Safe Bank 2 (79) 2020

DOI: 10.26354/bb.8.2.79.2020

Position of the European Financial Congress[1] with regard to the European Commission's consultation document on Digital Operational Resilience Framework for Financial Services[2]

based on expert responses in a group expertise of EKF

Methodology for preparing the answers

The answers were prepared in the following stages:

Stage 1

A group of experts from the Polish financial sector were invited to participate in the survey. They received the consultation document and selected consultation questions in Polish.

The experts were guaranteed anonymity.

Stage 2

Responses were obtained from experts representing:

- banks,
- insurance companies,
- e-commerce companies,
- consulting firms,
- the academia.

Stage 3

The survey project coordinators from the European Financial Congress prepared a draft synthesis of opinions submitted by the experts. The draft synthesis was sent to the experts participating in the survey with the request to mark the passages that should be modified in the final position and to propose modifications and additions as well as marking the passages they did not agree with.

[1] European Financial Congress (EFC – www.efcongress.com). The EFC is a think tank the purpose of which is to promote debate on how to ensure the financial stability and sustainable development of the EU and Poland.

[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

Stage 4
On the basis of the responses received, the final version of the European Financial Congress' answers was prepared.

Answers of the European Financial Congress to the consultation questions

1

EC.CD	Question	Yes	No
Q1	Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?	15	3

Building the principles of ICT risk management within the complex and thoroughly regulated sector of financial services in a way that requires reconciliation and making joint and agreed arrangements does not raise doubts among respondents. 83% of respondents see value in establishing a common template for ICT risk management rules within the sector.

As with any standardization approach, it is pointed out that standardization and appropriate principles of ICT risk management may prove useful. On the other hand, it should be understood that compliance with the new ICT risk management standards will entail compliance costs. Banks and other financial institutions are already heavily burdened with regulations, in addition, they currently manage operational risk and comply with the provisions of normative acts as well as supervisory guidelines and recommendations. One should consider (and estimate) whether the benefits will exceed the costs in the particular areas of ICT risk management in which new rules and requirements will be introduced. Therefore, there is a need to conduct a detailed Cost-Benefit analysis and feasibility studies on the implementation of risk management recommendations and rules, which will again increase the cost of managing the banking institutions' security area. One should consider using security experience from other areas of the market and sharing experience within the financial sector. This may contribute to reducing the expenditure concentrated within the financial sector institutions. It would, therefore, be appropriate to analyze the usefulness of possible new regulations in terms of the cost and risk of their implementation into business models and operational models of financial institutions and their partners.

2

EC.CD	Question	Area	1	2	3	4	5
Q2	Where in the context of the risk management cycle has your organization until now faced most difficulties, gaps and flaws in relation to its ICT resilience and preparedness? (1 – not problematic, 5 – highly problematic)		18	43	21	10	11
	»	Identification	1	7	2	2	1
	»	Detection	1	5	3	2	2
	»	Ability to protect	1	8	2	1	1
	»	Respond	2	6	3	0	2
	»	Recovery	2	6	2	1	2
	»	Learning and evolving	2	5	4	0	1
	»	Information sharing with other financial actors on threat intelligence	4	1	3	4	1
	»	Internal coordination (within the organization)	5	5	2	0	1

Respondents' answers indicate that organizations are unlikely to face security gaps that are highly problematic (around 60% rated the occurrence or identification of gaps as not problematic). About 20% treat major security gaps as a problem. It is not problematic to identify and ensure organization's preparedness for the ability to protect against gaps.

It also seems that organizations are prepared to respond appropriately to a gap and to recover from the effects of gaps. Attention should be drawn to the considerable willingness to share information about threats with other market participants and to the certainty about efficient management of that information within the respondents' organization.

Indicated currently as particularly problematic are areas of managing solutions located in the cloud – in terms of data security (in particular the ability to detect risks in the Cloud environment, docker, etc., and the ability to detect and eliminate risks in the development process of SDLC software).

3

EC.CD	Question	Area					
Q3	A) What level of involvement and/or what type of support/ measure has the Board (or more generally the senior management within your organization) offered or put in place/provided for, in order to allow the relevant ICT teams to effectively manage the ICT and security risk?						
	B) Is the Management Board of your organization involved in effective management of security incidents? (1 – no involvement, 5 – high involvement)	Rating scale	1	2	3	4	5
		Answers total	1	6	9	13	24
	»	Appropriate allocation of human and financial resources	1	2	2	3	5
	»	Appropriate investment policy	0	1	3	4	5
	»	Formal support and approval of security standards	0	0	1	4	8
	»	Active involvement and advice of the Board on security matters	0	3	3	2	6

Part A

Most responses highlighted the organization's Board's high involvement in supporting ICT departments to effectively manage security risks. The respondents defined the level of involvement as high or adequate to the requirements properly defined in this respect in the applicable KNF Guidelines. The high rank of this process was also pointed out as a company level strategic goal identified not only in the area of operations.

It was frequently emphasized that the Board should be realistically involved in key issues related to security risk management. They should regularly receive management information in this regard in a form adapted to the recipient. The replies also stipulated that there should be no belief that security risk management topics are confined to the ICT and CIO areas.

Additionally, the area of the Board's responsibility for the following issues was determined:

- determination of risk appetite, indicating issues that the ICT team can determine on its own;
- verification and acceptance of remedial plans for all risks beyond the scope delegated to be handled by the ICT team;
- acceptance of risks against which no remedial action will be taken;
- determination and review of an acceptable level of security risk (risk appetite);
- setting priorities to protect the organization's systems and information in accordance with the minimum security requirements, policies, business risk and applicable regulatory requirements;
- ensuring the provision and appropriate distribution of resources;
- promoting appropriate security behavior patterns throughout the organization;
- ICT security monitoring based on management information.

The Board's responsibility was also defined as direct involvement in making decisions regarding security risk management. It is important to ensure that the organizational structure has units responsible for monitoring the ICT area in terms of detecting and responding to security incidents. In addition to rapid response to security incidents, ensuring business continuity, it is necessary to use systemic risk management that will ensure the implementation of safeguards to minimize the vulnerability of ICT resources to emerging threats.

It was noted that in the era of digitization of financial sector services and the opening of banking systems, be it for regulatory or business reasons, the level of involvement on the part of the Management Board should be as high as possible from the point of view of direct supervision and reporting, participation in decisions and far-reaching support in terms of resource and budget. Periodic reporting of risks and their materialization potential, and fraud levels is required. The Management Board should also be made aware, including through training, of the types of risks, and management decisions should be expected when implementing solutions related to covering these risks or introducing additional ones (based on risk analysis in individual projects).

In addition, the role of the Management Board may be extended to include arbitration tasks, relevant members of the Management Board may or should sit on the ICT security committee and settle disputes between experts within a financial institution.

An adequate level of the Management Board's involvement to the risks, needs and outlays of the organization resulting from the work of the ICT department should be considered appropriate. In practice, this means that depending on the complexity of issues and the impact / results of work, Board Members should be involved accordingly.

Part B

Respondents identify the highest involvement of the organization's Board in the area of formal support and approval regarding security standards. Management Boards are active and participate in and advise on security matters. Less but still active support of the Management Boards of financial institutions can be seen in the area of allocation of human resources for effective management of security incidents. High and medium support is noted in the right investment policy in this area and in consulting.

4

EC.CD	Question
Q4	How is the ICT risk management function implemented in your organization? To the extent possible, please provide a description.

As should be expected, in the case of financial institutions which, by definition, care for high confidentiality standards, in most cases the answer was that they were unable to provide such information, but it was confirmed that the IT risk management process is set up in accordance with applicable good market practices and ICT risk management standards.

ICT risk management for financial institutions in Poland is a component of the Business Continuity Management procedure (simulations of total server room failure and data recovery solely from LTO backup tapes, failures of the Internet channel and replacement of optical fibers with a backup connection based on GSM access, etc.).

Financial institutions in Poland manage risk based on a standardized operational risk management model. Most institutions have documentation regulating in detail the process of technological risk management, including cyber risk.

The risk management process (including ITC risk) usually has the following scope and subprocesses:

- Planning and budgeting
- Identification and assessment
- Monitoring
- Risk mitigation
- Reporting

In financial institutions, ICT risk management processes are usually built into formally defined processes as part of operational risk management.

5

EC.CD	Question	Area	Answers	
Q5	Which of the listed main measures do you have in place to identify and detect ICT risks?		Yes	No
		Established and updated mapping of the organization's business functions, roles and supporting processes in relation to ICT risk management	8	4
		Registry of supporting ICT assets (systems, staff, contractors, third parties and dependencies on external systems)	11	2
		Defined and maintained IT support processes based on criticality	12	1
		Risk assessment performed before deployment of new ICT technologies / models	9	2

An overwhelming number of experts state that their organizations use defined and maintained mappings of business functions, roles and supporting processes in relation to ICT risk management, registers of ICT support elements, defined and maintained IT support processes depending on the degree of criticality and risk analyzes being carried out before deployment of new ICT models and technologies. In practice, it seems that due to the size of respondent institutions, this type of practice may exist in a smaller part of the market (smaller banks, cooperative banks and smaller insurance institutions).

It should be noted that standard ICT risk identification and detection measures are maintained in Polish financial institutions, based mainly on defined and maintained mapping of business functions, roles and supporting processes in relation to ICT risk management. Also registries of ICT support assets (systems, staff, contractors, third parties and dependencies on external systems) are maintained. All respondents confirmed identification and definition of the degree of criticality for ICT support processes. Institutions perform periodical risk assessment analyses before deployment of new ICT technologies / models.

Active risk reporting (including ICT risks) is confirmed at the following levels:

- during meetings of the Organization Management,
- on expert forums,
- at the Operational Risk Management Committee,
- at Management Board meetings.

One example of risk management control (including ICT risk) is the following process:

- self-assessment – a process of qualitative and quantitative risk assessment enabling identification, assessment, management and reporting of operational risk;
- the risks associated with operations, defined by organizational entities are mitigated by audits subject to the audit model;
- if the risk materializes, the internal escalation regulations are followed.

6

EC.CD	Question
Q9	Has your organization established a Multicloud (hybrid cloud) strategy?

Half of the respondents confirm willingness to construct multicloud or hybrid cloud solutions in their own organization. This means a great deal of readiness and flexibility in the choice of technology. Readiness refers to the mode of operation of financial institutions and openness to a variety of cloud solutions, but with signaled limitations on how to build this flexibility and independence. The hybrid cloud strategy provides the opportunity to ensure the necessary and expected reliability and performance, as well as considerable resilience to ICT risks. Reliability and performance are important factors for the financial institutions operating under service level regimes defined in contracts with end customers. The reason for choosing between a multicloud and hybrid cloud strategy is often the difference in the quality of individual available services, but also the specialization of specific suppliers and solutions. Hybrid cloud for financial institutions is a combination of opportunities offered by a public cloud and its private mutation. Hybrid operation makes it possible to migrate data and resources between both types of resources. A characteristic feature of the hybrid cloud is its versatility and greater possibilities of implementing critical systems – flexible technology offers wide possibilities of adapting the cloud to current needs or security formats. Resources of expected utilization are generated from a private cloud; in the event of shortage, they are deployed to the public cloud.

Implementation of a cloud-based operational model is the subject of cost and benefit analyses, especially in terms of information security and confidentiality, but also demonstrates that banks are open to new technologies. Half of respondents did not identify any of the available cloud technologies as being preferred or selected for implementation in their organizations. This may mean that institutions are only getting ready for implementation or even for building new business strategies based on cloud computing.

7

EC.CD	Question
Q11	Do you have legacy ICT systems that create new ICT security requirements? What are those requirements?

Changing new requirements regarding the need to ensure security also for legacy systems (often without support) are a problem for Polish financial institutions. Many respondents hide behind business secrecy or do not perceive requirements (about 60% of responders) for legacy systems in the area of security, with changing security risk standards. However, some financial institutions see the possibility of ensuring safe cooperation of legacy systems in most cases through integration with new technologies, in particular cloud technologies and containerization. Financial institutions recognize the need to respond to new challenges regarding the security of legacy systems, and in particular entire areas of ICT architecture, by the need to adapt them to new technological solutions and to provide an adequate level of support from suppliers.

Basically, problems with legacy systems result from the nature of their development, use and maintenance, and relate to lack of updates. The remedy is the need to implement solutions that provide additional separation, protection systems supporting virtual patching, purchase of additional extended support.

8

EC.CD	Question	Area	1	2	3	4	5
Q12	What in your view are possible causes of difficulties you experienced in a cyber-attack / ICT operational resilience incident? (rate from 1 – not problematic to 5 – highly problematic)		16/18	14/18	12/18	7/18	7/18
	»	ICT environmental complexity	2	3	4	1	4
	»	Issues with legacy systems	7	1	3	3	0
	»	Lack of analysis tools	2	4	3	2	3
	»	Lack of staff support	5	6	2	1	0

The answers to this question perfectly illustrate the low significance of problems with legacy systems, as identified in Question 11 and its answers. As may be seen, in the case of cyber attacks or security incidents problems are least related to

legacy ICT systems. Probably due to their role in application architecture (legacy systems have been replaced with new, more secure ones in the front-end areas that are vulnerable to cyber attacks). Legacy systems are usually transactional systems located in the back-end areas of the application architecture of financial institutions. In addition, new integration methods, which have been well tested for ICT risks and subjected to frequent security audits, have most likely been used in their case. It seems that possible operational difficulties in an organization in the event of a cyber attack may relate to the high complexity of the ICT environment and the low availability of analytical tools (in terms of availability – price of use, advanced functions, ability to use advanced functions – limitations in the education of staff operating the tools).

9

EC.CD	Question
Q15	Do you consider that your organization has established and implemented security measures (e.g. organizational structure, physical security, logical security, security monitoring, security reviews, assessment and testing, and training)?

Most respondents pointed to all the listed security mechanisms as already implemented within the organizations of financial institutions, but also indicated additional processes, mechanisms and tools (e.g. in the Threat intelligence family). The organizations of financial institutions have implemented many security mechanisms, both technological, process-based, procedural and administrative. Banks often ensure compliance with applicable regulations regarding security mechanisms, including Recommendation D, H, M (and other relevant) and the Act on the National Cybersecurity System. The above Recommendations of the Polish Financial Supervision Authority are issued on the basis of Article 137 (5) of the Banking Law Act and form a set of good practices for prudent and stable management of banks. Banks should expect their activities to be assessed based on recommendations.

The practice of issuing recommendations dates back to June 1996, when a recommendation of the National Bank of Poland was issued, signed by the General Inspector of Banking Supervision (executive body) „Recommendations for banks regarding the financial liquidity monitoring system". The prototype for the recommendation was the guidance for all banks from the President of the National Bank of Poland.

Drafts of individual recommendations are subject to public consultations, in particular with the National Bank of Poland, the Bank Guarantee Fund, the Association of Polish Banks and the National Association of Cooperative Banks.

Legal regulations and applicable market standards

As part of dedicated security policies, financial institutions maintain processes to ensure appropriate levels of security:

- patching and updating policy
- authentication management
- physical security
- reviews and audits
- resource management
- data processing policies
- incident management

Typical mechanisms used by financial institutions are:

- comprehensive and flexible security management system (understood as a part of security) based on three main principles: defense, prediction and involvement
- physical protection of the circuit with: ACS, CCTV,
- logical security measures (network security, endpoint protection, data encryption in transit and rest)
- incident recovery processes and capabilities
- security monitoring and incident response using SOC
- security awareness campaigns
- general control mechanisms in processes
- application-based control mechanisms together with dedicated SIEM, DLP, etc. class systems
- periodic penetration testing
- periodic checking of controls adequacy and effectiveness.

Sometimes, at organizations with a smaller scale of operations and potentially low business model complexity, only basic security tools (physical and logical security, monitoring and testing, incident reporting, training in the BCM / Disaster Recovery) may be implemented.

In general, security mechanisms are understood and organized as a multilayered and integrated defense system with three security barriers: protection, detection and response.

- protection – a set of systems, tools and services for preventing cyber attacks and for protecting client and organization information. It includes, among others: firewalls, anti-virus systems, e-mail filters and privileged access control mechanisms. In addition to other security systems, firewall also includes secure configuration and patching for all organization systems
- detection – a set of systems, tools and services used to monitor and quickly detect cyber attacks. These include: security operation center (SOC), incident monitoring tools, cybersecurity data lake, anomaly detection tools and machine learning.

- response – a set of systems, tools and services for analyzing cyber attacks, responding to them and mitigating their effects. These include: computer event response team (CERT), tools for taking over operations and system deactivation, forensic analysis and analysis of error causes.

Responses frequently pointed out to necessary regular monitoring of the organization's systems and networks for undesirable activities and constant readiness to respond to an effective cyber attack making it possible to cut its duration to a minimum and to mitigate the damage caused.

10

EC.CD	Question
Q17	Which issues do you struggle most with, when trying to ensure a quick restoration of systems and the need to maintain continuity in the delivery of your (critical) business functions?

Respondents report a frequent lack of problems, but each new attack is accompanied by only new challenges that the organization has to face within a properly planned budget.

Such challenges may be:

- network recovery
- unverified recovery procedures for some systems and data
- continued absence of current backups for some critical but locally managed systems and data

Interestingly, when preparing for quick system recovery after attacks in order to maintain critical business functions of the organization, a human factor was identified as a significant problem. Especially when it comes to carrying out the necessary activities to be completed within a specific timeframe. In addition to staff failure, low efficiency (performance) of backup systems was identified as a problem.

A potential problem identified in the case of system recovery after an attack is the scale effect in terms of the size and complexity of the ITC system, the number of users and clients, efficient cooperation among sectors and/or with law enforcement agencies.

In addition to backup systems, as a remedy for the speed and reliability of system recovery after a failure, implementation of a fully cloned and redundant test environment in the form of pre-production was pointed out, on which all patch tests can be run just as if implemented in a production environment.

Due to the scale of the enterprise and the quantitative range of data, in the case of financial institutions, comprehensive copies of systems, data and IT virtualization

infrastructure are created within one volume of external media, which ensures high security of recovery with full data integration.

In the case of rapid recovery of systems after attacks, generally speaking, each organization faces financial, organizational and technical issues in this area. For example, in the case of an attack of a larger scope than the area of business (attack affecting a wider group of entities or a larger region of the country), there may be problems with access to services necessary to maintain critical business functions of the organization. In this case, also for security and confidentiality reasons, an appropriate channel should be provided for the transmission of information on threats and failure effects to entities affected by the legislative process.

11

EC.CD	Question
Q18	What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)?

Respondents' answers entail various opinions, from a positive attitude: that they are needed and if properly discussed with business, supported with arguments, they permit adequate management of business continuity risks; to negative views that legislative definition of RTO or ROP is harmful, as these parameters should remain varied. These parameters are specific to each process and should be defined individually for each of them. There are propositions that an attempt to harmonize indicators across the industry would significantly reduce the efficiency of the entire sector, while not yielding any systemic benefits.

It is being suggested that these parameters should not be specified since access to data is an element that affects the quality of service more than the confidentiality and integrity of customer data, which should be of key interest for the regulator. Accessibility, as a feature of the service being purchased, should be regulated through competition between enterprises. In the market game, customers should decide whether they prefer a more expensive but less unreliable service or one that is cheaper but with the risk of longer downtime.

Observing various institutions operating in the local financial market, one can see that, as a rule, RTO and RPO times should be defined individually by organizations on the basis of risk analysis. This is due to the fact that each organization has a different risk profile and risk appetite. However, there may be resources whose criticality may be considered more broadly (in terms of potential sectoral, national or regional effects) – thus their RTO/RPO thresholds could be determined by legislation.

Statutory definition of RTO and RPO should not impose rigid parameters but rather refer to their adaptation to business operations and local conditions, at the most, with possible consideration of minimum RTO and RPO parameters for individual

areas. It should be remembered that incorrectly defined parameters may result in entities incurring costs that are disproportionate to the threat.

In today's development and condition of the Polish ICT market, the problem that is being pointed out is that RTO and RPO parameters are achievable at the 0 level since the technology available locally on the market (available for purchase by financial institutions) does not keep up with ICL solutions available globally.

Considering that these parameters are a derivative of the reliability and characteristics of business processes themselves, it is worth noting that the parameters should be defined for individual IT systems. Usually, they are the result of a Business Impact Analysis (BIA). If these types of parameters are set out in legislative documents, they may be harder to update later in the event of changes in business requirements.

12

EC.CD	Question
Q19	Through which activities or measures do you incorporate lessons post-incidents and how do you enhance the cyber security awareness within your organization? (please describe)

To implement lessons post-incidents to educate the organization, the basic system mechanism being used is the continually developed Security Awareness Program. After an incident, the root causes are analyzed and action proposals are put forward to reduce the risk of the incident's future recurrence, incident and problem management processes are analyzed, dedicated task groups are set up to solve the problem, the risk management process is used, and knowledge is shared on various internal forums. The ICT department management or the Management Board approve security measures for implementation. There are also additional recommended methods, such as internal training dedicated to a specific group of employees, covering detailed problem analysis (especially in the aftermath of an incident that is avoidable by enhancing employees' competences).

There are also limited post-incident methods being used, not the entire organization but only the units responsible for the incident are educated.

Often, financial institutions have formal rules for managing security incidents, whereby, if needed, actions are taken to provide appropriate units with recommendations about necessary corrective and remedial actions, followed by monitoring of their implementation and verification of their efficacy. This is accompanied by a dedicated process of raising users' awareness.

Appropriate risk mitigation measures are also used: Process Lessons Learned is an in-depth form of implementing risk mitigation measures. Corrective actions are

carried out taking into account each layer where gaps could occur: procedures/ configurations/lack of awareness.

Risk mitigation measures are based, among others, on:

- implementation of proper control processes and procedures,
- provision of classic or e-learning training to employees,
- information campaigns targeted at employees, contractors or clients of the bank
- changes in systems (parameterization),
- limitation of a possible recurrence of loss-generating adverse events.

Experts point to the mandatory post-incident analysis and a well-defined change management process in the context of post-incident recovery. A top-down approach may seem necessary to ensure proper communication and enforcement of changes throughout the organization.

13

EC.CD	Question
Q21	Do you agree that a comprehensive and harmonized EU-wide system of ICT and security incident reporting should be designed for all financial entities?

88% of respondents agree that a comprehensive EU-wide system of ICT and security incident reporting system should be designed for all financial entities. However, they signal a lack of a unified approach to the proper classification of event categories and classes.

14

EC.CD	Question	Area	Yes
Q22	If the answer to the previous question is yes, please explain which of the following elements should be harmonized?		
	»	Taxonomy of reportable incidents	13/18
	»	Reporting templates	13/18
	»	Reporting timeframe	10/18
	»	Materiality thresholds	13/18
	»	Other (please specify)	3/18

Respondents actively support the view that as part of a comprehensive EU-wide system for reporting security incidents for financial entities, the following elements (in the order of materiality) should be harmonized:

- Taxonomy of reportable incidents,
- Reporting templates,
- Materiality thresholds,
- Reporting timeframe.

As an additional comment, harmonization should encompass a breakdown and identification of attacks outside and within the EEA.

15

EC.CD	Question
Q24	Do you believe that the scope of reporting on security threats should be limited by materiality thresholds or unlimited?

The prevailing view among experts is that the scope of reporting on security threats should be limited by thresholds and to the data necessary to enable appropriate preventive measures to be taken by other market players. Also for security reasons, it should preferably be anonymized. It should be limited by thresholds so that only new/poorly identified threats that have a significant impact on system security are reported. In terms of information, the scope of reporting could be limited to a minimum necessary for the Supervisory Authority to make decisions and inform the public about the scope of possible consequences. All this information should be quantified to the extent possible. Excessive detail slows down the process of analyzing events and generating reports, raises the costs of its maintenance and additionally exposes the organization to difficulties with incident handling or to disclosure of sensitive data. Limiting and quantifying incident description may also be valuable for Supervisory Authorities which, due to limited resources and a large number of reports, will be forced to develop efficient processes for their assessment.

Other opinions take the view that only the full range of threats can provide a comprehensive picture of the security status. Thresholds should be maintained for detailed descriptions of serious incidents. In the annual cycle, the numbers of all incidents (as in PSD2) should be reported. Knowledge of the scale of threats and trends makes it possible to build detect and response strategies. Due to the changing nature of threats, as well as the diversity and volume of incidents, the scope of reporting should be limited.

It seems that a reasonable approach will be to work out an intermediate solution (analytical and synthetic). The most significant threats should be reported. Neither a full approach (e.g. each organization has a multitude of incidents related to e.g. breaches of internal procedures) nor a threshold-based solution (a short range incident may have serious consequences) is the best. The sector should develop an intermediate solution that takes into account incidents reported by thresholds (e.g. accessibility incidents) and cybersecurity incidents (advanced targeted attacks or attacks using advanced malware).

16

EC.CD	Question	Rating
Q26	Should there be a national platform for reporting incident reports?	13/16

In principle, there is an unequivocal view that a national incident reporting platform should be set up (over 80% of experts were in favor).

At the moment, provisions already regulate the issue of reporting and responsibility for collecting that information under the Act on the National Cyber Security System. There are reasonable suggestions that a platform could help but effective implementation of the current legislation in this area would probably be sufficient. The platform would provide data and knowledge about the type and scale of threats related to cybersecurity and operational risk. The pre-requisite for correct analysis results being provided to interested parties is that the platform should be fed good quality data from its stakeholders and other data providers.

17

EC.CD	Question
Q29	Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools at the country level?Please provide a brief description.

The question gives rise to concerns about the scope and purpose of such tests. If the purpose were to help enhance ICT security of the Organization, the measure is assumed to be reasonable.

Guidelines should be defined for each type of financial institution, setting out:

- the scope of testing
- testing frequency and conditions
- the method and place of reporting on test completion

Hard centralized management of this type of testing may be difficult due to differences between financial institutions (e.g. bank vs non-banking financial intermediaries).

However, the confidentiality of test results raises concerns. This, in turn, suggests that ICT risk management is sufficiently regulated by BCM requirements, therefor, security tests at the national level could, for example, be an option for market participants to enhance their credibility. This role may also be played by periodically completed ICL Risk questionnaires that verify the organization's maturity in terms of security (incident management; information security; infrastructure of network devices).

Most critical organizations should be required to prove that they carry out such tests at their organization level. Participation in national level testing may be voluntary.

An option could also be the scope of selected tests (some tests could, therefore, be selected as mandatory). At the public sector level, it is practically impossible to recruit enough competent people to conduct such tests. The only compromise would be to reduce the quality and scope of testing to a level that would be unreliable due to the complexity of the issue. At the regulatory level, however, the minimum scope of testing should be indicated, based on the adequacy mechanism – adapted to the scope of information processed (client volumes). Initially, three to five levels of test detail could be adopted. Adequacy assessment should be based on a defined key to limit discretion in determining the scope, as was the case with the GDPR implementation.

The method of notifying Supervisory Authorities about the results of completed tests should be regulated, ensuring comparability of those results within the sector.

Financial institutions should be subject to security and resilience tests at the national level in the sense of meeting requirements in this respect, implemented in various forms, but consistent with a jointly developed model/framework. In order to carry out those tasks, the work performed in this respect should be built upon, even if the EU Security Testing Framework TIBER-EU was defined at the level of the European Central Bank. Another example of the testing standard is the CBEST framework launched by the Bank of England, as well as CREST UK solutions which qualify entities, among others, for security testing. IT systems should also be subjected to penetration tests, and the most critical applications, also to source code reviews. The maturity of security processes should be periodically measured through audits. Operational effectiveness should be verified through periodic penetration tests under the „red teaming" approach (e.g. using the TIBER methodology).

18

EC.CD	Question	Rating
Q35	Have you experienced difficulties during contractual negotiations between your organization and any ICT third party providers, specifically with regard to establishing arrangements reflecting the outsourcing requirements of supervisory/regulatory authorities? If so, which specific requirements?	5/16

It should be noted that, in principle, Polish financial institutions have not experienced major difficulties during negotiations between their own organization and any ICT third party provider, especially with regard to the arrangements reflecting supervisory/regulatory outsourcing requirements (only ⅓ of experts mentioned such difficulties). There may be discrepancies in the understanding of the role and definition of outsourcing in relationships with suppliers. The most common problem is negotiation of the supplier's ability to use cloud-based solutions and legal compliance with regard to e.g. a chain of subproviders.

19

EC.CD	Question	Area	Yes
Q37	What is your view on the possibility to introduce an oversight framework for ICT third party providers of financial institutions (country and regional levels)?		
	»	Should an oversight framework be established?	11/18
	»	Should it focus on critical ICT third party providers?	4/18
	»	Should "criticality" of incidents involving third party providers be based on just qualitative and quantitative parameters (thresholds) of risk factors, or also should it include detailed descriptions?	8/18
	»	Should proportionality play a role in the identification of critical ICT third party providers?	5/18
	»	Should other related aspects (e.g. data portability, exit strategies, fair contractual practices, environmental performance, etc.) be included in the oversight framework?	4/18

Experts present quite decisive views on the oversight framework for ICT third party providers of financial institutions (country and regional levels), supporting its emergence. They also indicate that not only ICT providers should be registered on the platform. It is important that the criticality of registered incidents involving third party providers should reflect not just qualitative and quantitative parameters of risk factors (in the form of thresholds), but also detailed descriptions. Considering business secrecy and confidentiality of the business model, it seems reasonable not to register on the platform the proportional share of the supplier as an organization's business partner. For the same reasons, other parameters, such as data portability, exit strategies, fair contractual practices, supplier efficiency, should not be registered on the oversight platform.

20

EC.CD	Question	Area	Yes
Q38	What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers?		
	»	Diversification strategies, including a potential mandatory or voluntary rotation mechanism (e.g. auditing model)	11/18
	»	Mandatory multi-provider approach	4/18
	»	Should limits be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers?	3/18

Diversification strategies, including a mandatory or voluntary supplier rotation mechanism (e.g. audit model), were recognized as the most appropriate and effective solutions to address concentration risk among ICT third party service providers. Less enthusiasm was shown for mandatory use of multiple providers or limits set by the legislator or supervisory authorities to limit the excessive exposure of a financial institution to one ICT third party provider. In the subcontractor relationship model in relation to key business functions implemented as the financial institution's main responsibility, it is necessary to define the approach to basic services: if third parties, such as external ICT providers, are of key importance for the operation of key services. In this case, only the total assignment of risk and liability to the party providing the service ensures some security for the financial institution.

21

EC.CD	Question	Rating
Q39	Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of TTPs and IOCs between financial institutions?	16/18

In this case, the essentially unequivocal view is that the EU should have a role in supporting and promoting the voluntary exchanges of TTPs and IOCs between financial institutions. The question was basically closed, but respondents support voluntary exchange of information.

22

EC.CD	Question	Rating
Q40	Is your organization currently part of such information-sharing arrangements?	7/18

The Polish market is in the first phase of adopting a strategy for building security platform structures, and as may be seen, some institutions are already covered by voluntary exchange of TTPs and IOCs information between financial institutions.

23

EC.CD	Question	Area	Yes
Q45	Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?		
	»	Lack of a common taxonomy on cyber incidents	8/18
	»	Lack of available data on cyber incidents	14/18
	»	Lack of awareness on the importance of cyber/ICT security	10/18
	»	Difficulties in estimating pricing or risk exposures	16/18
	»	Legal uncertainties around the contractual terms and coverage	10/18

Respondents see the lack of data on cyber-incidents as well as the problems and complexity of estimating the cost of exposure to cyber risk and ICT risk as the most important challenges in the development of the market of risk transfers or ICT risk insurance, and in particular cyber-attacks in the region. As in any phenomenon with an unknown or poorly understood and unpredictable structure and course, the greatest uncertainty is associated with the type of risk and with preparedness for risk materialization. One way to mitigate the risk could be to share information via an exchange platform among financial institutions and to simplify application and process architectures of financial organizations.

24

EC.CD	Question	Rating
Q46	Should the EU provide any kind of support to develop EU or national initiatives to promote insurance of ICT risk and risk transfer systems?	14/16

The European Union should support European and national initiatives for insurance against ICT risks. There is a definite view that the role of the European Union in the case of Poland is important in the area of supporting European and even national initiatives in the field of insurance against ICT risks and risk transfer systems. This should be one of the practical elements incentivizing implementation of security measures while enabling cyber risk transfers. Better risk management means lower probability of the risk materializing, a developed ICT risk insurance market and a risk transfer system promote better risk management.

25

EC.CD	Question
Q59	Which of the future or expected specific measures for ICT risk would be completely new for your organization and potentially require the most expenditure in their implementation? Please provide a brief description.

The highest implementation expenditures for future or expected ICT risk solutions will be required for process areas such as stress testing and penetration testing which permit realistic identification of the areas exposed to the greatest risk of incidents as well as monitoring of the efficacy of implemented risk mitigation measures and tools, as well as:

- Reporting to the new risk supervision platform – building control and measurement mechanisms for new regulations
- Mandatory security tests
- Systems for integration and joint reporting will require expenditures and additional recruitment
- Attacks complexity
- Supervision of privileged accounts
- NIS directive updates (especially so-called „construction requirements"). New requirements especially for cloud service providers.
- Cloud solutions
- Open banking
- Lack of adequate supply of human resources
- Process automation
- Replacement of legacy systems (not supported by manufacturers)
- Identity management
- Systems integration
- Purchase of tools to detect attacks and to automate responses to attacks.

As in any company with such a large scale of operations and complexity of operational processes, especially those regulated for financial institutions, the biggest problem is the human factor and problems resulting from mistakes or malicious actions of people from within the organization.

26

EC.CD	Question
Q61	Which administrative formalities or requirements in respect to the ICT risks are today the most burdensome? Which of them require high labor input and cost from an economic point of view? What can be changed in this area? Please provide a brief description.

Particularly difficult or problematic administrative requirements and formalities in the area of ICT risk management are considered to be those that require high labor input and cost from an economic point of view:

- mapping of IT processes and assets, and assigning specific elements of infrastructure and software to the functions performed by the institution, and designating persons responsible for efficacy and efficiency monitoring;
- lack of a developed and uniform partnership culture of cooperation between public and private institutions relying on trust and mutual benefit;
- legal restrictions on sharing knowledge regarding different types of information;
- short incident reporting time, longer reporting time would be better;
- reporting to regulators with no feedback;
- lack of awareness or knowledge about various risk management options and compliance with legal and regulatory requirements. One example is the volume of implementations in the sector of technical tools and technologies (very expensive), which in practice do not achieve their objectives. Such solutions often only satisfy the need to ensure compliance with a given provision, i.e. literal reading of the requirements that a given measure is to be implemented, without saying that the measure needs to be effective;
- in the case of companies of several dozen employees, it is difficult to obtain a correct and functional separation of competences that ensures an actual increase in security while maintaining mutual independence of individual, arbitrarily identified areas;
- requirements for the construction of buildings in the context of the Act on the National Cybersecurity System;
- inclusion of the financial sector in the group of critical infrastructure suppliers.
- lack of developed private-public partnership;
- no requirements as to adequate technological awareness among Board members;
- in practice, public procurement law leads to protracted proceedings which do not select the best security measures;
- recommendation D regarding IT system management – at a time when SI is gaining in significance;
- current reports: quarterly KNF surveys, BION report (annual), reporting on service work to the KNF Office;
- special functionality and service processes: GIIF reporting, MIFID2.

It also seems that the formalities involved in ICT risks registration are a challenge for small teams, in particular in the context of labor input versus resulting benefits.

Effective monitoring and response to cyber attacks is costly for individual institutions. It may be helpful to set up SOC/CSIRT industry teams.

Basing requirements on an enigmatic rule of adequacy, the assessment of which in most organizations is the responsibility of internal and external legal units that do not have the authority to make such a decision (lack of knowledge and experience in the areas of IT/IT Security). As a result, many organizations in the market have mechanisms that do not improve the level of security (there are even those that can harm), but instead make it difficult to introduce changes within the organization. This raises the costs of projects and may force the use of solutions that are not optimal.

In principle, it can be generally said that for mature institutions with an appropriate scale of operation (degree of organizational maturity) administrative requirements and formalities regarding the IT risk management area are not particularly difficult or problematic.

27

EC.CD	Question
Q62	Do you have an estimation of the costs that your company incurred because of ICT incidents, and in particular cyber-attacks? Please provide a brief description.

It is clear that sharing confidential information on estimated costs incurred in connection with ICT operational incidents, in particular cyber attacks, is a problem for respondents. As a rule, they hide behind business secrecy or confidentiality of this very type of information. From the point of view of informational value, such data are of particular importance in designing ICT risk response mechanisms and for the security of financial institution systems. In some cases, institutions (mostly insurance companies) did not estimate the costs associated with ITC incidents due to the fact that the organization is able to survive a relatively long period without access to IT infrastructure, which does not cause financial losses (RTO = nn days), while reducing the RPO time to an acceptable level is easy to obtain due to the scale of the company in both geographical and quantitative terms when it comes to electronic data. There are suggestions that such data, however, do exist in each of the financial institutions because the costs related to ICT operational incidents are mandatorily measured for purposes of operational risk assessment. Rarely, institutions confirm that the risk area has an estimate of the costs (losses) associated with operational risk incidents (including ICT), which is prepared as part of a periodic risk control self-assessment (RCSA) and within defined operational risk scenarios.