UDC 368.03:004.7
DOI: 10.5937/TokOsig2501069T

***Iva Tošić*[1]**

INSURANCE COMPANIES BUSINESS IN A DIGITAL ENVIRONMENT – WHAT DOES DORA BRING?

REVIEW PAPER

Abstract

The operation of insurance companies offers a range of advantages in a digital environment, such as accelerated transactions, easier access to insurance services, and cost reduction. However, they also carry the risk of ICT (Information and Communication Technology) risks and cyber attacks. In order to overcome the discrepancies in the national legislations of EU member states and the fragmentation of the financial market, the Digital Operational Resilience Act, known as DORA, was adopted.

In this paper, the author aims to highlight the challenges that insurance companies face in a digital environment, the current regulation regarding ICT risk management, and the difficulties that both states and insurers may expect during the implementation of DORA's provisions. It should be noted that this approach also enables the protection of insurance customers, which is the main goal of EU insurance regulation (Solvency II).

Keywords: DORA, digital environment, digital operational resilience, ICT risk, cyber incidents, EIOPA.

I Introduction

Historically, the financial sector has been highly proactive in utilizing information technologies to develop new business models and optimize internal

[1] Assistant professor, Union University, School of Law, E-mail: iva_tosic@hotmail.com; iva.tosic@pravni-fakultet.edu.rs. ORCID ID 0000-0002-9786-0757
Paper receivd: 20.12.2024.
Paper accepted: 21.1.2025.

processes. In recent years, the digital transformation process has accelerated significantly, becoming crucial for the survival of companies operating in the financial market for many reasons. Firstly, customer expectations have evolved, with increasing demand for flexible, personalized services that are instantly accessible anytime and anywhere. Additionally, the economic environment has impacted financial institutions, prompting them to adapt their business models, introduce new services in search of alternative revenue streams, and improve internal efficiency to reduce costs. This approach enhances system capacity while reducing costs.

As a result of this transformation, insurance companies, being part of the financial sector, have become entirely dependent on their technology, which is no longer merely a tool for streamlining operations, but also a key differentiating and competitive factor. On the other hand, despite numerous advantages, the high degree of digitalization increases the risk of cyber incidents. Various other factors contribute to this growing risk, including the complexity of the technological environment of most financial institutions, which makes it challenging for them to maintain an effective control framework and increases their vulnerability.

It is important to note the following: to implement these digital transformation processes and gain access to technological innovations that best support their operations, insurance companies often rely on external service providers and third-party products. Consequently, the resilience and cybersecurity of these third parties, particularly service providers, have become just as critical as the resilience of the insurance companies themselves, as incidents affecting these providers can impact the entire sector.[2]

Although some research suggests that the financial sector is among the best-equipped industries for managing cyber and ICT risks, partly due to stringent regulation and oversight, cyber resilience among market participants remains inconsistent. The financial sector has been a primary target for cyberattacks, prompting regulators and supervisory authorities to recognize the need for mitigating and managing ICT risks while working to enhance the overall resilience and stability of the financial system.[3] However, the security measures and controls implemented within companies, especially smaller ones, are often insufficient for managing the new cyber and ICT risks that have emerged during the COVID-19 pandemic. Therefore, it is not surprising that insurance companies, which are part of a sector with a high concentration of small institutions, have recorded the most significant increase in cyberattacks.[4] The specific nature of cyber threats, typically cross-border

[2] S. Senabre, I. Soto, J. Munera, „Strengthening the Cyber Resilience of the Financial Sector - Developments and Trends", *Financial Stability Review*, 2021, 89-90.

[3] P. S. Krüger, J.P. Brauchle, *The European Union, Cybersecurity, and the Financial Sector: A Primer*, Cyber Policy Initiative Working Paper Series – „Cybersecurity and the Financial System", Carnegie Endowment for International Peace, 2021, 6.

[4] S. Senabre, I. Soto, J. Munera, 90.

and not confined to specific jurisdictions, has led to the internationalization of both cyberattacks and response measures, as well as their global impact (both direct and indirect through the "contagion effect"). In this context, the European Union has become increasingly active in developing legal regulations aimed at creating digital operational resilience for companies.[5] Among the most significant regulatory measures is the NIS 2 Directive,[6] followed by the Digital Operational Resilience Act (DORA),[7] which serves as a *lex specialis* and will become mandatory for all financial sector entities starting in 2025.

II Concept of Digital Operational Resilience

Digital operational resilience refers to a company's ability to build, maintain, and reassess its operational integrity and reliability, ensuring the security of the networks and information systems it uses through the application of ICT services, thereby enabling the continuous provision and quality of financial services. The importance of digital resilience is a natural outcome of advancements in digitalization and two interconnected challenges, cyber and ICT risks.[8] The proposed EU regulation will require insurance companies to establish internal governance and control frameworks capable of ensuring effective and prudent management of ICT risks. Although this obligation will be delegated to a specific function within the insurance company, the management will remain responsible for any shortcomings, given its duty to approve and oversee the management of these risks.[9] DORA aims to introduce a harmonized and comprehensive framework for the digital operational resilience of European financial institutions, explicitly outlining requirements for addressing and mitigating ICT and cyber risks. This is a direct response to the joint recommendations of the European Supervisory Authorities (ESA). The ESA has identified four areas of focus for regulatory development in the near future: first, requirements for ICT security and risk management; second, sector-specific requirements for reporting

[5] P. Pelc, „The Role of Cybersecurity in the Public Sphere – The European Dimension. Financial Institutions", in: *The Role of Cybersecurity in the Public Sphere – The European Dimension* (eds. K. C. Jentkiewicz, I. Hoffman), Maribor, 2022, 60.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[7] Regulation (EU) 2022/2554 of the European Parliament And of The Council Of 14 December 2022 on Digital Operational Resilience For The Financial Sector And Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, *Official Journal of the European Union L333/1* - DORA.

[8] J. R. Martínez Resano, „Digital Resilience and Financial Stability - The Quest For Policy Tools in The Financial Sector", *Revista de Estabilidad Financiera*, 2022, 65.

[9] P. Marano, M. Siri, „Regulating Insurtech in The European Union", *Journal of Financial Transformation,* 2021, 173.

cyber incidents; third, direct oversight and supervision of third-party service providers; and fourth, a framework for testing cyber resilience. DORA regulates all these issues and provides potential responses and solutions to current legal gaps.[10]

III The Operation of Insurance Companies in the Digital Environment

Technological advancements and the development of digital technologies enable insurance companies to improve their operations and enhance customer experience. Digitalization primarily allows for the analysis of vast amounts of data, which becomes crucial for making informed decisions in the insurance sector. By analyzing historical data, insurance companies can assess risks more accurately and tailor policies, thus facilitating the personalization of offerings to customers. Based on user behavior data, it is possible to create customized insurance policies that are tailored to the specific needs of individual clients. Another significant advantage is the optimization of the claims processing procedure, as automating data analysis speeds up the claims processing and reduces the time required to resolve requests. Additionally, the use of AI and digital platforms enables automated processing of claims, decreasing the need for human intervention. AI algorithms can analyze behavioral patterns and identify suspicious activities, thereby reducing the risk of fraud. Most importantly, considering that customer trust in insurance services is central to all activities of insurance companies, this approach facilitates an improvement in customer support. However, while digitalization brings many advantages, it also presents substantial challenges for insurance companies. Given that they handle large volumes of sensitive data, including personal and financial information of their clients, protecting this data from cyberattacks has become a critical priority. Incidents highlight how vulnerable insurance companies are to cyber threats, which can lead to a loss of customer trust and significant financial losses. Therefore, managing ICT risks and cybersecurity represent one of the key responsibilities and objectives in business today. During the process of adapting to changes in business, compliance with numerous and often changing regulations will be required, along with investments in modern IT infrastructure and its maintenance, continuous investment in system upgrades, and employee training. Adjusting to digital transformation necessitates a change in corporate culture, and establishing an innovative and flexible work environment is crucial for the success of digital transformation.

IV Managing ICT Risks in Insurance Companies

The speed at which the IT environment is changing and evolving daily exposes the insurance market and its environment to new risks. Timely risk control

[10] P. S. Krüger, J.P. Brauchle, 4.

measures must be continuously evaluated to ensure they remain effective in identifying and managing the risks these companies face.[11] The Solvency II Directive[12] came into force in 2016 to harmonize insurance regulation within the EU. However, it does not explicitly regulate ICT risks and cybersecurity, but addresses them implicitly as part of operational risks. Article 41 of the Solvency II Directive requires insurance companies to establish an effective management system that allows for the prudent management of business operations. These companies must take reasonable steps to ensure continuity in their activities, including developing contingency plans. Insurance firms „must implement appropriate and proportional systems, resources, and procedures". In accordance with Article 44, as part of the management system, they shall „have in place an effective risk-management system... to identify, measure, monitor, manage, and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies". In this way, the Directive governs the management of all risks to which a company is exposed, without explicitly analyzing ICT risks. Given that European regulations concerning insurance undertakings do not specifically address proper management of ICT and cyber risks, the regulations of member states often differ significantly. While some countries, such as Germany, have specific requirements for ICT security and management in the insurance sector,[13] other countries don't have any regulation on this matter. This points out a strong need for harmonization of European regulations regarding the management and overcoming of these risks.[14]

European supervisory authorities (ESA), as previously mentioned, conclude that the current fragmented regulatory and supervisory landscape can lead to inconsistent practices across Europe and jeopardize fair competition. Therefore, it is proposed that general requirements for managing ICT risks and ensuring cybersecurity should be established in relevant subsectors to create conditions for the secure provision of services. Such harmonization would help promote greater ICT security and cybersecurity. In this regard, the European Insurance and Occupational Pensions Authority (EIOPA) has published Guidelines on Security and Management in the field of Information and Communication Technologies (EIOPA Guidelines).[15] The EIOPA Guidelines cover areas such as ICT risk management, ICT strategy, information security

[11] S. Grima, P. Marano, „Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings", *Risks*, 2021, 2.

[12] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Official Journal of the European Union – Solvency II.

[13] Federal Financial Supervisory Authority (Bafin), „Supervisory Requirements for IT in Insurance Undertakings", 2022.

[14] P. S. Krüger, J.P. Brauchle, 16-17.

[15] European Insurance and Occupational Pensions Authority (EIOPA), *Guidelines on Security and Management in the field of Information and Communication Technologies*, EIOPA-BoS-20/600 – EIOPA Guidelines.

policies and measures, ICT operational security, ICT operations management, change management in ICT, response and recovery plans, etc. They were developed based on the Guidelines of the European Banking Authority (EBA)[16] to ensure consistency among subsectors. These guidelines require the management of the company to ensure that ICT and security risks are appropriately managed through risk management systems and internal control systems. Additionally, the company must ensure that the number of members and their skills (*fit and proper*) are adequate to support the operational needs in the area of ICT, ICT risk management, and security risks on a continuous basis, to ensure the implementation of the ICT strategy.[17] The principle of proportionality also applies here, i.e. the right of companies to apply the EIOPA Guidelines in a manner consistent with the nature, scope, and complexity of the risks to which they are exposed. Insurance undertakings should establish information security training programs for all employees, including board members, to ensure they are equipped to carry out their duties and responsibilities. Furthermore, they should organize and implement periodic security awareness programs on how to handle information security-related risks.[18]

V DORA in Insurance Companies

As previously mentioned, the COVID-19 pandemic and its impact on business operations accelerated digitalization. Facing regulatory fragmentation, the EU decided to introduce DORA. DORA represents a harmonized EU approach to replace what has been termed "uncoordinated national initiatives".[19] The regulation establishes unified requirements regarding the security of network and information systems that support the business processes of financial entities, essential for achieving a high common level of digital operational resilience.[20] With the DORA proposal, the European Commission directly responded to the ESA's recommendations. Recognizing the risks arising from the lack of detailed and comprehensive regulations in this area, the proposal suggests that DORA should have a broad scope, covering almost all financial institutions across all three subsectors.[21] To achieve digital operational

[16] EBA Guidelines on ICT Risk Management and Security Risks, EBA/GL/2019/04 https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880816/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_HR.pdf, 10.07.2024.

[17] EIOPA Guidelines, Guideline 2.

[18] EIOPA Guidelines, Guideline 13.

[19] S. Kourmpetis, „Management of ICT Third Party Risk Under the Digital Operational Resilience Act", *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, Macmillan, 2023, p. 220.

[20] L. Barroso, „Fintechs: Concept, Level Playing Field and the Supervisory Approach", *Fintech Regulation and the Licensing Principle*, 2023, 43.

[21] P. S. Krüger, J. P. Brauchle, p. 22.

resilience, companies are expected to establish and maintain robust ICT systems and tools that minimize the impact of ICT risks; continuously identify all sources of ICT risks; implement protective, preventive, and detective measures; and establish dedicated and comprehensive policies for business continuity, including contingency and recovery plans as an integral part of operational continuity policies. The regulation itself does not impose specific standardization but relies on European and internationally recognized technical standards and best industry practices.

1. Objectives and Importance of DORA

In the EU, DORA enables the harmonization of regulations concerning digital operational resilience.[22] The main goal is to ensure the resilience of the financial sector, particularly in operational terms, to guarantee its technological security, efficient functioning, and rapid recovery from ICT-related breaches and incidents. This ensures the effective and uninterrupted provision of financial services across the EU while maintaining consumer confidence in the market.

This approach enables the consolidation and enhancement of requirements related to ICT risk, which had previously been classified under operational risk in various EU legal acts (including the Solvency II Directive for insurance companies). While these legal frameworks addressed key categories of financial risks (such as credit risk, market risk, liquidity risk, and market conduct risk), they did not comprehensively cover all components of operational resilience at the time of their adoption. Provisions related to operational risks were often based on a traditional quantitative risk management approach, lacking qualitative rules for protection, detection, mitigation, recovery, reporting, and digital testing in case of ICT attacks. By consolidating and updating various rules on ICT risks, all provisions related to digital risks in the financial sector are consistently integrated into a single legislative act. In this way, DORA helps fill legal gaps and eliminate inconsistencies in previous legal acts, including issues related to terminology. It explicitly defines ICT risk, ICT risk management, incident reporting, operational resilience testing, and the monitoring of ICT risks associated with third parties. As a result, it raises awareness of ICT risks and highlights the fact that ICT incidents and inadequate operational resilience can jeopardize the stability of financial entities.[23]

By adopting a unified legislative act regarding digital operational efficiency, financial entities can follow the same approach and rules in managing ICT risks. The proposed provisions will have a significant impact on the cybersecurity measures taken by insurance undertakings, including the introduction of requirements for

[22] J. R. Martínez Resano, 77.
[23] DORA, recital 12.

conducting penetration tests, which will affect their operations.[24] In applying these rules, insurance undertakings should consider their size and overall risk profile, as well as the nature, scope, and complexity of their services, activities, and operations (principle of proportionality). Consistency will contribute to increasing trust in the operations of insurance undertakings and the entire financial sector. Furthermore, it helps preserve stability, which is particularly important at a time when business heavily relies on ICT systems, platforms, and infrastructure, leading to increased digital risk. Adhering to basic "digital hygiene" should help avoid significant costs for the economy by minimizing the impact and costs associated with disruptions in ICT operations.[25]

2. Impact on the Operations of Insurance Companies

Insurance companies, like the rest of the financial sector, will be obliged to implement these provisions, which will require compliance at all levels of the undertaking. In addition to taking all necessary measures at the organizational level to address ICT risks (risk management, incident reporting, testing digital operational resilience, and information sharing), it is particularly significant that the Regulation establishes requirements concerning contractual arrangements with third parties providing ICT services, as well as rules for cooperation between competent authorities and oversight and reporting they carry out. According to the provisions of DORA, insurance companies that are not micro-enterprises will be obliged to establish an independent control function for managing ICT risks and ensure oversight of the implementation of this function, which must be separate from other control functions and internal audit functions in accordance with the "three lines of defense" model or an internal risk management and control model.[26] The independence of this control function is crucial to avoid conflicts of interest. This clearly indicates that, in today's digital business environment, ICT risks are among the primary risks that companies face. The very term control function points out the significance and responsibility that such a function carries. However, regardless of the obligation to establish a dedicated function for managing ICT risks, the responsibility for all duties related to managing these risks rests with the company's management.[27]

In addition to the above, insurance companies will, in accordance with the principle of proportionality, need to establish a function for monitoring contractual arrangements made with ICT service providers or appoint a senior management member for such oversight. In order to regularly evaluate and monitor the ability

[24] P. Pelc, 63.
[25] DORA, recital 13.
[26] DORA, Article 6, Paragraph 4.
[27] P. Marano, M. Siri, 173.

to provide services without negative effects on the digital operational resilience of the insurance company, several key contractual elements should be aligned with ICT service providers. Such alignment needs to cover the minimum areas that are crucial to enable the company to fully monitor the risks it may be exposed to from third parties providing ICT services. This is significant for maintaining the digital resilience of the company, which is directly dependent on the stability, functionality, availability, and security of the ICT services it receives.[28]

It is necessary to take appropriate measures for crisis management and for implementing a strategy for ICT incidents. Insurance companies are expected to implement a comprehensive framework for managing ICT risks as part of the overall risk management system, including strategies, policies, guidelines, procedures, protocols, and applications necessary for comprehensive and adequate protection of all information and ICT resources from harmful impacts of any kind.[29] To be able to overcome these risks, companies will need to establish internal processes for detecting, managing, and reporting ICT-related incidents,[30] as well as programs for reviewing their own digital operational stability. In this way, they will be able to assess readiness, identify weaknesses, deficiencies, or gaps in digital operational stability, and apply corrective measures at early stages.[31] The regulation provides for the full responsibility of the company itself for properly handling incidents and the consequences arising from them, regardless of the provision of relevant feedback or general guidance from supervisory authorities as a measure following the reporting of an incident.[32] Therefore, insurance companies will be obliged to establish measures for risk and security assessment, as well as to adopt strategies for managing ICT risks to be able to respond to the challenges of the digital environment in which they operate today.[33]

2.1. Management of ICT Risks

In the modern digital environment, the management of ICT risks by insurance companies has become crucial for remaining competitive and maintaining the trust of insurance customers. In accordance with the provisions of the Regulation, ICT risk management is carried out through several interconnected phases: risk identification, protection and prevention, detection, response and recovery, learning and development, and communication.

[28] DORA, recital 68.
[29] DORA, Article 6.
[30] DORA, Article 17.
[31] DORA, Article 24.
[32] DORA, Article 22.
[33] T. Ammann, I. Syed, V. Sanchez, „Exploring Operational Resilience in Financial Services – the Effects of DORA on Risk and Regulation in Top 3 Financial Markets", *Computer Law Review International*, 2/2023, 44.

To successfully manage these risks, it is essential for the company to first identify, classify, document, and keep records of all business functions that rely on and utilize ICT. Additionally, it must conduct a risk assessment and identify specific sources of ICT risks, evaluate potential threats and vulnerabilities, and review risk scenarios. Given that the Regulation pays particular attention to risks arising from third parties providing ICT services to the company, it is necessary to identify, document, and maintain records for all processes dependent on these entities. As part of this first phase, it is required to conduct a risk assessment for all obsolete ICT systems at least once a year.[34]

Once the first phase is completed and risks are identified, companies are expected to take all preventive measures against ICT risks. During this phase, the company should monitor and control the security and functioning of ICT systems and the impact of ICT risks on these systems, establish an information security policy, and develop a reliable structure for managing networks and infrastructure. Furthermore, to prevent the occurrence of ICT risks, companies implement management, logical, and physical access controls for ICT assets, authentication mechanisms, documented policies, procedures, and controls for managing ICT changes.[35]

In the third phase, referred to as "detection" by the Regulation, the company must establish mechanisms for the rapid detection of unusual activities, set thresholds for alerts, and criteria for activating and initiating the response process to ICT incidents, including mechanisms for automatic alerting in case of ICT incident outbreaks.[36] Once this phase is completed, the company must be capable of responding to ICT incidents and recovering from them. A significant obligation will be the establishment of a comprehensive business continuity policy in the field of ICT, as well as the introduction of a crisis management function that must be established by companies that are not microenterprises, along with the obligation to provide the supervisory authority, upon request, with an assessment of the annual costs and losses caused by ICT incidents.[37]

After ICT incidents disrupt the operations of an insurance company, it is crucial to gather all information and analyze the company's weaknesses, internet threats, ICT incidents, and attacks, as well as their impact on the company's digital operational efficiency. Insurance companies that are not microenterprises are required to inform the supervisory authority about the changes implemented during the review following ICT incidents. It is determined whether the company acted in accordance with established procedures and whether the measures taken were effective. The company must map the development of ICT risks, analyze the frequency,

[34] DORA, Article 8.
[35] DORA, Article 9.
[36] DORA, Article 10.
[37] DORA, Article 11.

types, scale, and patterns of incidents and attacks, conduct training and awareness programs for staff on ICT security and digital operational resilience, and monitor technological advancements to better understand how these advancements may affect ICT security requirements and digital operational resilience.

The final phase of risk management involves communication, which is achieved by creating communication plans and publicly disclosing at least significant ICT incidents or vulnerabilities to clients, partner financial entities, and the public, depending on the case. Communication policies vary depending on whether they pertain to internal policies or communication with external partners, clients, etc. From this, we see that DORA provides for a comprehensive system for managing ICT risks, which requires companies not only to establish such a system but also to monitor and analyze whether specific measures and policies have been effective. If the opposite is found to be true, the company is expected to continuously improve its ICT risk management system. Given that these risks are constantly evolving, only such an approach can ensure effective management and overcoming the challenges that digital business presents to insurance companies and the entire financial sector.

2.2. Management, Classification, and Reporting of ICT Incidents

DORA stipulates the process for managing and classifying ICT incidents and cyber threats, reporting significant ICT incidents, and *voluntarily notifying* about serious cyber threats.

As part of the ICT incident management process, insurance companies will need to establish a procedure for recording, monitoring, and taking action on all ICT incidents and serious cyber threats while documenting their causes. This includes setting up an early warning system, classifying and categorizing ICT incidents based on severity and impact on critical services, activating roles, responsibilities, and plans for internal and external communication, handling customer complaints, reporting at least significant ICT incidents to senior management, and establishing response mechanisms for ICT incidents.[38]

For the classification of ICT incidents and cyber threats (such as number, impact, duration, spread, data loss, criticality, and economic effect), a draft Regulatory Technical Standards (RTS) has been prepared, which outlines specific criteria for classifying ICT incidents and cyber threats, as well as assessing their significance and severity.[39]

[38] DORA, Article 17.

[39] Draft Regulatory Technical Standards to Further Harmonise ICT Risk Management Tools, Methods, Processes and Policies as Mandated Under Articles 15 and 16(3) of Regulation (EU) 2022/2554, JC 2023 86, 2024, https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf, 25.7.2024.

When it comes to ICT incident reporting, DORA distinguishes between *reporting* of significant ICT incidents and *voluntary notification* of serious cyber threats if the company considers the threat relevant to the financial sector. The reporting and voluntary notification process also involves service users, as insurance companies are required to inform them when an incident affects their financial interests. This aligns with the primary objective set for insurance companies—to protect insurance consumers. For the long-term operations of these companies, it is crucial to maintain a strong business reputation and customer trust, which can only be achieved by keeping them informed about all matters relevant to protecting their interests.

In the case of a serious cyber threat, it is important for the company to notify clients who may be affected and to educate them about appropriate protective measures they may consider implementing.

The reporting that an insurance company conducts in relation to the supervisory authority consists of:

- *an initial notification*;
- *an interimediate repor*t (as soon as the status of the original incident significantly changes or actions related to a significant ICT incident are modified based on newly available information);
- *updated notifications* (as needed, whenever relevant updates on the status arise, as well as upon the explicit request of the supervisory authority);
- *a final report*.

The supervisory authority is obliged to notify EIOPA, which assesses the significance of the ICT incident and, based on its own assessment, further informs the relevant regulators or authorities of the member states to take measures aimed at maintaining the stability of the financial sector.[40] For reporting purposes, the ESA has prepared a joint draft of RTSs that will further define the content and deadlines for reporting and notifications, as well as standard templates, forms, and procedures for reporting significant ICT incidents and notifying about serious cyber threats.[41] Additionally, DORA mandates that the ESA prepare a joint report by January 17, 2025, assessing the feasibility of centralizing reporting on significant incidents by introducing a unified reporting center for major ICT incidents.[42]

[40] DORA, Article 19.

[41] Draft Regulatory Technical Standards on the Content of the Notification and Reports for Major Incidents and Significant Cyber Threats And Determining the Time Limits for Reporting Major Incidents and Draft Implementing Technical Standards on the Standard Forms, Templates and Procedures for Financial Entities to Report a Major Incident and to Notify a Significant Cyber Threat, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf, 20. 7. 2024.

[42] DORA, Article 20.

Notification increases the likelihood of better understanding and identifying the source of the incident, analyzing potential consequences, and seeking assistance. Rapid incident notification can also help other institutions better prepare for similar attacks.[43] This would enable a swift response to ICT incidents across the EU and significantly facilitate ICT incident management, which is of great importance given the increasing frequency of such incidents and their potential to severely disrupt the functioning of the entire financial sector.

2.3. Testing Digital Operational Resilience

In accordance with the provisions of the Regulation, an essential part of the framework for managing ICT risks, incidents, and threats is the development of a digital operational resilience testing program. This encompasses vulnerability assessment and scanning, network security testing, physical security evaluation, compatibility and performance testing, as well as integrated testing. Testing can be conducted by an independent parties external or internal testing. If conducted internally, independence must be ensured to avoid conflicts of interest during the design and execution phases of the testing. Insurance companies are required to conduct ICT system and application testing that support critical or important functions at least once a year.[44] Additionally, companies that are not microenterprises will be obligated to perform advanced ICT system, tool, and process testing based on TLPT (Threat-Led Penetration Testing) every three years (the frequency may be adjusted, either decreased or increased, depending on supervisory authority requirements).[45] Insurance companies must assess which critical and important functions will be included by this testing (functions whose disruption would significantly affect financial results or the company's ability to continuously meet its obligations); the results of this assessment must be confirmed by the supervisory authority, while a summary of the test results will be submitted to a designated central public authority determined by the member states. For conducting advanced testing based on TLPT, only qualified individuals, either within or outside the company, who meet specific requirements and criteria established by DORA may be engaged. Additionally, ESA will define further requirements, standards, and criteria related to TLPT. In this way, DORA prescribes *fit and proper* conditions that the testing executor must fulfill.

[43] D. Clausmeier, „Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)", *International Cybersecurity Law Review,* 4/2023, 85.
[44] DORA, Article 24.
[45] DORA, Article 26.

2.4. Management of ICT Risk Related to Third Parties, Information-Sharing Arrangements, and Supervisory Authorities

DORA puts special focus on managing ICT risk associated with third parties. This is not an entirely new requirement for insurance companies, as they have already had the ability to "outsource" key or important business functions. However, DORA extensively and thoroughly regulates the core principles of effective business management of ICT risks linked to third parties, as well as the supervisory framework for third-party ICT service providers. Since the new provisions on digital operational resilience also apply to these entities, they are at least indirectly affected by the same regulatory requirements as insurance companies. As a result, third-party ICT service providers will be required to adjust their standard contractual terms and services in line with DORA's requirements if they wish to maintain or expand their client base.[46]

DORA regulates the exchange of information among financial entities related to cyber threats, including indicators of compromise, tactics, techniques, and procedures, security alerts, and configuration tools. Insurance companies will be required to notify the supervisory authority about their participation in such information exchange arrangements.

The regulation lists the supervisory bodies for all entities in the financial sector and governs their mutual cooperation, cooperation with the main supervisory body, and the body established under the NIS 2 Directive. It also establishes mechanisms for sharing effective best practice examples and specifies the powers for supervision, investigations, and sanctions necessary to carry out the prescribed tasks, including the authority to impose administrative fines and corrective measures and to publish administrative penalties. In addition, it regulates the obligation to notify the Commission, ESMA, EBA, and EIOPA about laws and regulations that facilitate the implementation of new provisions on digital operational efficiency, the safeguarding of business secrets, and data protection.

Interestingly, while DORA provides for various supervisory and investigative measures, as well as the possibility of imposing sanctions by the supervisory authority to compel the addressees of the new provisions to comply with the legal and regulatory framework, it does not specify explicit monetary fines or other criminal penalties for non-compliance, except for third parties providing ICT services.[47] In this regard, the regulation differs from the General Data Protection Regulation (GDPR)[48]

[46] T. Ammann, I. Syed, V. Sanchez, 44.

[47] DORA, Article 35.

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union L 119/1* – GDPR.

and the NIS-2 Directive.[49] Instead, according to Article 50 of DORA, EU member states are left to determine administrative fines and criminal sanctions for non-compliance with provisions in their national laws. It is currently unclear how EU member states will enforce these provisions, but this approach may lead to inconsistent treatment.[50]

DORA presents a series of challenges for the operations of insurance companies, but those that manage to tackle these challenges will be well-positioned for continuous advancement in an increasingly digital financial and business environment.[51]

VI Conclusion

The operation of insurance companies in a digital environment represents a dynamic and comprehensive process of transformation, encompassing technological innovations, changes in business models, and adaptation to new customer expectations. Digitalization enables insurance companies to enhance efficiency, reduce costs, and improve the customer experience through faster and more personalized services. However, given that such operations involve various risks and that overcoming market fragmentation resulting from differing legislative solutions among member states is necessary, the EU has adopted the Digital Operational Resilience Act (DORA). Generally speaking, DORA represents a significant step forward in improving the digital operational resilience of insurance companies, as well as other financial institutions within the EU. However, it also presents substantial challenges for these companies, including enhancing their operational resilience capabilities, establishing a dedicated control function for managing ICT risks, improving incident reporting capabilities, and developing more sophisticated testing and scenario analysis methods. Additionally, companies will need to make significant investments in staff training, enhancing communication with partners, clients, and supervisory bodies.

To successfully implement the new regulation, insurance companies must take a series of steps. First, they need to invest in IT infrastructure, as only continuous investments in modern and secure IT infrastructure can ensure a successful digital transformation. Furthermore, it is necessary to conduct employee training to enable a better understanding and application of security measures and procedures. Additionally, the implementation of the regulation can be facilitated by collaborating with and engaging external experts, which will also help identify and eliminate vulnerabilities in security systems. Regular resilience testing and incident simulations will enable better preparedness for real threats.

[49] Where monetary fines are prescribed up to a maximum of €20,000,000 or 4% of total annual revenue in the previous financial year.

[50] T. Ammann, I. Syed, V. Sanchez, 45.

[51] P. Gusiv, Development of a Compliance Gap Analysis Method For The Digital Operational Resilience Act (DORA), master rad, Lapland University of Applied Sciences, 2023, 29.

Insurance companies that successfully integrate digital technologies into their operations have the potential to significantly enhance their competitiveness in the market, providing higher quality and more efficient services to their clients. The digital environment not only transforms the way they operate but also opens up new opportunities for innovation and growth within the insurance industry. In this regard, the existence of detailed regulation for ensuring digital operational resilience will be of particular importance to them.

Literature

- Ammann, T., Syed, I., Sanchez, V., „Exploring Operational Resilience in Financial Services – the Effects of DORA on Risk and Regulation in Top 3 Financial Markets", *Computer Law Review International*, 2/2023, 43-48.
- Barroso, L., „Fintechs: Concept, Level Playing Field and the Supervisory Approach", *Fintech Regulation and the Licensing Principle*, 2023, 25-44.
- Clausmeier, D.,„Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)", *International Cybersecurity Law Review,* 4/2023, 79-90.
- Draft Regulatory Technical Standards on the Content of the Notification and Reports for Major Incidents and Significant Cyber Threats and Determining the Time Limits for Reporting Major Incidents and Draft Implementing Technical Standards on the Standard Forms, Templates and Procedures for Financial Entities to Report a Major Incident and to Notify a Significant Cyber Threat, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_ _Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf, accessed: 20.07.2024.
- Draft Regulatory Technical Standards to Further Harmonise ICT Risk Management Tools, Methods, Processes and Policies as Mandated Under Articles 15 And 16(3) of Regulation (EU) 2022/2554, JC 2023 86, 2024, https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf, accessed: 25.07.2024.
- European Insurance and Occupational Pensions Authority (EIOPA), *Smernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija,* EIOPA-BoS-20/600 – EIOPA Smernice.
- Federal Financial Supervisory Authority (Bafin), „Supervisory Requirements for IT in Insurance Undertakings", 2022.
- Grima, S., Marano, P., „Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings", *Risks*, 2021, 1-12.

- Gusiv, P., Development of a Compliance Gap Analysis Method For the Digital Operational Resilience Act (DORA), master rad, Lapland University of Applied Sciences, 2023.
- Kourmpetis, S., „Management of ICT Third Party Risk Under the Digital Operational Resilience Act", *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, Palgrave Macmillan, 2023.
- Krüger, P. S., Brauchle, J.P., *The European Union, Cybersecurity, and the Financial Sector: A Primer*, Cyber Policy Initiative Working Paper Series – „Cybersecurity and the Financial System", Carnegie Endowment for International Peace , 2021.
- Marano, P., Siri, M., „Regulating Insurtech in The European Union", *Journal of Financial Transformation,* 2021, 166-177.
- Martínez Resano, J. R., „Digital Resilience and Financial Stability – the Quest for Policy Tools in the Financial Sector", *Revista de Estabilidad Financiera*, 2022, 59-88.
- Pelc, P., „The Role of Cybersecurity in the Public Sphere - the European Dimension. Financial Institutions", in: *The Role of Cybersecurity in the Public Sphere – The European Dimension* (eds. K. C. Jentkiewicz, I. Hoffman), Maribor, 2022, 59-69.
- Senabre, S., Soto, I. Munera, J., „Strengthening the Cyber Resilience of the Financial Sector - Developments and Trends", Financial Stability Review, 2021, 86-102.
- *Smernice EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima*, EBA/GL/2019/04, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880816/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_HR.pdf, accessed: 10.07.2024.

Translated by: ***Tijana Đekić***