Short economic and financial analyses

Cyber stress tests 2024

Authors: Borut Poljšak and Marko Bračković

January 2025

BANKA SLOVENIJE
EVROSISTEM

Collection: Short economic and financial analyses

Title: Cyber stress tests 2024

Authors: Borut Poljšak and Marko Bračković, Banka Slovenije

Email: Borut.Poljsak@bsi.si, Marko.Brackovic@bsi.si

Issue: January 2025

Place of publication: Ljubljana

Issued by:
Banka Slovenije
Slovenska 35, 1505 Ljubljana, Slovenija
www.bsi.si

Electronic edition:
https://www.bsi.si/publikacije/raziskave-in-analize/kratke-ekonomsko-financne-analize

The views expressed in this paper are solely the responsibility of the authors and do not necessarily reflect the views of Banka Slovenije or the Eurosystem. The figures and text herein may only be used or published if the source is cited.

© Banka Slovenije

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID **224421635**
ISBN 978-961-7230-13-0 (PDF)

Table of contents

Abstract

This paper shows the results of cyber stress tests conducted among Slovenian banks in 2024. The exercise was divided into two parts. In the first part of the cyber test, banks had to provide a cyber attack report as defined in the scenario. The report is divided into three parts to provide background information on the cyber attack. The second part of the report was followed by a questionnaire, which constituted the central and most comprehensive part of the test. The resilience of the banking sector to the hypothetical scenario was measured using various measures and indicators that show the impact of the scenario on the operational functioning of key economic functions such as deposit-taking and lending and on financial losses. The results of the scenario were evaluated using measures designed to assess operational risk, reputation, operational resilience and negative financial impact by economic function. We also assessed the potential impact of a hypothetical cyber attack on operational and financial stability. The impact of a hypothetical cyber attack on financial stability was measured in terms of operational dysfunction of key economic functions, direct and indirect financial losses, and impact on confidence in the banking system. However, the findings of our test are primarily intended to further supervisory activities or dialogue, learning and raising awareness of the importance of cyber security among all stakeholders.

1 Introduction

In recent years, cyber risks have increasingly grown in number and sophistication at the EU and SSM levels.

Their relevancy prompted the ECB to conduct a targeted cyber risk stress test in 2024, encompassing all the significant institutions. Following the ECB's lead, Banka Slovenije decided to conduct its own exercise encompassing all less significant institutions and subsidiaries of Member State banks, aiming to obtain results for all institutions active in Slovenia.

Cyber stress tests represent a supervisory tool for testing the performance of the financial system to ensure the continuity of key economic functions with timely and effective response and recovery from a severe but plausible cyber scenario that causes significant disruptions and could affect financial and operational stability. Supervisors conduct cyber stress tests to identify potential cyber vulnerabilities that could pose risks to financial and operational stability.

The approach was based on that of the ECB exercise but simplified in scope, aiming to obtain systemic, aggregate insights rather than conclusions and recommendations at the level of individual banks. The exercise was divided into two main parts. The first part involved a hypothetical cyber attack, defined with a common scenario. Based on this, the banks were required to submit a Cyber Incident Report in accordance with existing EBA guidelines. The report itself was divided into three parts (initial, intermediate and final) and gathered basic information about the cyber incident. Following the report was a questionnaire, which constituted the core and most extensive part of the exercise. At the same time, banks were required to provide appropriate evidence and documentation to support their responses. Based on the approach of Banka Slovenije, the ECB questionnaire was supplemented with a smaller set of additional questions relating to systemic risks.

On 26 January 2024, Banka Slovenije presented the approach and timeline of the exercise to the banks. The cyber exercise began on 19 February 2024 and concluded on 15 April 2024 with the submission of the completed questionnaires and accompanying documentation.

2 Approaches, objectives and scope of recent cyber stress tests

Given the increasing importance of cyber risks, a number of regulators have already implemented various approaches in order to assess the resilience of the institutions under their jurisdictions.

The Bank of England (BoE) carried out its cyber stress tests in 2022. Internal specialists were used to draft an initial scenario, which was then challenged by senior experts in the sector in order to assure its efficacy. The direct participation of the institutions in shaping the scenario allowed the banks to effectively prepare and assign their resources to the exercise. At the same time, the Bank of England indicated that the scenario was subject to change until the launch date in order to prevent "gaming" by the participants. The 2022 Cyber Stress Test focused on a UK retail payments system, including the main participants and the financial markets infrastructure. The objectives of the test were to understand the response and recovery capabilities of the banks and the impact on their clients and UK financial stability. The Bank of England designed and conducted tests using internal specialists with experience working in financial markets or conducting similar operational resilience tests and exercises. It also had access to internal supervisory and specialist knowledge in technical areas such as liquidity management. It did not use external resources. The Bank of England also completed an additional Cyber Stress Test in 2024 (Bank of England, 2024).

The Danish Financial Supervisory Authority (DFSA) conducted its cyber stress tests in 2023. The aim was to make a quantitative assessment of possible consequences of a successful attack at bank level. The focus was on the ability of individual firms and on gaining insights into the specific issues affecting each firm. Furthermore, the DFSA gained important insights into the capabilities of the participating institutions. The result was a list of individual follow-up points for each participant directing to where improvements had to be made. In this way, the DFSA could also identify a common set of best practices to be shared with the institutions later on. The DFSA also supported involving the banks as early as possible in order to gain knowledge of the technical and business set-ups. The DFSA made use of external expertise during the first CST, primarily for the design of the technical details of the disruption scenario. This provided technical competencies that were not available in the DFSA. Since one of the objectives in the DFSA's first CST from 2023 was to test recovery capabilities, the addition of details of the technical causes of the disruption in the scenario design was needed (DFSA, 2024).

The SSM Cyber Resilience Stress Test were carried out in 2024 and encompassed 109 institutions directly supervised by the ECB. The focus was primarily on the micro-

prudential impact of a cyber-related scenario and to ascertain the ability of each institution to respond and recover. The SSM also used internal specialists to design the cyber scenario, which was inspired by the information collected about real incidents in supervised institutions. While the basic approach of the scenario was shared by the banks, detailed information was withheld in order to simulate the desired shock. During the first phase of the execution, every tested entity was required to share with the SSM a report explaining the impact of the scenario in their institutions. This report helped the SSM to assess whether the scenario was well understood. The exercise resulted in a collective overview as well as individual reports describing the main weaknesses identified during the exercise and proposing actions for their mitigation. The SSM, however, did not make use of external resources neither on the design of the exercise nor in its execution and was able to identify and assign to the exercise enough resources with the right level of expertise (ECB, 2024).

3 Approach of cyber stress test in 2024

3.1 Scenario, Cyber Incident Reports and Questionnaire

The exercise of Banka Slovenije was based on the scenario defined by the ECB, but with an adjusted timeline.

Banks had to proceed according to the guidelines based on the scenario and submit Cyber Incident Reports to Banka Slovenije following the incident. The reports were submitted in three parts. In the first report, which was to be sent within four hours on the day of the incident (19 February 2024), banks had to provide contact persons and preliminary data. Timely and accurate reporting immediately after the incident was crucial. Banks were required to submit an intermediate report within three working days of the incident (i.e. by 22 February 2024). This represented the most comprehensive segment of the report. Banks provided more detailed information about the incident itself – a description of the incident, its impact and how they mitigated the consequences of the attack. The intermediate report was particularly crucial for the first quantitative assessments such as the financial impact (in EUR) and the number of transactions affected by the incident. Thus, the intermediate report represented the first estimate of the extent of damage from the cyber attack and the basis for the quality assurance (QA) checks of the main questionnaire. The final report was submitted 20 working days after the incident (18 March 2024) and contained a concluding analysis of the root cause and a description of the subsequent monitoring of banking operations.

The supplemented ECB questionnaire was the key element of the exercise and included data on the impact of the defined scenario on banks and savings institutions

and their response, actions and procedures. Banks and savings institutions were required to securely submit the questionnaire to Banka Slovenije by 15 April 2024.

3.2 Key Measures

We evaluated the results in terms of several metrics.

- The first encompassed an assessment of operational risk. It measured the direct potential nominal loss (in EUR) due to the hypothetical scenario both on the system and on individual banks.[1]
- Similarly, we also assessed the potential impact of reputational risk. This would encompass the negative effects that the institutions would incur following the incident. They relate to the consequences following a potential loss of confidence in the institution as well as measures taken by the banks to stop the trend and reverse it.
- Finally, we evaluated the impact of the hypothetical cyber attack on the banking system and its financial stability (systemic effects) from three aspects: (i) the operative (non)functioning of key economic functions[2] and transfer of this non-functioning to other banks and savings banks, (ii) the amount of financial loss (in connection with the duration of the long-term non-functioning of key economic functions), and, through an estimated, (iii) drop in confidence in the banking system.

[1] The individual assessments were weighted by the total risk-adjusted assets (RWA) for operational risks.

[2] The key economic functions represent the main operations conducted by the bank, such as loan approval, payments, deposit infrastructure, etc.

4 Results of cyber stress test 2024

The results indicate that the hypothetical direct negative financial effects are low but heterogeneous. At the level of the entire system, they amount to only €18.5 million, which is approximately 0.71% of the risk-adjusted assets for operational risks at the end of 2023 and 1.72% of net profits.

At the same time, it is evident that the results vary both among groups of banks (significant institutions, less significant institutions and subsidiaries of Member State banks) and between individual banks. The largest negative direct effects arise from:

- loss of fees and commissions from payment transactions and losses from late payment interest on unprocessed payments,
- costs of fines and penalties[3] and additional compensation claims from clients,
- activities related to immediate security upgrades after the incident, which often included external consultants, and costs of conducting security re-evaluations.

The results show that the various institutions generally had different approaches to estimating the potential losses, irrespective of their size. There are three fundamental reasons for this. First, the scenario allowed for a high level of interpretation as to the scope of the effects and it was often up to the banks themselves to define which systems were affected and to what extent. Banks could manoeuvre within the basic infrastructure of the exercise in a way that could mirror how comprehensively they wished to conduct the exercise. As is the case with stress tests, institutions which were more rigorous in their approach were also likely to exhibit larger losses compared to less conservative institutions. The second reason for the heterogeneous results lies in the general disparity in the know-how of the participating institutions. To some degree, this relates to the size of the institution and the complexity of its system, but this was not always the case. The last reason lies in the limited ability to conduct a quality assurance process by the regulator owing to the lack of comparable data.

Hypothetical indirect negative effects of reputational risk were also assessed as low. They amounted to €5.1 million, representing 0.20% of the risk-adjusted assets for operational risk at the system level or 0.47% of net profits for 2023. It should be stressed, however, that the assessment was not required for SI banks, while nearly half of the institutions estimated that there were no such effects. The remaining banks and savings institutions used various methods to evaluate indirect effects, largely based on

[3] Such as under Article 396, paragraph 2, of the Banking Act (ZBan-3).

existing internal processes such as the Internal Liquidity Adequacy Assessment Process (ILAAP). The largest effects stemmed from:

- the loss of customers and net income due to an estimated decrease in the number of account holders in the short-term time period following the incident. This was primarily estimated using historical data or using existing Liquidity Adequacy Assessment Process models to assess outflows of demand deposits and consequently reduced net income,
- media campaigns and related PR activities aimed at restoring reputation in the subsequent months.

Many institutions considered the aforementioned effects minimal or even non-existent due to two main reasons. The duration of the incident itself was estimated as limited at a number of banks and was compared to similar technical issues which actually did happen in the past and which did not result in a decrease in the number of account holders. Second, many of the institutions judged customer behaviour to be more resilient and understanding or that they would consider closing their accounts too bothersome given that the incident was a singular event.

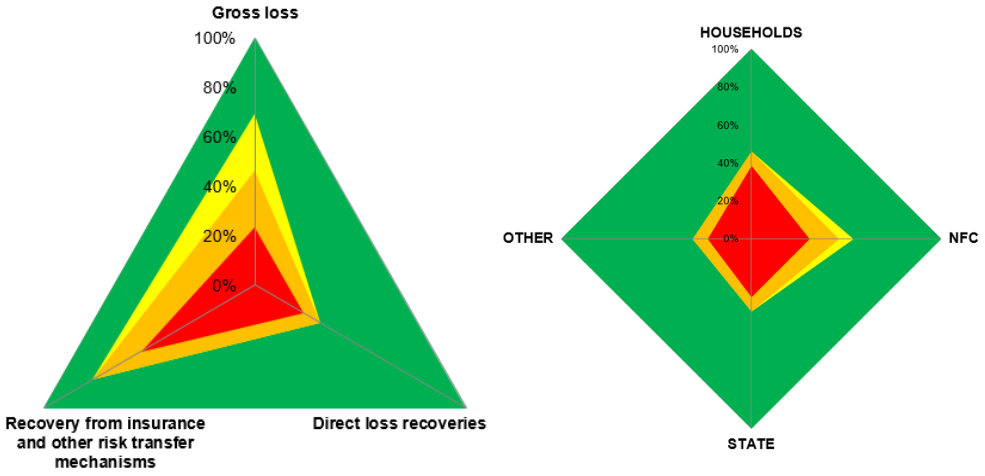
The assessment of operational resilience is identified by the direct (negative) impact of the hypothetical scenario, measured by the number and share of non-functioning key economic functions. According to the banks' self-assessment, the hypothetical scenario would have a moderate impact on the functioning of key economic functions, both at the level of individual banks and at the banking system level. All banks assessed that deposit-taking, lending, and the provision of payment services and cash operations would be impacted by the hypothetical scenario. Key economic functions that would be less impacted by the hypothetical scenario included settlement, clearing, cloud services and wholesale funding. The hypothetical scenario would also have a moderate impact on the services provided by banks to customers through outsourced services.

The results show that the largest negative effects came from the deposit and loan segments, which is also consistent with our banks' business models. In the deposit segment, banks and savings banks estimated outflows that would occur in the aftermath of a cyber attack (e.g. in the first three months) due to inoperability and loss of confidence. In the lending segment, banks mostly estimated a reduction in lending volumes over a certain period of inoperability (e.g. 2–3 days), which would make it impossible to lend to customers. It is important to point out that this partially explains the discrepancy between the estimated number of economic functions that were affected or not operational for a certain period of time and the estimation of the actual economic impact in EUR. As an example, most banks confirmed that a hypothetical attack would have an impact on the provision of payment services, but they also estimated that the actual

financial impact due to the non-functioning of this key economic function would be insignificant. More specifically, banks and savings banks recognised that there would be a minimal loss of fees due to the non-functioning of digital channels but also estimated that in this case the vast majority of customers would simply wait to pay (similarly, they estimated the impact for the cases of non-functioning ATMs or cards). At the same time, banks also reported different, heterogeneous results in this part of the analysis, which directly depended on the conservatism of the institution's approach.

At the level of the banking system, the largest negative impact came from the deposit segment (decrease of 2.5%) and more specifically from the segment of deposits of non-financial corporations (decrease of 5.1%), as these are more responsive to potential changes and less "sticky" compared to household deposits.

Figure 1: **Reputational damage assessment based on financial losses**



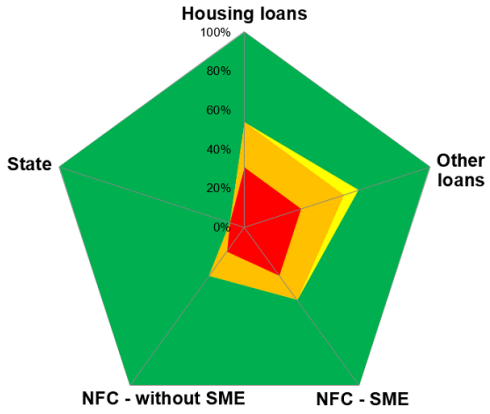
Note: The graphs show the share of banks at each risk level[4] according to operational risk indicators for financial losses and losses in the household, non-financial corporations, government and other deposit segments.

Source: Banka Slovenije.

The negative effects on lending at the system level were largest for consumer credit (decrease of 0.3%) and large non-financial corporations (decrease of 0.3%). In both cases, however, the financial impact arising from the inability to make new loans was smaller compared to the potential (consequent) outflow of deposits due to a loss of confidence.

[4] The estimate of the risk level is defined as the negative impact (in EUR) per economic function is calculated as the ratio of the scenario results to the items reported within the reporting ITS. This gives the proportions of economic impact by key function. For each operational risk indicator, we have defined thresholds based on statistical analysis. The indicator values are colour-coded according to the predefined threshold. The indicators are colour-coded on a 4-level colour scale, with red indicating very high risk and dark green indicating low risk.

Figure 2: **Operational risk assessment for the loans segment**



Note: The graph shows the share of banks at each risk level according to the operational risk indicators by loan segment: loans to residential property, loans to government, loans to non-financial corporations and other loans.

Source: Banka Slovenije.

5 The impact of the hypothetical scenario on banking system performance and financial stability

In this exercise, we also assessed the systemic effects, i.e. how a hypothetical cyber attack would impact the banking system and financial stability.

We measured the impact of the hypothetical cyber attack on financial stability from three perspectives: (i) the operational disruption of key economic functions and the spillover of this disruption to other banks and savings banks, (ii) the magnitude of the financial loss (in relation to the duration of the long-term disruption of key economic functions), and (iii) the decline in confidence in the banking system (ESRB, 2020).

The hypothetical cyber attack had a moderate impact on the operational functioning of the bank's IT systems, and we therefore assess that it did not pose a threat to the operational and financial stability of the banking system. Because of low direct and indirect financial losses, we estimate that the hypothetical cyber attack would not have led to a funding risk, as the majority of banks resumed their operations within 20 hours. The liquidity of the banking system would not be compromised. Settlement of liabilities (payment and cash transactions) would not be affected by a hypothetical cyber attack. The hypothetical cyber attack would not have received any media coverage and therefore would not have had a significant impact on confidence in the banking system.

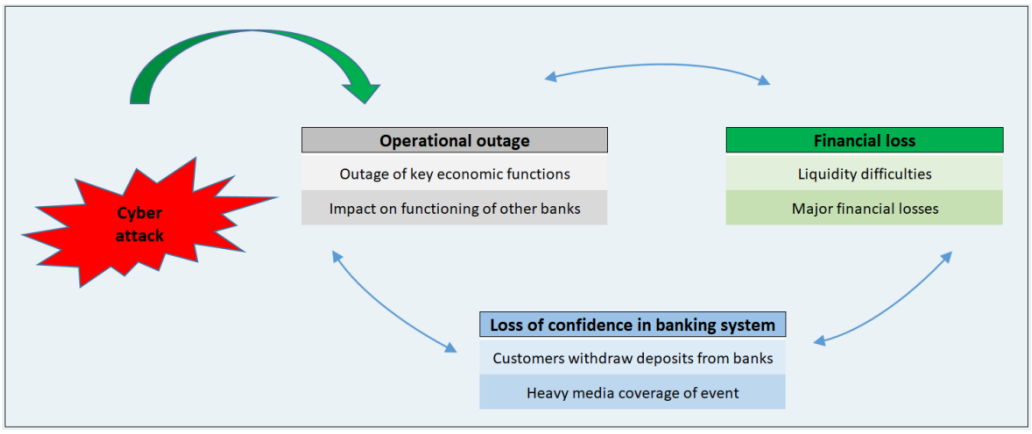
Systemic cyber risk can be defined as the combination of the probability of cyber incidents and their potential impact on banks' operations, which may materialise in the form of operational disruptions, financial damage or risk transfer to other institutions.

The hypothetical cyber attack was primarily aimed at disrupting the functioning of key economic functions and, as a consequence, the operational functioning of the banking system and the wider economy (Poljšak, 2024).

To mitigate operational disruptions to the banking system, banks and savings banks already use a variety of operational tools relating to cyber incident information sharing, crisis management and coordination in dealing with cyber incidents, and the operation of back-up IT systems (ESRB, 2022). The operational tools make banks and savings banks more prepared for operational disruptions by ensuring that they have adequate information-sharing mechanisms in place to deal with incidents more quickly and that they have back-up systems in place to enable a rapid return to business as usual (ESRB, 2023). The results of the exercise show that banks and savings banks are already using various operational tools to mitigate operational disruptions, such as information-sharing on cyber incidents, crisis management and coordination in dealing with cyber incidents, and the operation of back-up IT systems.

The hypothetical cyber attack was used to measure the direct and indirect financial loss of key economic functions at the level of the banking system. If a cyber attack disrupts key business operations for a longer period, this means a loss of access to financial resources and the ability to settle liabilities, and customers and market participants may lose confidence in the banking system. In the event of a high-profile media event, public confidence in the banking system is severely affected and it is important that banks run media campaigns aimed at restoring public confidence in the banking system as a result of a cyber event.

Figure 3: **The impact of a hypothetical cyber attack on financial stability and potential channels of contagion in the banking system**



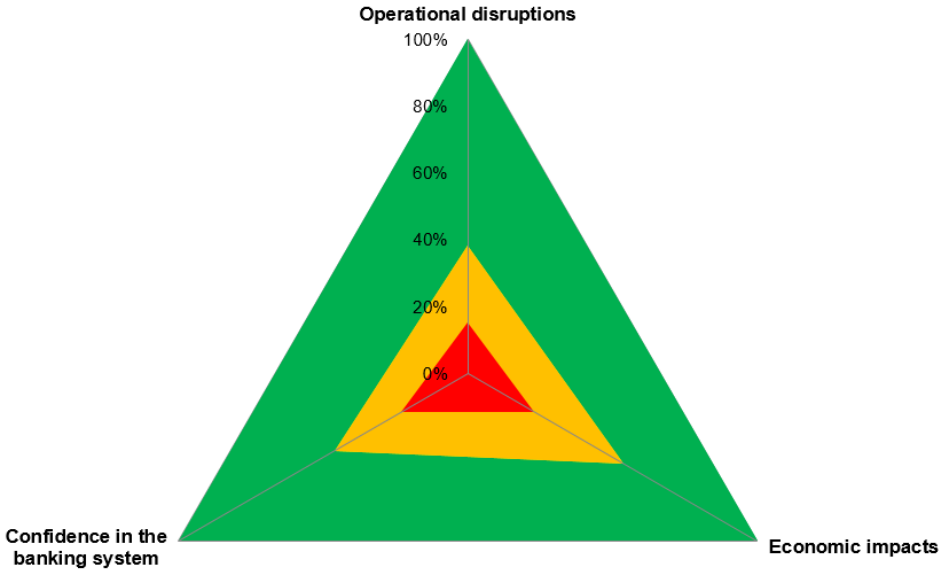
Source: Banka Slovenije, 2024.

In this cyber stress testing exercise, we monitored and identified the non-functioning of certain key economic functions across banks and central bank IT systems. We conclude that a hypothetical cyber attack would have a moderate impact on the operational functioning of the banks' IT systems. We did not detect an operational contagion in the system, as the hypothetical cyber attack did not affect interbank operations, the functioning of other bank IT systems or shared ICT service providers. Banks and savings banks did not report that the hypothetical cyber attack impacted the functioning of the

central bank IT system, which is managed by external or internal service providers. Based on the results of the stress tests, we assess that the hypothetical cyber attack did not threaten the operational stability of the banking system.

The hypothetical cyber attack was also used to measure the direct and indirect financial loss at the banking system level. Based on the banks' self-assessment, we can conclude that the hypothetical negative economic impact on the banking system would be low. Because of the low direct and indirect financial loss, we estimate that a hypothetical cyber attack would not lead to a funding risk. A cyber attack could lead to a direct loss or loss of access to funds, which would affect the ability of banks to fund their operations in the market. The liquidity of the banking system would not have been compromised. The hypothetical cyber attack would not affect the settlement of liabilities (payment and cash transactions). A hypothetical cyber attack would not disrupt the operation of key economic functions for a prolonged period of time. Based on the banks' self-assessment, they would have resumed operations within 20 hours. Direct and indirect financial losses were negligible at the banking system level. Half of the banks estimate a minor decline in public confidence. These banks announced that they would organise media campaigns to restore their reputation within one year of the event. A hypothetical cyber attack, as the scenario suggests, would not have a high profile in the media and would therefore not have a significant impact on confidence in the banking system.

Figure 4: **Cyber risk and impact on financial stability**



Note: The graph shows the share of banks at each risk level according to the banking system risk indicators: confidence in the banking system, economic effects and operational interruption.

Source: Banka Slovenije.

Based on the results of the cyber scenario, which assumed a hypothetical attack on the central banking IT system, we estimate that such a cyber attack would have a low impact on the operational and financial stability of the banking system. The impact on the functioning of key economic functions was moderate, with banks recovering most

of their functions within a reasonable time. Banks reported the cyber incident within the required timeframe to the relevant supervisory and other authorities normally involved in dealing with major cyber events (reporting the cyber incident to Banka Slovenije, the ECB, SI-CERT, etc.). Banks therefore reacted swiftly and restored their operations to the situation pertaining before the cyber event. On this basis, we assess that the operational resilience of the banking system is at a moderate level. Based on the banks' self-assessment, the direct and indirect gross loss[5] caused by the hypothetical cyber attack would be negligible and would not have a material impact on the customer and corporate business. The cyber attack had a low impact on deposit outflows and on the liquidity of the banking system. Banks have calculated the indirect financial loss based on the stress scenario of the Internal Liquidity Adequacy Assessment Process (ILAAP), or the outflow of demand deposits and the resulting reduction in net income, which is negligible at the level of the banking system. We have not detected that the hypothetical cyber attack would cause operational and financial contagion in the banking system. This means that the non-functioning of a single core banking system did not affect the functioning of other banking IT systems or third-party ICT service providers that banks use in their operations.

6 Conclusions

The results of the cyber stress tests show that the direct financial impact on the banks included in the exercise would be small under the scenario in question. It would amount to less than 1% of the risk-weighted assets for operational risk from the end of 2023 and approximately 1.7% of net profits. The largest negative impacts would come from customer reclaims and lawsuits resulting from the outage of payment services, the cost of sanctions and fines, and the costs of further security enhancements after the actual recovery, including external consultants. It should be mentioned that the latter represents additional costs which are necessary for amending the situation rather than direct damages. The negative financial impact of reputational risk would be even smaller. The banks used a variety of methods to assess the indirect effects, which were largely based on existing internal business processes.

According to the banks' self-assessments, the hypothetical scenario would have a moderate impact on the functioning of key economic functions both at the level of the individual banks and at the level of the banking system. The attack would affect key economic functions related to deposit-taking, lending, payments and cash operations. The key component of the negative financial impact would come from the deposits and loans segment. The negative impact in connection with deposits is attributable to a loss of customers and withdrawals of deposits caused by a lack of confidence. The (smaller)

[5] Gross loss is defined as the loss not reduced by the other two items: direct loss recoveries and insurance recoveries.

negative impact in connection with loans comes from the decline in loan stock compared with the situation in the absence of the cyber attack, with customers being unable to enter into credit agreements while key economic functions are not working and subsequently failing to replace the credit agreements. The assessed decline in net income was negligible at the level of the banks included in the exercise.

The scenario would cause considerable yet short-term disruption to the functioning of the core banking system or affect a number of key economic functions, most notably deposit-taking.

However, the response and recovery procedures to the scenario presented were not fully effective. We identify that there are areas for improvement, such as ensuring consistent business continuity, regular checks on how backup is ensured, incident response planning, and regular review and revision of contractual relationships with third-party providers. Raising awareness of the importance of information security among staff and customers can also play a role. Our assessment is that the banks are adequately prepared for a security event such as that envisaged in the scenario. A different cyber incident could have a different, perhaps greater, impact on banks' operations. We therefore encourage the banks to continue investing additional resources in upgrading bank information systems, which can further improve cyber resilience.

7 References

Bank of England (2023). Thematic findings from the 2022 cyber stress test. Available at: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test.pdf.

Banka Slovenije (2024). Poročilo o finančni stabilnosti. October 2024. Available at: fsr_2024_okt_eng.pdf.

Danish Financial Supervisory Authority (DFSA, 2024). Cyber stress testing. Available at: Cyber stress testing_v4.pdf.

ECB (2024). ECB concludes cyber resilience stress test. Available at: https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html.

ESRB (2020). Systemic cyber risk. February 2020. Available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

ESRB (2022). Mitigating systemic cyber risk. January 2022. Available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf.

ESRB (2023). Advancing macroprudential tools for cyber resilience. February 2023. Available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf.

Poljšak, B. (2024). Kibernetska varnost bančnega sistema. Ljubljana: Banka Slovenije, 2024. Available (in Slovene) at: https://www.bsi.si/publikacije/raziskave-in-analize/prikazi-in-analize.