technological advancements and regulatory changes may struggle to remain competitive, while those that successfully

integrate new technologies will be better positioned to thrive (Cappiello, 2018).

## Insurability of Technological Risks

Technological advancements and the associated risks (Volosovych et al., 2021), along with the civil liability they entail, underscore the necessity for compulsory insurance. These risks are distinct from those related to traditional activities and products, as they stem from complex technological programs and systems. Furthermore, the widespread nature of these risks complicates the task of defining their scope or extent. as the damages can be vast and beyond the capacity of any single party to bear. Therefore, compulsory insurance is the only effective way to ensure protection and adequate compensation for such risks. This form of insurance addresses the specific nature of technological risks, which cannot be handled through ordinary liability coverage. It provides a solution to the substantial financial consequences, ensuring full coverage and safeguarding against potentially catastrophic damages (Al-Sadeeq, 1999: p. 404).

To elaborate on the above, this chapter is divided into two sections. The first section discusses risk management and insurance strategy in the context of technological risks, while the second section examines the insurability of technological risks from both a legal and technical perspective.

## Subsection One: Risk Management and Insurance Strategies in the Context of Technological Risks

Risk is the core element of an insurance contract, as it justifies the existence of the system and the premiums paid by policyholders (Zahra, 2018). Technological and industrial advancements have introduced new risks, especially technological ones, and insurance plays a key role in managing these (Cappiello, 2018). The rapid pace of technological change requires effective strategies to address emerging risks (Al-Shobri, 2016). However, traditional insurance methods often fail to meet the challenges of technological risks. Poor risk management results in higher costs and failures in insurance strategies. The information revolution demands stronger protection of data and a reengineering of processes in the insurance sector to keep pace with these changes (Cappiello, 2018). Insurance companies must adapt by utilizing information technology to manage risks and stay competitive (Ahmed et al., 2024).

The reliance on traditional insurance models remains a major issue, as many companies are slow to adopt modern risk management techniques. There is also an overemphasis on technology as a solution without considering the organizational and cultural shifts needed within insurance companies to embrace these advancements fully.

## The Concept of Digital Transformation and Its Importance in the Insurance Industry

Digital transformation integrates technology across all business operations, changing management, culture, and customer value delivery. In the insurance sector, digital transformation is essential for modernization and competitiveness, driven by technological advancements like AI, IoT, and cloud computing (McKinsey & Company, 2021). These technologies improve risk prediction and operational efficiency, automate processes, reduce costs, and enhance customer experiences (Lissy et al., 2023). By adopting modern technologies, insurance companies can better assess risks, improve management, and deliver enhanced services to customers (Jaafar, 2024).

While digital transformation offers substantial benefits, many companies face significant barriers to implementation, including a lack of sufficient technical

expertise and resistance from staff. The broad definition of "digital transformation" can be too vague, and without clear metrics or strategic direction, it may lead to fragmented or incomplete adoption.

## Challenges Facing Insurance Companies in Light of Digital Transformation

Despite digital transformation's advantages, insurance companies face challenges in adapting to new technologies (Cappiello, 2018). To overcome these, companies must invest in technology and innovate to seize opportunities (Jaafar, 2024). Accordintg to (Jaafar, 2024), Key challenges in today's digital landscape include security and privacy, resistance to change, and rising technology costs. As cyber threats grow, stronger investments in cybersecurity are needed to protect sensitive data and maintain public trust. Resistance to change also poses a significant barrier, as employee pushback and a lack of necessary skills can slow progress. To address this, organizations must foster a culture of innovation, provide adequate training, and create incentives to support transformation. Additionally, high technology costs present a major obstacle, particularly for smaller companies. These organizations often struggle to afford the latest technologies, making it essential to allocate budgets wisely and explore more affordable technology solutions.

While these challenges are valid, the suggested solutions may oversimplify the complexity of these issues. Security, for instance, requires not just investment in technology but also a complete overhaul of organizational culture to embrace cybersecurity at every level. Resistance to change often stems from more than just a lack of training it's also tied to deeper issues like organizational inertia and risk aversion.

## Risk Management Tools

Risk management involves identifying, evaluating, and mitigating threats to organizations. Increasing technological risks require updated strategies to effectively address modern challenges. The key steps in this planning framework include: First, precise planning and scoping to establish objectives and benchmarks. Second, identifying and assessing risks in terms of their likelihood and potential impact. Risk management strategies are then implemented, including techniques such as risk transfer (through insurance), prevention, mitigation, or acceptance, depending on the nature of the threat. Finally, appropriate security controls are implemented, and plans are adjusted based on experience and changes in the technological environment (Al-Shabry, 2016).

Digital transformation enhances risk management by employing technologies like:

– AI: Improves risk prediction and decision-making by analyzing large datasets (reducing time for decisions).

– ML: Machine learning enhances claim assessments and pattern recognition for more flexible insurance options.

– IoT: Collects data on customer behavior, improving insurance solutions based on real-time data (e.g., driving habits).

– Blockchain: Provides security, transparency, and reduced administrative costs (Grima et al., 2020).

– Cloud Computing: Offers scalable, cost-effective data management without the need for physical infrastructure.

– Process Automation: Enhances efficiency by automating processes, improving speed and accuracy (Johansson & Vogelgesang, 2016).

While these technologies offer promising improvements, their implementation in risk management is not without challenges. AI, for

example, is only as good as the data it analyzes, and any biases or gaps in data can lead to inaccurate predictions. Additionally, the integration of multiple technologies, such as IoT and blockchain, can lead to complexity, requiring not just financial investment but also substantial organizational capacity and expertise to make the systems work harmoniously. The promise of "full automation" may also overlook the critical role of human judgment in nuanced risk assessments.

## Discussion

This section discusses the topic of examples of successful insurance companies in applying emerging technologies in a systematic and comparative manner. It presents four cases of major insurance companies (MetLife, Allianz, Lemonade, and Progressive) that have relied on modern technologies such as artificial intelligence, the Internet of Things, blockchain, and big data to enhance their operations and services. The discussion focuses on three main aspects for each company: the technologies used, the results achieved, and the challenges faced. For example, MetLife used artificial intelligence to customize insurance products and improve claims processing, while Allianz turned to the Internet of Things to enhance risk assessment. Lemonade relied entirely on automation and blockchain to offer fully digital insurance services, while Progressive focused on using big data and machine learning to improve pricing strategies:

## Examples of Successful Insurance Companies in Applying Emerging Technologies (Siddiqi, 2021)

### MetLife - Using Artificial Intelligence in Life Insurance

MetLife is one of the largest life insurance companies in the world, and it has successfully integrated artificial intelligence (AI) to enhance its life insurance processes.

### Technologies Used

- Artificial Intelligence (AI): MetLife uses AI to analyze customers' medical and financial data to provide customized insurance solutions. AI is also used to improve the claims process, making it faster and more accurate.

- Virtual Assistants (Chatbots): MetLife also offers customer support through AI-powered virtual assistants (chatbots) that answer questions and provide insurance consultations.

### Results

- Improved Insurance Product Customization: By analyzing data using AI, MetLife was able to offer life insurance products tailored to each client based on their health and financial needs.

- Faster Claims Processing: AI technology helped accelerate the claims processing procedures, enhancing the overall customer experience.

- Reduced Operational Costs: Through automation and process improvements, MetLife was able to reduce operational costs and increase efficiency.

### Challenges

Acceptance Issues: Despite the advantages offered by technology, some customers faced challenges with accepting and feeling comfortable using automated systems.

### Allianz Digital Transformation with IoT and AI.

As one of the largest insurance companies globally, Allianz has significantly benefited from emerging technologies such as (IoT) and Artificial Intelligence (AI) (Finkelstein & Leonard, 2020).

### Technologies Used

- Internet of Things (IoT): Allianz utilized IoT technologies to collect data from connected

devices, such as sensors in cars or smart home appliances. For instance, car sensors are used to monitor driving behavior and improve the risk assessment for car insurance.

- Artificial Intelligence (AI): AI was leveraged to enhance claims evaluation and analyze the data collected from connected devices. Advanced analytics techniques were also applied to offer personalized recommendations to customers regarding their insurance policies.

## Results

- Improved Insurance Personalization: By using IoT data, Allianz was able to offer more personalized insurance products. For example, customers can receive discounts based on their actual driving behavior, helping to reduce costs for them.

- Enhanced Operational Efficiency: AI helped speed up the claims evaluation process, allowing the company to handle claims more quickly, which improves the customer experience.

- Risk Reduction: By using sensors in homes and cars, Allianz can better monitor risks and reduce the likelihood of accidents.

## Challenges

The main challenge was integrating IoT technologies with the existing systems of the insurance company, which required significant investments in upgrading the technological infrastructure.

## Lemonade Insurance - Digital Transformation through Artificial Intelligence

Lemonade is a U.S.-based insurance startup, established in 2015, that has successfully implemented emerging technologies to radically change the way insurance services are offered. Lemonade is considered a model for

using AI to deliver faster and simpler insurance services.

## Technologies Used

- Artificial Intelligence (AI): Lemonade utilizes AI algorithms to analyze customer data and provide personalized insurance offers in record time. For instance, customers can obtain home or life insurance through their app within a few minutes something that used to take much longer with traditional systems.

- Blockchain: Lemonade uses blockchain to facilitate the rapid and transparent processing of insurance claims, ensuring that no manipulation or delays occur in transactions.

## Results

- Improved Customer Experience: Lemonade significantly enhanced customer experience by reducing the time it takes to obtain insurance. Customers no longer need to interact with human insurance agents, as the entire insurance and claims process is automated and fast.

- Cost Reduction: Thanks to automation through AI, Lemonade has managed to reduce operational costs compared to traditional insurance companies.

## Challenges

Despite its successes, Lemonade faces challenges in building trust with customers who may not feel entirely comfortable dealing with AI in the insurance sector.

## Progressive Insurance – Using Big Data to Improve Pricing and Product Customization

Progressive is one of the leading insurance companies in the United States, which has invested in utilizing big data to enhance pricing and customize insurance products

## Technologies Used

- Big Data: Progressive relies on big data analytics to examine customer behavior and

set prices more accurately. For instance, it can analyze data related to traffic patterns, car types, and driving behaviors to offer personalized insurance rates.

- Machine Learning**:** Progressive employs machine learning techniques to improve pricing strategies. Machine learning enables the analysis of patterns and precise risk prediction, allowing the company to offer more flexible and competitive insurance deals.

## Results

- Insurance Customization**:** By leveraging big data, Progressive was able to offer insurance tailored to individual customers based on their actual behavior, rather than just traditional factors like age or gender.

- Improved Pricing**:** With the use of machine learning, the company can now determine more accurate pricing by continuously analyzing data.

- Increased Customer Satisfaction: By personalizing offers and providing fairer and more flexible prices, Progressive has enhanced customer satisfaction and loyalty.

## Challenges

Despite the success with big data, challenges remain in data protection and compliance with privacy regulations.

## The Insurability of Technological Risks from a Legal and Technical Perspective

Liability insurance (has evolved considerably in recent times), which has led to a wider scope of risks being eligible for coverage. This development has given rise to the notion that technological risks may not be significantly different from traditional liability insurance (in terms of their insurability). In other words, it is believed that there are no substantial legal doubts regarding the insurability of technological risks. This is especially true given the rapid technological advancements affecting insurance companies (Reslan, 2013, p. 21). However, in determining the insurability of technological risks within an insurance contract, one must distinguish (between the legal and technical aspects of such risks).

## The Legal Insurability of Technological Risks

The legal insurability of technological risks (refers to whether these risks fulfill the legal conditions required for them to be covered under an insurance contract). This brings up the question: Does the risk meet the legal criteria to be insurable?

Before answering this, it is important to note that (the methods employed by many industrial and nuclear organizations to minimize the risks arising from their operations are insufficient) to fully reduce these risks. As a result, some organizations have opted to transfer the risk to insurance companies, which would guarantee compensation for the damages caused by such risks (Al-Kilani, 2025, p. 270).

In many cases, industrial and nuclear entities have turned to a risk management approach where they (assume the damages caused by their operations) instead of fully covering the risks through insurance. These risks are considered difficult to insure because of their magnitude. This method, known as "risk prevention," involves taking all necessary precautions to reduce the dangers posed by such risks.

Nonetheless, the risk management approach (based on self-insurance or retaining the risk) has proven to be inadequate when dealing with technological risks. This has led to the conclusion that insurance becomes a (necessary measure) to cover these risks, especially after all other methods have failed to sufficiently mitigate the potential damages.

Therefore, the legal insurability of technological risks is determined based on whether they fall under contractual or tortious faults. (Insurance for these risks is valid) whether the damages arise from a contractual fault or a tortious fault, provided that the risk has an element of uncertainty about whether it will occur or not.

Civil liability associated with technological risks has several characteristics that make it insurable, bringing it closer to the field of commercial insurance. The first of these characteristics is objective liability, whereby proof of fault is not required for liability to arise; rather, the occurrence of the damage and its connection to the technological activity are sufficient. Second, this liability is specific, meaning its scope and criteria are clear, making it easier for insurance companies to assess the extent of the risk and estimate potential compensation. The third characteristic is the concentration of liability, as it is often confined to a specific party or entity, which reduces the complexity of allocating liability and helps design appropriate insurance programs. These combined features make civil liability for technological risks a suitable area for insurance intervention as a tool for risk management and compensation. These characteristics, when proven, (make technological risks eligible for insurance from a legal perspective) (Al- Shobri, 2016, p. 277).

The concept of technology is based on the implementation of new human ideas and intentional mental actions. As a result, one might argue that the risks arising from technological activities (are legally uninsurable due to a lack of probability), which is a requirement for an insurable risk. The first issue to consider is whether technological risks (involve an element of probability) or whether the risk is entirely voluntary, which would determine its legal insurability.

In conclusion, the nature of technological risks does not exclude them from having a (probable element), and therefore there is no legal barrier to insuring technological risks unless the risks (are entirely voluntary incidents) (Abd al-Salam, 2018, p. 137).

## Technical Insurability of Technological Risks

Insurance relies on key principles, mainly the aggregation of risks by pooling a large number of policyholders, each paying a premium to cover potential damages. This risk pooling is managed through netting similar risks and applying statistical laws (Zahra, 2018, p. 28).

Technological risks, however, do not meet these principles well due to their rarity and unpredictability. This makes them hard to fit within the statistical framework of insurance. Insuring technological liabilities presents significant technical challenges. Even with data on risk frequency and size, the small number of these risks makes it difficult to pool them, leading to high premiums that may be unaffordable for businesses (Al-Kilani, 2025, p. 270).

Thus, a new type of guarantee is needed, requiring a re-evaluation of traditional insurance principles. Some technological risks may be insurable by adapting existing technical and legal foundations, especially through cooperation and reinsurance strategies (Al-Shobri, 2016, p. 303).

The question remains: Can technological risks be technically insured? The difficulty of predicting their size and frequency has made insurers hesitant to cover them. This type of risk does not align with the traditional concept of risk aggregation (Abd al-Salam, 2018, p. 138).

## Technological Risk and Risk Aggregation

Technological risks are fewer compared to traditional risks, making it harder to aggregate

them for insurance. This might be due to high premiums or the uncertainty around the risk's scale. However, methods like risk segmentation, reinsurance, or setting coverage limits can help achieve necessary homogeneity. Although natural aggregation may not work, non-natural aggregation through legal and insurance systems is possible (Al- Shobri, 2016, p. 307).

## Frequency and Probability Calculation

Estimating the likelihood of a risk occurring is essential for insurers. For technological risks, predicting frequency and compensation is difficult due to their link with new products or activities. However, modern development and legal regulations show that it is possible to estimate risks more accurately (Reslan, 2013, p. 34).

## Technological Risk and the Concept of Diffused Risk

For a risk to be insurable, it must be distributed or diffused. This means that the risk should not materialize for the majority of policyholders or most of them at the same time and to the same degree. In order for risk pooling to succeed, the actual risks that will materialize must be few in comparison to the total number of insured risks. Certain risks, such as earthquakes, war-related risks, or the consequences of economic crises, are too generalized to be insured from a technical standpoint, as they affect large numbers of people simultaneously. In contrast, technological risks do not have this level of generality, which keeps them within the realm of insurability (Zahra, 2018, p. 32).

However, when we look at situations where damages occur due to technological use, we face difficulties in extending insurance coverage. Many technological risks, such as those related to information systems, affect a large number of users, both individuals and corporations, all at once. This creates

challenges in providing coverage. Hence, there is a need to develop insurance systems that can accommodate or adapt to the specific nature of these risks.

Regarding the condition of risk uniformity, technological risks do not present an insurmountable obstacle to coverage. What is needed is some adaptation in terms of the scope of coverage and how to deal with damages that are not entirely uniform. It is believed that uniformity in the source of the damage is sufficient for these risks to be included under a standard insurance cover. (Al- Shobri, 2016, p. 310).

Therefore, technological risks can indeed be insurable from a technical standpoint, but this requires modification, development, and a rethinking of some traditional insurance principles and technical conditions to align with the unique nature of these risks. This has been recognized by insurers in technologically advanced countries.

In conclusion, if insurance plays a significant role in transferring technology to markets and fostering new industries, it is essential to have appropriate methods for evaluating emerging technological risks. This, in turn, calls for the creation of a new insurance market to manage technically complex and high-risk industries.

## Insurance Coverage for Damages Resulting from Cyberattacks

Advancements in information technology have positively impacted the collection and processing of personal data, leading to the creation of information banks that serve specific purposes through electronic data processing (Reed, 2018). However, this has also introduced negative consequences, as new technologies can store, retrieve, and analyze vast amounts of personal data. Artificial intelligence applications now pose significant risks, especially regarding personal data.

Companies face major challenges in maintaining privacy, data protection, and information security (Ahmad, et al, 2018).

In response, insurance companies have introduced cyber insurance, a relatively new product (Joshi & Joshi, 2020). This type of insurance specifically addresses modern technological risks, including those related to personal data processing. Cyber insurance offers coverage for a range of technology-related risks, such as data breaches and cyberattacks (Abu Al-Hassan, 2022, p. 149).

As industrial transactions involving information increase, it has become essential to provide insurance for risks arising from these activities. The insurance industry has responded by offering tailored services to cover risks associated with the use of information and communication technologies (OECD, 2017, p.7). Known as "Cybersecurity Insurance," this type of coverage targets risks like data breaches, operational disruptions, and network corruption (Abu Al-Hassan, 2022, p. 149). Digital transformation is crucial for business improvement, but it also makes companies vulnerable to cyberattacks, which are the leading threat globally (Allianz, 2020). Cyber risks include any electronic incidents that harm data confidentiality or disrupt operations, resulting in significant business impacts (Granato & Polacek, 2019). Cyber insurance has thus become an essential part of corporate risk management strategies.

**Cyber Insurance and Emerging Risks**

Despite the opportunities that emerging technologies offer to insurance companies, big data stands out as one of the most significant advantages. With vast amounts of data available, insurers can enhance risk analysis and pricing accuracy (Cohen & Anderson, 2000). However, risks are also associated with the use of these emerging technologies, particularly security risks such as cyberattacks

that may lead to data loss or theft. For instance, cyberattacks like viruses or malware can disrupt sensitive systems used by insurers to manage clients' personal data, causing substantial financial losses and eroding customer trust. The widespread digital transmission of data has led to security concerns, including eavesdropping, cyber-espionage, and hacking, which facilitate the theft of financial data through sophisticated methods (Gatzert & Schubert, 2022).

Furthermore, laws and regulations play a critical role in managing the use of emerging technologies in the insurance sector. As technology evolves, the need to update legislation to align with modern advancements has grown. Many countries have already developed laws regarding artificial intelligence and data protection, providing a regulatory framework that ensures technology is used ethically, reducing security risks. Insurance companies that adapt well to these regulations can avoid significant legal risks and build customer trust (Peters et al., 2018).

Countries like those in the European Union and Jordan, through their respective laws, have imposed obligations on companies to protect information and personal data (Tikkinen-Piri et al., 2018). Although traditional insurance policies may cover some risks related to information transactions, they do not address the specific complexities of cyber risks such as human errors, cybercrimes, or system failures. Cyber insurance policies generally cover liability and the costs incurred during an electronic event, including breach notifications, recovery expenses, and more (Kent Baker et al., 2021, p. 216).

Cyber insurance services are offered either as standalone products or as additional coverage to traditional insurance services. These policies are not uniform; rather, they consist of a range of services tailored by

insurers for their clients, including financial coverage for compliance with data protection laws (Abu Al-Hassan, 2022). These services are typically included under liability insurance and are essential in addressing the unique technological risks faced by modern industries (Steiner & Maas, 2018; Nicholson, 2019).

Some argue that cooperative insurance could overcome challenges in covering technological risks, including data breaches, by bypassing the traditional principles of commercial insurance. However, the unique legal value of personal data calls for mandatory insurance for data-related risks (Al-Balushi, 2017, p. 229).

## Results

Emerging technologies present both opportunities and challenges for the insurance industry. They offer significant potential for innovation, enhanced efficiency, and improved risk management. However, they also necessitate the implementation of robust systems and strict compliance with legal frameworks to address the security, data privacy, and operational risks they may introduce. These findings were revealed through the study:

Information systems software is one of the newest areas in which civil liability can be established based on the concept of "strict liability." This liability primarily aims to provide guarantees, protection, and compensation for damages resulting from technological activities in the field of information systems software. Liability arising from information systems is not limited to traditional activities or products, but rather relates to complex technological programs and activities. For example, the use of personal data to determine or automate decision-making based on this data is one of the most important applications of artificial intelligence, posing increasing risks to personal data and individual

rights. This use may have serious consequences for the individual concerned, as it may lead to erroneous or biased decisions, harming their rights and interests.

Emerging technologies offer numerous opportunities for insurance companies, particularly through the use of big data. With the availability of vast amounts of data, insurers can enhance the accuracy of risk analysis and pricing, taking into account a wide range of variables. Additionally, technology offers improvements in operational efficiency through process automation, increasing efficiency across all stages of the insurance process, from quoting to claims processing. It also improves customer experience and enables the innovation of insurance products based on customer data and needs. As a result, the insurance sector has undergone significant digital transformations that have impacted operational and competitive dynamics. Emerging technology consists of innovations that are still in development but are expected to have a profound impact across various sectors in the near future. These technologies are not limited to any one sector but impact most sectors, including insurance. They have the potential to radically transform the insurance industry by automating numerous processes and reducing costs.

While emerging technologies offer opportunities for insurance companies, they also pose risks that could impact their sustainability and competitiveness. Security risks are significant, as reliance on new technologies exposes insurers to cyberattacks, which can lead to data loss or theft. Additionally, data and privacy risks arise if systems fail to protect or process information accurately, leading to incorrect insurance decisions and a loss of customer confidence.

The insurance sector is undergoing significant changes in its operations, altering

the scope and concept of insurance. Many companies still rely on traditional methods, leading to poor risk management and unsuccessful strategies. The increasing demand for automation is also driving rapid technological developments in information and communications technology (ICT), such as artificial intelligence, the Internet of Things (IoT), and cloud computing, to drive digital transformation. This makes the adoption of these technologies essential for insurance companies to improve performance, enhance risk management, and ultimately provide better customer service, which in turn enhances financial performance and competitiveness. However, some insurance companies face challenges such as security concerns, resistance to change, and high costs when adopting new technologies. Overcoming these obstacles requires strategic investments in modern technologies to deliver efficient services and maintain competitiveness.

Technological risks are insurable, as long as they do not involve intentional harm. However, traditional insurance models may need to adapt to address these unique risks, a shift already recognized by insurers in developed countries. Data protection liability insurance (cyber insurance) provides coverage for technological risks, including those related to the protection of personal data, ensuring that businesses are covered in the event of a data breach.

Cyberattacks and global threats are among the greatest global threats, as they can compromise data integrity and disrupt operations. These risks are defined as the potential harm caused by cyber incidents, resulting in operational disruptions and physical damage. This has made it necessary to amend regulations and laws related to the use of technology to regulate emerging technologies to ensure ethical use and reduce security risks. This has already prompted countries to develop laws related to artificial

intelligence and data protection, providing a framework for companies to avoid legal risks and enhance customer confidence.

**Recommendations**

– Insurance companies should approach startups with caution by employing specialized and diverse technological expertise while maintaining strong relationships with clients. This requires balancing the use of technology with providing high-quality, personalized services.

– It is essential to establish general guidelines for an effective insurance strategy within a renewed, diverse philosophy, transitioning from traditional management concepts to those addressing the rapid emerging developments. This necessitates the reengineering of processes to align with the current era, ensuring insurance services meet modern demands.

– Modern laws and regulations must be updated to keep pace with this, as specialized insurance companies generate clients and prepare them for emerging technologies. Additionally, risk adjustments are necessary to keep up with rapid technological advancements. It is crucial to ensure that insurance is both technically valuable and effective in addressing future challenges.

– There is a growing need to reevaluate some traditional technical concepts in insurance, leveraging the capabilities offered by modern technology. Personal data protection is essential, requiring mechanisms to safeguard against potential risks and cover technological damage. Given the increasing number of cyber incidents for various reasons, it is vital for companies to adopt advanced, secure technologies and enforce effective data management and protection controls.

– Modern insurance companies should invest in training their employees on technologies such as artificial intelligence and big data analysis to maximize benefits. This also requires fostering a culture of adaptability and continuous learning within the company through technical training and incentivization. Strategic planning should include transitioning from traditional technical solutions to the adoption of open-source digital programs.

## Conclusion

Emerging technologies offer significant opportunities and challenges for the insurance industry. On the positive side, the integration of digital technologies, particularly artificial intelligence, is expected to transform the sector by improving efficiency, risk management, and the development of innovative products. On the other hand, they also pose risks, especially in relation to data security, privacy, and operational integrity, particularly those arising from cyberattacks and data breaches, which insurers must address. The study emphasizes the need for adopting a comprehensive risk management approach. Insurers must adopt flexible technology strategies, invest in robust cybersecurity, and regularly assess their risk exposure. Additionally, it is essential to adapt to evolving regulations concerning data protection and the ethical use of technology. By aligning with these regulations and training their workforce, insurers can protect their operations and maintain customer trust. While emerging technologies offer opportunities for growth and efficiency, they require careful management to mitigate risks. By updating traditional principles and fostering innovation, the insurance industry can thrive in the digital age. This highlights the importance of directing studies toward emerging technologies in the insurance industry and also exploring aspects related to digital transformation in the insurance sector.

## References

- Abdel-Salam, S. S. (2018). *The problem of compensating for technological environmental damage*. Dar Al-Nahda Al-Arabia.

- Abu Al-Hassan, A. A. (2022). *The legal system of digital personal data (Doctoral dissertation, Alexandria University)*.

- Ahmed, S., & Miskon, S. (2020, November). *IoT driven resiliency with artificial intelligence, machine learning, and analytics for digital transformation*. In 2020 International Conference on Decision Aid Sciences and Application (DASA) (pp. 1205–1208). IEEE. https://doi.org/10.1109/DASA49798.2020.9313895

- Ahmed, A. A., Osman, O. S., & Nadi, M. A. Z. (2024). Measuring the impact of information and communication technology on insurance sector performance: An empirical study on Misr Life Insurance Company. *The Scientific Journal of Financial and Commercial Studies, Faculty of Commerce, Damietta University, 5*(2), 4.

- Al-Ahmad, A. A., Omar, M. A., & Hodeib, A. A. (2018). The digital divide as one of the contemporary ethical problems. *Studies Journal, Human and Social Sciences, 45*(2), 61-71.

- Al-Balushi, M. M. K. (2017). *The impact of informatics on data confidentiality* (Doctoral dissertation, Alexandria University).

- Al-Kilani, M. M. (2025). *Insurance contracts from a legal perspective*. Dar Al-Thaqafa for Publishing and Distribution.

- Al-Siddiq, A. A. M. (1999). *Liability insurance and its contemporary compulsory applications: A comparative study between the UAE Civil Transactions Law and Egyptian Law*.

- Al-Shobri, A. S. (2016). *Civil liability for technological risks*. Dar Al-Jamea Al-Jadida.

- Baker, H. K., Nikbakht, E., & Stein Smith, S. (Eds.). (2021). *The Emerald handbook of blockchain for business*. Emerald Group Publishing.

- Botros, A. W. (2015). A conceptual framework for evaluating banking risks: A theoretical study. *The Scientific Journal of Economics and Commerce*, Ain Shams University, 4.

- Cappiello, A. (2018). *Technology and the insurance industry: Re-configuring the competitive landscape*. Springer.

- Czerwińska, T. (2017). *Impact of insurance companies' investment policy on risk management in the public sector*. In Risk management in public administration (pp. 361–388).

- Eckert, C., & Osterrieder, K. (2020). How digitalization affects insurance companies: Overview and use cases of digital technologies. *Zeitschrift für die gesamte Versicherungswissenschaft, 109*(5), 333–360. https://doi.org/10.1007/s12297-020-00248-7

- Eling, M., & Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. *The Geneva Papers on Risk and Insurance-Issues and Practice, 43*, 359–396. https://doi.org/10.1057/s41288-018-0090-5

- Eling, M., Nuessle, D., & Staubli, J. (2022). *The impact of artificial intelligence along the insurance value chain and on the insurability of risks*. The Geneva Papers on Risk and Insurance-Issues and Practice, 47(2), 205–241.

- Finkelstein, A., & Leonard, J. (2020). *The impact of technology on insurance markets*. Springer.

- Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance, 89*(3), 725–763. https://doi.org/10.1111/jori.12329

- Grima, S., Spiteri, J., & Romānova, I. (2020). A STEEP framework analysis of the key factors impacting the use of blockchain technology in the insurance industry. *The Geneva Papers on Risk and Insurance-Issues and Practice, 45*, 398–425. https://doi.org/10.1057/s41288-019-00171-9

- Guzmán Ortiz, C. V., & Navarro Acosta, N. G. (2020). Impact of digital transformation on the individual job performance of insurance companies in Peru. *Journal of Business Research, 34*(1), 15–28.

- Hilkevics, S., & Semakina, V. (2019). The classification and comparison of business ratios analysis methods. *Insights into Regional Development, 1*(1), 47–56.

- Hilkevics, S., & Semakina, V. (2019). The classification and comparison of business ratios analysis methods. *Insights into Regional Development, 1*(1), 48–57. https://doi.org/10.9770/ird.2019.1.1(4)

- Isleem, M. J. (2025). The Use of Artificial Intelligence in Criminal Justice: An Analytical Study in Light of Fair Trial Guarantees. *An-Najah University Journal for Law and Economics*, Received: 3rd Apr. 2025, Accepted: 4th May. 2025, https://journals.najah.edu/journal/anujrle/first-online/article/2490/

- Jaafar, W. A. A. K. A. (2024). The impact of digital transformation on insurance risk management using scenario analysis and stress testing. *Arab Journal of Scientific Publishing, 7*(71), 2024.

- Johansson, S., & Vogelgesang, U. (2016). *Automating the insurance industry*. The McKinsey Quarterly.

- Kadtke, J. B., & Wells, L. (2014). *Policy challenges of accelerating technological change: Security policy and strategy implications of parallel scientific revolutions*. Center for Technology and National Security Policy, National Defense University.

- Lissy, N., Bhuvaneswari, V., & Krupa, M. E. (2023). *Impact of digital transformation in the insurance industry*. Digitalization of the Insurance Sector, 71.

- McKinsey & Company. (2021). *Transforming insurance with artificial intelligence: A roadmap for insurers. McKinsey Insights*.

- Nicholson, J. E. (2019). Challenges for the insurance industry in the future. *Journal of Insurance Regulation, 38*(6).

- OECD. (2017). *Enhancing the role of insurance in cyber risk management*. OECD Publishing.

- Pearson, R. (2002). Growth, crisis, and change in the insurance industry: A retrospect. *Accounting, Business & Financial History, 12*(3), 487–504.

- Pisoni, G. (2021). Going digital: Case study of an Italian insurance company. *Journal of Business Strategy, 42*(2), 106–115. https://doi.org/10.1108/JBS-07-2020-0164

– Pletneva, E., & Zagorska, D. (2024). Digital transformation and the use of artificial intelligence in social insurance and insurance. *Social Economics, (67),* 146–155.

– Raslan, N. I. (2013). *Insurance against pollution risks*. Tanta University.

– Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1), tyz002. https://doi.org/10.1093/cyber/cyz002

– Siddiqi, M. (2021). *Digital insurance: Business innovation in the post-crisis era*. Wiley.

– Soboh, R. (2025). The Suitability of the Theory of Acceptance Declaration for the Conclusion of the Electronic Contract in the Digital Environment. *An-Najah University Journal for Law and Economics, 1*(1), 69-76.
https://doi.org/10.35552/anujrle.1.1.2363

– Stark, J. (2020). *Digital transformation of industry*. Springer International Publishing.

– Steiner, P. H., & Maas, P. (2018). When customers are willing to disclose information in the insurance industry: A multi-group analysis comparing ten countries. *International Journal of Bank Marketing, 36*(6), 1015–1033. https://doi.org/10.1108/IJBM-07-2017-0157

– Taherdoost, H. (2024). *Risk management in R&D projects*. In Innovation Through Research and Development: Strategies for Success (pp. 247–269). Cham: Springer Nature Switzerland.

– Ullah, M. S., Muttakin, M. B., & Khan, A. (2019). Corporate governance and corporate social responsibility disclosures in insurance companies. *International Journal of Accounting & Information Management, 27*(2), 284–300.

– Volosovych, S., Zelenitsa, I., Kondratenko, D., Szymla, W., & Mamchur, R. (2021). Transformation of insurance technologies in the context of a pandemic. *Insurance Markets and Companies, 12*(1), 1–13.

– Wilkinson, D., Christie, A., Tarr, A. A., & Tarr, J. A. (2023). *Big data, artificial intelligence and insurance*. In The Global Insurance Market and Change (pp. 22-46). Informa Law from Routledge.

– Zahra, M. M. (2018). *Insurance contract provisions*. Dar Al-Nahda Al-Arabia.

– Zhang, C., Khan, I., Dagar, V., Saeed, A., & Zafar, M. W. (2022). *Environmental impact of information and communication technology: Unveiling the role of education in developing countries*. Technological Forecasting and Social Change, 178, 121570.