ESJ Humanities Peer-reviewed

The key role of the most recent EU regulation – the "Digital Operational Resilence Act" in the legal system, contemporary challenges, and Georgian perspectives[1]

Magda Ositashvili
LL.M at University of Hamburg
European Master in Law and Economics
University of Pompeu Fabra, Barcelona

Doi:10.19044/esj.2024.v20n26p1

Submitted: 19 August 2024
Accepted: 20 September 2024
Published: 30 September 2024

Cite As:
Ositashvili M. (2024). *The key role of the most recent EU regulation – the "Digital Operational Resilence Act" in the legal system, contemporary challenges, and Georgian perspectives.* European Scientific Journal, ESJ, 20 (26), 1.
https://doi.org/10.19044/esj.2024.v20n26p1

Abstract

The challenges of the modern world, such as globalization, digitalization, and other technological advances, have exposed all fields of science, including economics and law, to severe trials. The bold and visionary attempt of legislative bodies in various countries, to evaluate the advantages and disadvantages of existing regulations and consider new ones was complemented by the development of methods and mechanisms to oversee, regulate, and incorporate the latest technological advancements into the legal framework. After ineffective efforts to deal with various objections, the European Union adopted a new regulation called the "Digital Operational Resilience Act." This regulation aims to address the challenges presented by the increasing cybersecurity threats, operational resilience, and digitalization in the financial sector, both ex-ante and ex-post. In this paper, you will learn about the role of "DORA" in the legal system, the economic analysis of the law, the challenges it faces in the European Union, and the perspectives of the Georgian reality. This paper will employ qualitative and theoretical research methods, focusing on the in-depth analysis of existing legal frameworks and

[1] This article is dedicated to the memory of the Ecuadorian Lawyer and Activist Mikaella Andrade Rodriguez

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

expert perspectives. These methods will allow for a comprehensive understanding of DORA's implications in both the European Union and the Georgian context, offering valuable insights into its potential effectiveness and challenges.

Keywords: Legal regulation, financial sector, digital law, EU regulation, legal sustainability

1. Introduction

1.1. The purpose of creating "DORA"

The main purpose of creating the "Digital Operational Resilience Act" is to enhance **cyber-security and operational resilience within the financial sector** across the European Union. Given the circumstances and key factors, the creation of this act was inevitably necessary.

On the one hand, the financial sector has been significantly enhanced by digital technologies to date, creating a fertile ground for cyber threats like hacking attacks, data loss, and system failures. The efforts of the financial institutions, despite putting a lot of resources into preventing such failures from happening again, were not sufficient. The mentioned threats hindered not only individuals but also posed a significant obstacle to the overall economy and the integration of financial institutions. Therefore, ensuring operational resilience to maintain financial stability and protect consumers was of paramount importance (Cuel R., Ponte D. & Virili F., 2022).

On the other hand, the European Union has lacked regulatory mechanisms until today that could effectively address obstacles. Despite numerous countries having already set up regulations and standards for cybersecurity, these measures were deemed inadequate due to their lack of comprehensiveness and various shortcomings. That is why, first of all, the purpose of "DORA" was formed in a way that it should harmonize similar regulations with comprehensive and consistent mechanisms for all financial institutions that the European Union follows. Namely, this harmonization helps organizations establish conditions that require all financial institutions to adhere to the same high standards (Devezas T., Leitao J. & Sarygulov A., 2021).

Thirdly, there has been a notable rise in the frequency and intensity of cyber attacks recently. The financial sector, holding valuable data and substantial financial resources, is a key target for cybercriminals. Hence, "DORA" focuses on creating and executing efficient plans. These plans require institutions to implement stringent security measures, perform routine risk assessments, and establish a clear incident response strategy. The goal of imposing these regulations is to minimize the risks of cyber-attacks and regulate the financial sector (Onetrust, 2024).

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Additionally, "DORA" also highlights the importance of third-party risk management. Financial institutions frequently depend on third-party service providers for both risk management and overseeing other IT functions. These third parties are vulnerable subjects, as they are not properly monitored and regulated. Therefore, the "Digital Operational Resilience Act" strongly requires all financial institutions to maintain effective control and supervision over their third-party providers to guarantee high-security standards (Schröder M. & Hartl K., 2024).

To put it in a nutshell and follow chronologically, the European Union published “DORA” in 2020, as a package of measures to further digitalize the financial sector. During that period, preparatory work on amending national legislation was conducted in EU countries, including Germany. In 2021-22, the European Parliament published a report on the Mandates of Trilogue Negotiations. The negotiation occurred between the Council of the European Union, the Commission, and the European Parliament. As a result, in 2023, the regulation officially entered into force, marking a significant milestone in the development of the digital economy and law.

1.2. The relevance of the topic

In today’s context, the “Digital Operational Resilience Act” remains a highly relevant topic for several reasons. It should be noted that the rapid development of the financial sector in the digital realm is reaching its peak, which is based on digital services, fintech, cloud-based controlling, data technology analysis, and digital control. These events undoubtedly bring many benefits to the financial market, but they also introduce new risks and additional security concerns (Onetrust, 2024).

Dora's thorough approach ensures that the financial sector, despite its rapid evolution, stays strong and secure against threats. Additionally, in today's geopolitical environment, cyber-attacks and other forms of cyber-warfare are increasing. Financial institutions, due to their economic significance, are often targeted by such attacks. With Dora's requirements, they will maintain the ability to quickly and effectively respond to such threats through continuous monitoring, incident logging, and cooperation with regulatory authorities (PWC 2024).

The increasing importance of data privacy and protection also highlights the need for “DORA”. Financial institutions today handle highly sensitive personal and financial information. Any potential breach could have severe consequences for both individuals and the broader economy. The strict cybersecurity requirements of the mentioned act help protect this data, ensuring that financial institutions maintain consumer trust and comply with broad data protection regulations such as GDPR (General Data Protection Regulation) (Milkau U., 2022).

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

In short, it was essential to create "DORA" in a new era to address the growing digital threats faced by the financial sector, harmonize regulatory standards across the European Union, and enhance the overall operational resilience of financial institutions.

Its relevance today is emphasized by the ongoing digital transformation of the financial sector, the growth of cyber threats, and the critically high importance of data protection (DoRA, 2024).

2. The Digital Operational Sustainability Act and the legal system

2.1. The relation of "DORA" to the legal system

Although, as mentioned in the previous chapter, the "Digital Operational Resilience Act," regulation of the European Union, primarily aims to enhance the digital resilience of the financial sector, it also has several direct and clear connections with the legal system (PWC, 2024).

We can highlight six fundamental topics that make "DORA" an extraordinary legal precedent. These include regulatory compliance, legal enforcement, contractual obligations, incident reporting and legal consequences, data protection and privacy, as well as cross-border legal issues (Pattison A., 2024).

Regulatory Compliance: As mentioned above, "DORA" imposes legal obligations on financial entities to ensure their operational resilience. It is worth noting, that aligning the practices of financial institutions with these legal standards will serve as the foundation for imposing legal responsibilities. Failure to meet obligations can lead to legal consequences, such as fines and other regulatory measures (Cuel R., Ponte D. & Virili F. 2024).

For example, in a 2018 incident known as the "Facebook and Cambridge Analytica scandal", Cambridge Analytica acquired the personal data of millions of users from the social network. This data was then utilized for political marketing without the users' consent. This incident raised several questions regarding the protection of personal data. Already in 2019, it was reported that the proceedings were over and Facebook was fined 5 billion dollars (EsmaEU, 2024).

How could the "Digital Operational Resilience Act" have prevented the scandal?! "DORA" includes strict reservations and requirements that control how much personal data can be collected, accessed, and shared. Therefore, this regulation prevents future violations even in an ex-ante circumstance (Husovec M., 2024).

Legal Enforcement: In the EU, there are authorities like the NCA that oversee institutions' compliance with "DORA". These authorities have the power to enforce regulations as well as conduct audits and impose sanctions. It is obvious that enforcement mechanisms are crucial in the legal system to ensure that financial institutions adhere to regulatory rules (Press L., 2023).

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

In 2020, a Russian government-backed group initiated a significant cyber-attack that infiltrated numerous organizations worldwide, including various sectors of the United States federal government, leading to a prolonged series of electronic data breaches. The mentioned cyber-attack was rated as one of the biggest cyber incidents that ever happened in the USA. Within days of the discovery of the precedent, around 200 organizations worldwide were also affected, including NATO, the UK government, the European Parliament, and Microsoft departments.

"DORA" emphasizes the importance of creating a secure software plan and ensuring the security of the supply chain. This approach helps reduce the risk of attacks by enforcing strict security standards and conducting regular audits. With the above example, we can see that the role of digital operations in law and the economy is significant. Their instability and lack of sustainability result in significant financial losses, impacting not only the European Union but also other continents.

Contracts: "DORA" also impacts financial institutions and their third-party service providers. This means that the parties must ensure the long-term sustainability of obligations arising from specific contract provisions and protect their claims and rights. This legal aspect involves the "DORA" standards as a legal framework during the drafting and negotiation of relevant agreements (Tagarev T. &Stoianov N., 2020).

Disclosure of incidents and their legal consequences: "DORA" stipulates that financial institutions must report important ICT-related incidents to the appropriate authorities. This process, of course, may have some legal consequences. The report must be precise, delivered on time, and follow the format specified by the regulation.

Failure to report or misreporting incidents may lead to legal action and fines. It should be noted that the European Union has consolidated the "Whistleblower Protection Act." The objectives of this act were mentioned in other European Union regulations as early as 1996-1997. However, for some countries, the protection of whistleblowers' rights is still a new concept. For instance, the German government only managed to adopt this law in 2023, known as the "*Hinweisgeberschutzgesetz"*.

Data Protection and Privacy: Financial institutions must ensure that their operational resilience measures align with data protection requirements. This connection establishes a legal relationship between "DORA" and data protection regulations.

Cross-border Legal Issues: Finally, it should be noted that due to the cross-border nature of many financial services and ICT services, "DORA" also takes into account the importance of cooperation and sharing information among different jurisdictions. This may include, on the one hand, complex

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

legal issues directly related to jurisdiction, as well as data transfer and regulatory coordination (Schröder M. & Hartl K., 2024).

To summarise, although "DORA" primarily serves as a regulatory mechanism focused on ensuring the digital sustainability of the financial sector, it is closely linked to the legal system in terms of its requirements, enforcement mechanisms, contractual obligations, incident reporting, and intersections with other legal sources.

3. Economic analysis of sustainable development of digital operations

In the modern era, digital operations have become the primary driving force behind economic activity, encompassing various processes such as financial transactions, demand-supply chain management, and interactions between producers and customers (Matos F., Selig P. & Henriqson E., 2023). As organizations rely more on digital technologies, ensuring the sustainable development of these operations has become a crucial economic concern (Husovec M., 2024).

In this section, we will examine how the quality of digital operations resilience can affect the economy and explore how the EU "Digital Operational Resilience Act" can help reduce the economic consequences of major operational failures.

3.1. The economic value of sustainability in digital operations

The resilience of digital operations refers to an organization's ability to prevent, respond to, and adapt to adverse digital events such as cyber-attacks, system failures, or data breaches. It should be noted that the economic significance of the durability and sustainability of digital operations must be emphasized due to several factors. First, operational disruptions can cause significant financial losses due to business interruption, loss of revenue, and costs associated with restoration and remediation (Stephan L., Rupprecht S. & Tamdjidi C., 2024). For instance, a cyber-attack that disrupts a company's systems can lead to millions of dollars in lost revenue. This includes expenses related to restoring services and enhancing security measures to avoid potential future cyber-attacks (Bafin, 2024).

Second, maintaining consumer confidence plays a critical role in the digital economy. An incident like a data breach can significantly reduce consumer trust, resulting in long-term damage to reputation and a loss of customers. When customers believe that a company is unable to safeguard their personal information, they are more inclined to switch to other providers (Priller M., 2024). This can impact the company's market share and profitability. Furthermore, ensuring market stability is especially crucial in the

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

financial sector, as operational disruptions can lead to systemic consequences (Cuel R., Ponte D. & Virili F., 2022).

A failure in one institution can quickly spread to others, causing a chain reaction and potentially destabilizing markets and threatening economic stability. This relationship between digital technologies and financial sustainability is a vital aspect of the 21st-century economy (Esma, 2024).

Regulations concerning digital operations, their extent, and legal concerns are crucial for the overall sustainable development of the economy. Today, we observe a global trend where organizations in developing countries face challenges in sustaining their digital operations, despite the growing implementation of regulations (Devezas T., Leitao J. & Sarygulov A., 2021).

In Article 13 of the Regulation on the **"Digital Operational Resilience Act",** it is stated that financial institutions should adhere to consistent standards and rules as they would in the context of risk assessment for "Information and communication technology". When working to strengthen and maintain the stability of the financial system, the platforms and overall infrastructure face increased digital risks. Maintaining basic cyber order will help reduce economic disruptions and costs, thus contributing to economic stability by minimizing impacts and expenses (Matos F., Selig P. & Henriqson E., 2023).

In recent years, the risks linked to information and communication technology have become very prominent. International and national organizations, legislators, regulators, and legal structures have set minimum standards to uphold financial stability in the global economy after significant efforts.

According to the words of **the famous economist Jean Baptiste Say, "Supply itself creates demand."** Financial institutions depend on ICT services to fulfill customer needs and expand their operations, striving to adjust to the changing and competitive global economy. To meet customer demands and expand their business, financial entities rely on using "ICT" services to adapt to the evolving and competitive global economy. The scope and objectives of such attitudes have been constantly evolving in recent years. This process leads to a reduction in financial costs, enabling businesses to expand and increase the range of financial activities (Milkau U., 2022).

In conclusion, the sustainability of digital operations is of great economic importance in today's interconnected world. Operational interruptions can lead to substantial financial losses, breach consumer rights and trust, destabilize capital markets, and prompt legal sanctions. The “Digital Operational Resilience Act” (DORA) establishes a detailed framework to enhance the resilience of digital operations in the financial sector. It emphasizes managing risks, reporting incidents, and overseeing third-party entities. By implementing provisions outlined in the “Digital Operational

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Resilience Act" (Dora), financial institutions can enhance their management of risks associated with digital operations. This helps reduce the economic impact of disruptions, ensuring the stability and integrity of the financial system, which significantly influences overall economic outcomes.

4. The economic analysis of the law

The relationship between economics and law as distinct fields, especially the study of how legal frameworks and regulations impact economic behavior and outcomes, has been a significant research focus for a long time. In the realm of digital operations, this interaction becomes even more crucial, as digital technologies now cover almost every aspect of economic activity. The "Digital Operational Resilience Act" (DORA) is a crucial piece of legislation aimed at enhancing the resilience of digital operations in the financial sector. In this part, we will discuss the economic analysis of the EU regulation mentioned above and conclude with how the "Digital Operational Resilience Act" can minimize economic disruptions and promote economic stability.

4.1. The economic importance of legal frameworks in digital operations

Legal regulations play a major role in shaping an efficient economic environment by setting up rules and standards that govern economic behavior. In the field of digital operations, laws and regulations ensure that organizations maintain stringent cybersecurity measures, protect sensitive data, and effectively manage risks. The economic importance of the "Digital Operational Resilience Act" can be understood clearly through several key points (DoRa-Info, 2024).

First, legal frameworks in the economy reduce uncertainty and transaction costs. When legal norms clearly define obligations and expectations, organizations can more effectively allocate resources and plan their business activities. For instance, regulations mandating financial institutions to perform routine cybersecurity assessments and implement robust data protection measures assist companies in preventing the substantial expenses linked to data breaches and cyberattacks. By providing a clear legal framework, "DORA" helps financial institutions understand their responsibilities, thereby reducing the uncertainty and costs associated with risk management (Devezas T., Leitao J. & Sarygulov A., 2021).

Second, the legal framework plays a crucial role in **facilitating the internalization of external factors.** This means that negative impacts on the digital domain, such as data breaches and cyber-attacks, can have extensive economic consequences that go beyond the affected organization. (Stephan L., Rupprecht S. & Tamdjidi C., 2024) The "Digital Operational Resilience Act"

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

encourages companies to take measures to accurately internalize the costs of potential damage. In the future, this process will encourage financial institutions to invest in cybersecurity and sustainable infrastructure. These investments will impact not only individual digital operations but also enhance the overall stability and security of the digital economy (Onetrust, 2024).

Third, legal frameworks are a guarantee of market stability and a high level of consumer confidence. Operational disruptions in the financial sector can lead to systemic risks that have the potential to destabilize markets. In this context, "DORA" ensures that financial institutions can better handle disruptions by establishing requirements that enhance market stability and consumer confidence. These aspects are vital for the smooth functioning of financial markets and the wider economy (Press L., 2023).

"DORA's" focus on thorough risk management practices holds economic importance. "DORA" provisions on third-party risk management relate to economic risks associated with outsourcing and reliance on vendors.

As mentioned, financial institutions are increasingly relying on third-party providers for various digital services, which introduces additional risks and potential vulnerabilities. By mandating comprehensive research, ongoing supervision, and robust contractual commitments regarding data protection and cybersecurity, "DORA" guarantees the efficient handling of risks associated with third parties. This not only protects individual business entities but also reduces the systemic risks posed by interconnected digital ecosystems. From an economic perspective, this results in a more sustainable and reliable financial sector, boosting confidence and stability in the market.

For instance, during the development of "DORA," major companies like KPMG, Deloitte, EY, and PWC, known as the "Big Four," carried out research. This research helped pinpoint several critical issues that required significant changes in the company's policies, to meet "DORA's" specific needs in the right sequence. In this market experience research, it was evident that nearly every issue was of high critical importance. The issue of developing a digital sustainability strategy (in line with Article 6 of "DORA"), accountability, "Patch" strategy (Articles 5, 9), crisis management, reviewing crisis recovery plans, and detection mechanisms (Articles 10 and 11). According to the research above, it was found that the peak criticality value was exceptionally high for two issues, based on the "DORA" conformity index. In particular, regarding the departure from the current strategy and the sustainability testing system, which did not completely align with Articles 25 and 28 of the "Digital Operational Sustainability Act."

What did the insurance companies do? They developed a three-phase system of "DORA" analysis. This system focuses on ensuring thoroughness, clarity, and transparency in the corporate culture of firms, consolidating them into a single framework.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

First, the action started with seminars. The management teams of the companies summarized and presented the basic context of the "Digital Operational Sustainability Act" to the employees for their future actions. Following best practices, requirements were defined to ensure that stakeholders had a clear understanding of regulatory expectations. This initial phase also involved identifying the companies' current operational sustainability status at a high level. In order to support the analysis with actual data and statistics, relevant documentation was requested, and the "triage" was conducted. It should be mentioned that this systematic approach ensured that all parties involved in the process understood the main content of "DORA" well. This laid a solid foundation for analyzing and planning future projects and procedures in detail.

The second phase involved conducting a set number of surveys and interviews in different departments of the companies, such as risk, outsourcing, business continuity management (BCM), IT service continuity management (ITSCM), and resilience testing. These surveys proved to be crucial in clarifying important issues and discussing measures at a high level. Through these discussions, the companies were able to gather detailed information on current practices and potential areas for improvement. It should be noted that, during this design phase, companies were able to explore specific details that provided a comprehensive understanding of their corporate culture's operational sustainability landscape. The information obtained from the surveys mentioned above was crucial in shaping future recommendations.

The third strategy of the above design was the closing meetings, where the conclusions and recommended actions were presented by the companies, the current situation analysis was shown, and the gap analysis was conducted. They highlighted areas where they particularly needed to align with "DORA's" mandates. A high-level gap analysis identified the required actions to enhance the operational sustainability of corporations. This was based on strategically determining relevant information. That is why all stakeholders have been supported in the process of analyzing plans of common importance and taking clear steps.

This design, created by insurance companies, effectively manages compliance by analyzing regulatory requirements and developing strategies to achieve significant results. This aspect is crucial in the economic analysis of law.

In conclusion, the economic analysis of law in the context of digital operations emphasizes the crucial role that legal frameworks play in improving economic outcomes. "The Digital Operational Resilience Act" (DORA) provides a comprehensive legal framework that addresses the specific challenges of digital operations in the financial sector. By focusing on

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

risk management, incident reporting, and third-party oversight, "DORA" reduces economic inefficiencies, internalizes external factors, and enhances market stability. Implementing "DORA" provisions helps financial institutions manage risk more effectively, reduce the economic impact of disruptions, and ensure a stable and resilient digital economy.

5. Perspectives of the "Digital Operational Sustainability Act" in Georgia and the European Union

As stated, many times, the "Digital Operational Resilience Act" ("DORA"), consolidated by the EU, represents an important step towards increasing the sustainability of digital operations in the financial sector (Müller-Terpitz K., 2024). As digital technologies become more essential in economic activities, the importance of robust legal frameworks to guarantee the stability and security of these operations is now more critical than ever! In this section, we will assess the potential of "DORA" in both the EU and Georgia. We will explore how this law could improve digital resilience, strengthen economic stability, and increase confidence in digital financial services. (PWC, 2024)

5.1. Perspectives of "DORA" in the European Union

In the European Union, "DORA" plays a crucial role in enhancing the digital sustainability of financial institutions. The legislation's emphasis on thorough risk management, precise incident reporting, third-party service providers, and robust oversight aligns with the EU's extensive regulatory framework designed to safeguard financial stability and consumers (Milkau U., 2022).

First, it should be noted that "DORA's" comprehensive risk management requirements will significantly enhance the EU's ability to prevent and mitigate digital disruptions. The basis for this is the requirement for financial institutions to regularly evaluate risks and continuously monitor their digital environment. This proactive approach will not only reduce the likelihood of cyber incidents but also reduce their impact if they do occur, ensuring the continuity of financial services and protecting the wider economic system. (DORA-info, 2024)

Second, the incident reporting mandates of "DORA" will boost transparency and improve the coordinated response of EU countries to digital threats. By requiring prompt notification of significant incidents, "DORA" ensures that regulators have timely information to address emerging risks (Pattison A., 2024). This facilitates improved coordination and quicker action, leading to shorter durations and less severe disruptions. Enhanced incident reporting also helps build a detailed database that regulators can utilize to spot

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

trends and implement proactive measures to enhance the overall resilience of the financial sector.

Furthermore, the provisions in the "DORA" regarding third-party risk management are especially important within the context of the EU's circular digital economy. Financial institutions often depend on third-party service providers for essential functions like cloud-based accountability and data processing (Pattison A., 2024).

5.2. What should we expect in the near future?

Several critical milestones and regulatory developments are on the horizon, along with the implementation phases of the "Digital Operational Resilience Act." It is also interesting to see what are the specific terms and what we can expect in the next two years.

As we know, in January 2023, the "DORA" regulation officially entered into force, marking the start of a comprehensive "journey" towards digital operational sustainability. In a relatively later period, in January 2024 as well, detailed specifications known as "Regulatory Technical Standards" (RTS) were issued to address some fundamental issues. It also includes enhanced risk management tools, methods, processes, and policies that serve as an excellent guide for incident classification and cyber threat identification. This encompasses standard incident reporting templates and processes for third-party service providers to uphold a comprehensive information registry. Moreover, specific requirements have been established for contracts that support and include critical and important functions of third parties (Esma, 2024).

We should probably wait until July 2024 for the release of another part of RTS. These standards are expected to include specific content requirements for annual cost and loss assessments, reporting incidents, and deadlines for submitting these reports. The standards mentioned above will focus on evaluating tools, systems, and processes based on the quality of supervision, the removal of critical inconsistencies, and the harmonization of supervision activities (Müller-Terpitz K 2024).

By January 17, 2025, the regulation will be fully implemented. This means that organizations must be willing to ensure full compliance with all aspects of "DORA," integrating all of the requirements into their operational frameworks. By the beginning of 2025, we should anticipate the start of monitoring by authorities to ensure compliance and the effective implementation of sustainability measures (D-o-r-a, 2024).

In the outlook for 2024 and 2025, organizations must already be proactive in adapting to these regulatory changes. This period involves a thorough process of preparation, which includes improving risk management practices, conducting comprehensive tests on resilience measures, and setting

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

up oversight mechanisms. By anticipating these events, organizations can not only guarantee compliance with the "Digital Operational Resilience Act" but also enhance their digital operational resilience to defend against cyber threats effectively and manage operational risks efficiently.

The "journey" through the process of full compliance with "DORA" is difficult, but extremely necessary. By understanding and anticipating these important milestones, organizations can confidently navigate through the regulatory landscape to ensure they are effectively prepared to meet the demands of a rapidly developing digital environment (Tagarev T. & Stoianov N., 2020).

Finally, considering the provisions of the "Digital Operational Sustainability Act" will significantly enhance consumer confidence in digital financial services. By maintaining high standards of cybersecurity and operational resilience, "DORA" ensures that consumers have greater confidence in the security of their data and assets. This will promote more use of digital financial services and drive innovation and economic growth in the EU.

5.3. Perspectives of Georgia

For Georgia, adopting a legislative regulation like "DORA" presents a significant opportunity to enhance the country's digital resilience and to align more closely with the EU financial ecosystem. As Georgia progresses in building its digital economy, adhering to EU standards will be crucial for attracting investment, fostering economic growth, and maintaining the stability of the financial sector.

The adoption of regulations like "DORA" in Georgia will significantly strengthen the country's cybersecurity situation. By implementing thorough risk management practices, financial institutions in Georgia can improve their ability to recognize, evaluate, and manage digital risks. This, in turn, will decrease the occurrence and severity of cyber incidents, guarantee the uninterrupted provision of financial services, and safeguard the wider economy (Bafin, 2024).

Moreover, implementing strict incident reporting requirements will strengthen Georgia's ability to respond to digital threats. Prompt and transparent reporting of significant incidents ensures that regulators can quickly address emerging risks and coordinate an effective response. This will reduce the impact of disruptions and strengthen the overall stability of the Georgian financial system.

In the context of third-party risk management, implementing regulations like "DORA" will assist Georgia in handling the complexities of digital supply chains. As Georgian financial institutions rely more on third-party providers for important functions, it will be crucial to make sure that

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

these relationships follow strong due diligence and monitoring practices. This will reduce the risks linked to third parties failing and enhance the stability and security of the Georgian financial sector.

Furthermore, adhering to EU standards by implementing regulations similar to those of "DORA" will help enhance integration with the EU financial ecosystem. This will increase the interest of foreign countries and individuals in Georgia, both for investments and will promote stronger economic ties with the European Union. Increasing investor confidence, stemming from stringent regulatory standards, will form the foundation for economic growth and the introduction of innovations in Georgia's financial sector.

Finally, enhancing digital resilience through regulations like "DORA" will boost consumer confidence in Georgian financial services. By ensuring that financial institutions uphold high standards of cybersecurity and operational resilience, Georgian consumers will have more confidence in the security of their data and assets. This increased confidence will, in turn, contribute to the growth of digital financial services.

Conclusion

The EU consolidated act, named the "Digital Operational Sustainability Act," seems to be the main "savior" to the 21st-century challenge of regulating digital operations. It provides skilled professionals in law, economics, finance, IT, or other relevant fields with valuable insights to enhance the digital sustainability of their companies. This initiative aims to boost economic stability and foster trust in digital financial services, benefiting both the EU and Georgia. For the EU, "DORA" will enhance the digital resilience of financial institutions, improve the collective response to digital threats, and boost greater consumer confidence.

For Georgia, adopting a framework similar to "DORA's" and following the directives will enhance its cybersecurity, ensure adherence to EU regulations, and stimulate economic growth and innovation. By establishing a robust legal framework to regulate digital operations, both the EU and Georgia can protect the stability and security of their financial sectors in the current era of rapid digital growth and innovation.

By aligning their regulatory approaches, the EU and Georgia can also promote stronger cross-border cooperation, creating a more integrated and secure digital marketplace. This will not only facilitate smoother trade and financial exchanges but also position Georgia as a trusted partner within the global digital economy.

Additionally, the adaptability of DORA's framework can serve as a model for other regions seeking to enhance their digital operational resilience. Ultimately, this collaboration represents a critical step toward a more secure,

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

resilient, and innovation-driven financial ecosystem for both the EU and Georgia.

Conflict of Interest: The author reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The author did not obtain any funding for this research.

References:

1. *Analysis of Digital Operational Resilience Act*, https://www.dora-info.eu
2. Bundesanstalt für Finanzdienstleistungsaufsicht https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html
3. Cuel R., Ponte D., Virili F., (2022). *Exploring Digital Resilience, Conference Proceedings*
4. Devezas T., Leitao J., Sarygulov A., (2021). *The Economics of Digital Transformation*, 281
5. *Digital Finance and Innovation*, https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
6. *DORA Countdown: Aktueller Stand und Umsetzungsansätze* https://www.onetrust.com/de/resources/dora-countdown--aktueller-stand-und-umsetzungsansaetze/
7. *Harmonisierung der Sicherheit im gesamten EU-Finanzsektor* https://www.pwc.de/de/cyber-security/digital-operational-resilience-act.html
8. Husovec M., (2024). *Principles of the Digital Services Act*, 512
9. Matos F., Selig P., Henriqson E., (2023). *Resilience in the Digital Age*, 333
10. Milkau U., (2022) *Operational Resilience in Finanzinstituten - Grundlagen, Beispiele und Anwendungen*, 321
11. Müller-Terpitz K., (2024) *Digital Services Act: DSA, Kommentar*, 860
12. Pattison A., (2024). *Dora: A Guide to the EU Digital Operational Resilience Act*, 114
13. Press L., (2023). *Digital Operational Resilience Act (DORA): The Essential Refference*, 142
14. Priller M., (2024). *DORA in Versicherungsunternehmen: Regulatorik, Vorgehensmodell, praktische Aspekte, Erfolgsfaktoren*, Karlsruhe: Verlag Versicherungswirtschaft, 182
15. *Regulation Analysis* https://www.digital-operational-resilience-act.com

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

16. Schröder M., Hartl K., (2024). *Cyber Resilience Act: CRA*, 600
17. Stephan L., Rupprecht S., Tamdjidi C., (2024). *The Resilient Culture: Gow Collective Resilience Leads to Business Success*, 256
18. Tagarev T., Stoianov N., (2020). *Digital Transformation, Cyber Security and Resilience*, 2nd edition, Varna, Bulgaria, 258