NIS implementation challenges in the banking sector

Liliana Apetri

1. Identification of the banking sector on the list of essential services operator

The (EU) Directive 2016/1148 of the European Parliament of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union, was entirely transposed in the Romanian regulation in Law no. 362/2018 on ensuring a high common level of security of computer networks and systems, with subsequent amendments and completion. Based on the Romanian Government Decision no 963/November 05,2020 was approved the list of essential services operators mentioned in the Low 362/2018 and the banking sector is mentioned with the following services: accounts administration, including those related to the activity of attracting deposits and granting loans, Payment services and Investment services.

2. Project Management related to NIS regulation

Project management structures are dependent on the size of the organization and complexity of business/operation.

Project management is the application of knowledge, skills, tools and techniques to a broad range of activities to achieve a stated objective such as meeting the defined user requirements, budget and deadline for the project.

The project management process begins with the project charter and ends with the completion of the project. Project management knowledge and practices are best described in terms of their component processes of initiating, planning, executing, controlling, monitoring, and closing a project.

A project is initiated by a project manager or a sponsor gathering the information required to gain approval for the project to be created. Depending on the size and complexity of the

project and the affected parties the initiation of a project may be achieved by: one-on-one meetings, kick off meeting, project start workshops, a combination of the three.

A project manager should determine in planning the following : scope of the project, various tasks, that need to be performed to produce the expected business application system, sequence or order in which these tasks need to be performed, duration or the time window for each task, IT and non-IT supporting resources that are available and required to perform these tasks, budget or costing for these tasks, source and means of funding for labor, services, materials and plant and equipment resources involved in the project.

Once planning efforts have been completed, it starts the project execution of the planned tasks. The project manager initiates monitoring of the internal team and quality metrics and monitor them. A key success factor is the project oversight of the integrated team in the IT system requirements, architecture, design, development, testing, implementation and transitioning to production operations.

Project controlling and monitoring include management of scope, resource usage and risk. It is important that new requirements for the project be documented and if approved, allocated appropriate resources. Control of change during a project ensures that project is completed in terms of time (it should be taking into considerations the deadlines established but h National Authorities in order to avoid penalties), use of funds and quality objectives.

A project has a finite life and at some point, it must be closed. The project sponsor should be satisfied that the system produced is acceptable and ready for delivery. Hand -off of relevant documentation and duties occur at this stage and the project team and other relevant stakeholder will identify lessons learned from the project.

A post implementation review is completed after the project has been in use for time-long enough to realize its business benefits and costs and measure the project overall success and impact on the business units. Metrics used to quantify the value of the project include return on investment (ROI).

3. Risks faced by the bank related to NIS implementation

Any bank is exposed to the following risk: compliance risk, ICT risk (information and communication technology and security risk), reputational risks.

Compliance risks may affect profits, own funds or liquidity, which may lead to significant financial losses or which may affect the reputation of a bank as a result of a breach or non - compliance with the legal framework and regulations, agreements, best practices or ethical standards applicable to its activities.

The bank may be also affected by the Information and communication technology (ICT) and security risk which means risk of loss due to breach of confidentiality, loss of systems and data integrity, improperness or unavailability systems and data or the inability to change information technology (IT) over a period of time reasonable and at reasonable costs when environmental or business requirements change (agility). This includes security risks arising either from inadequate internal processes or which they have not performed their duties properly, either from external events, including cyber-attacks or inadequate physical security.

The bank should also take into consideration that operational events have a strong impact in terms of reputation.

4. Steps to be followed in the NIS implementation:

- identification of essential services provided by the company based on the Decision of the Romanian Government no 963/November 05, 2020 related to the list of operator's essential services.
- establish of a NIS responsible person and communicates within a maximum of 30 days to CERT-RO, as the competent authority at national level, any change in the data provided in the process of identification as an operator of essential services.
- enrollment notification of the company as essential services operator to the National Authority for Security of Networks and Information's Systems under CERT-RO.

  A service is considered essential if its provision fulfils cumulatively the following conditions:

  (a) The service is essential in supporting societal and/or economic activities of the utmost importance.

  (b) Its supply depends on a network or computer system.

  (c) The provision of the service is significantly disrupted in the event of an incident.

- self-assessment documentation of the fulfillment of the minimum-security requirements.
- statement one's responsibility related to the fulfillment of the minimum security to achieve a high level of security of networks and Information's Systems. Security of networks and Information's Systems means the ability of a network and a computer system to withstand, at a given level of trust, any action that compromises the availability, authenticity, integrity, confidentiality or non-repudiation of stored or transmitted or processed data or related services offered by or accessible by the network or information systems through that network or information systems.
- creation of, or improvement of procedures used to detect, analyze, and limit an incident and respond to it in which should be described mechanisms related to security in the light of evolving threats to the security of networks and information systems. These procedures should be annually updated if necessary, taking into considerations also the internal or external recommendations.

The steps mentioned below are related to incidents reporting process:

(a) implements appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and computer systems used to provide these essential services, in order to ensure the continuity of those services

(b) immediately notify CERT-RO as a national Romania CSIRT of incidents having a significant impact on the continuity of essential services. Notification should also be made when the event is due to some incidents that affect a digital service provider on which the provision of essential services depends. Impact of an incident is decided based on the number of affected users, incident duration and geographical distribution in terms of the area affected by the incident

(c) provide CERT-RO with information enabling the cross-border impact of the incident

(d) interconnects within 60 days from the registration in the Register of essential service operators to the alert and ensures the permanent monitoring of the alerts and requests received through this service or through the other contact modalities and takes into account as soon as possible the appropriate response measures at the level of their own networks and information systems;

(e) Immediately ensures the response to the incidents that occur and restore in the shortest time the operation of the service to the parameters before the incident.

(f) are subject to the control carried out by CERT-RO in order to establish the degree of compliance with their obligations under the law

(g) establish the permanent means of contact, designate those responsible for the security of networks and computer systems responsible for monitoring the means of contact and communicate to CERT-RO within 60 days of registration in the Register of essential service operators their list and any subsequent changes what happened.

(h) communicate within a maximum of 30 days to CERT-RO, as the competent authority at national level, any change in the data provided in the process of identification as an operator of essential services.

Documents that should be provided to CERT-RO annually are:

- the information necessary for the evaluation of the security of the networks and information systems covered by the law, including the documented security policies. The security policy should be approved and assumed by the management.
- the results of the security audit carried out at the request of CERT-RO, including the information and documentation on which it is based, as well as other elements attesting to the effective implementation of the minimum-security requirements.

5. Obligations related to NIS implementation

In order to implement technical measures the following domains should be taken into considerations: governance, protection, cyber defense, resilience.

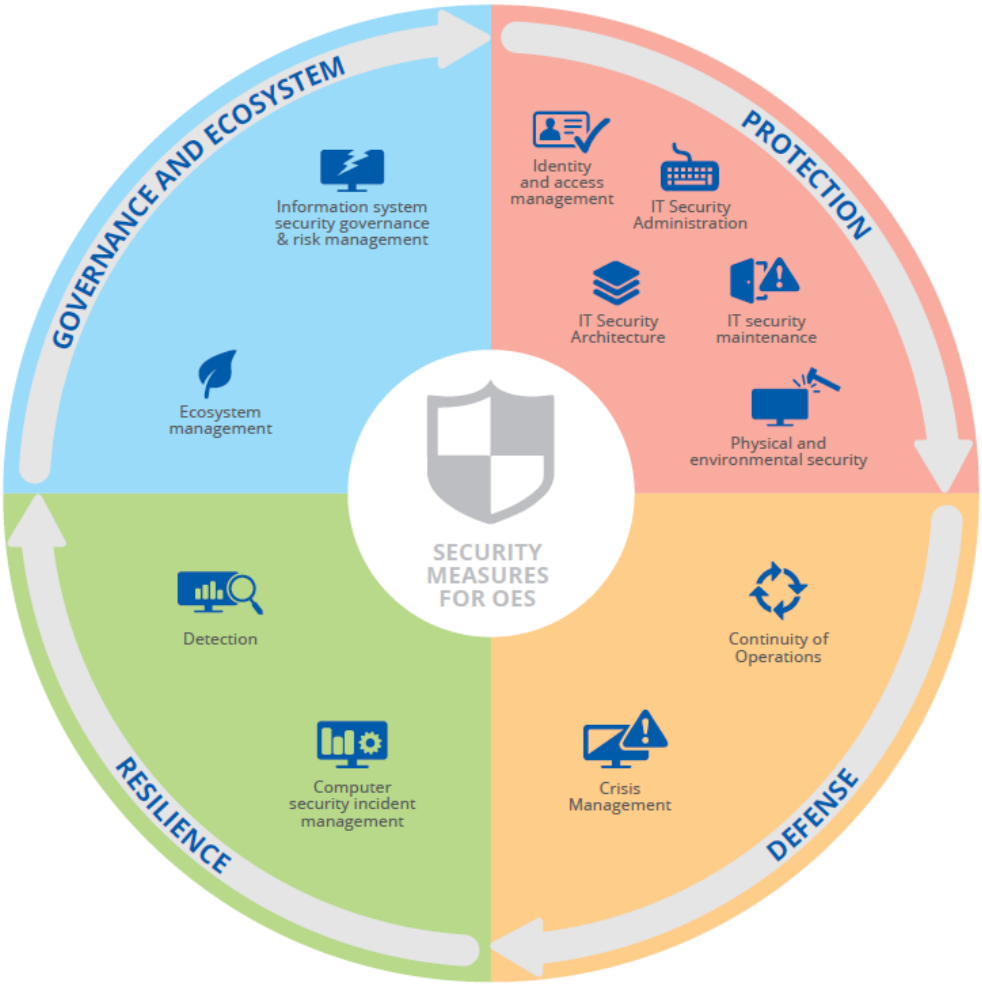

Figure 1: Security Measures for OEs - Source: *ENISA Guidelines on assessing DSP and OES compliance to the NISD security requirements*

The four security areas are also divided into categories of security activities, and for each of them security measures are established with one or more security requirements, which in turn contain control indicators.

We choose to describe below the characteristics of the governance domain.

Governance domain

Governance involves the performance of IT operations, specifically those areas that relates to data its availability, integrity and confidentiality. It contains objectives related to the information system security governance and risk management and ecosystem management.

Information system security governance and risk management relates to the following aspects:

- information system security risk analysis
- information system security policy
- information system security accreditation
- information systems security indicators
- information systems security audit
- human resources security
- asset management

For the *analysis and risk evaluation* it should be established a risk management model for the provision of essential services that will reflect the risk assessment process of the economic operator, the criteria for analysis, acceptance and reduction of risks. The result of risk evaluation should be documented in a risk register. It should include: new threats in cyber security domain, weak points recently discovered, loss of security measures efficiency, modifications made on the system architecture.

Based on the risk analysis which should be annually updated based on the systems/ equipment's that are critical is created an implemented a *security policy*. Information's related to the implementation of the security policy are presented annually in a report which contain risk inventory, level of security of networks and information systems and security actions planned and realized.

The next step related to the governance include the *accreditation of security of networks and information systems*. Accreditation is the official management decision to authorize operation of the information system and to explicitly accept the risk to the operations 's operations, assets or individuals based on the implementation of an agreed -upon set of requirements and security controls. Security accreditation provides a form a QC and challenges managers and technical staff at all levels to implement the most effective security controls possible in an information system, given mission requirements, and technical operational and cost/schedule constraints. Annually or when occur changes related to the modification of security of networks and information systems configuration the essential service operator has the responsibility to revise the security accreditation immediately.

The essential service operator establishes a series of *security indicators* related to the risk management performance, maintaining success in safe conditions, user access rights, authenticating access to resources, resource management. The essential service operator has to identify the modification of the indicator and identify the reasons for this modification.

The essential service operator should perform a security audit at least at 2 years which will end with a report on the security of networks and information systems. The *audit will be conducted by cyber security auditors.*

The testing and evaluation of security of networks and information systems should take into consideration the application security, the security of infrastructures of security of networks and information systems. The results testing should be presented only the persons who need this information.

For *human resources security of* the essential services operators should use the following tools: job description, individual work contract, collective labor agreement. The job description has to contain responsibilities in accordance with tasks performed and the KYC/AML lows and be updated whenever the responsibilities change.

The essential service operator should have a security program for all employees who uses the networks and information systems.

An *asset* is something of either tangible or intangible value that is worth protecting and includes people, information, infrastructures, finances and reputation. An asset cannot be effectively protected or managed if it is not identified. It makes of more difficult to protect an asset if its location is unknown or no owner is assigned reporting. The first step in an IT asset management is the process of identifying and creating an inventory of IT assets. The inventory record of each information asset should include: owner, designated custodian, specific identification of the asset, relative value to the organization, loss implications and recovery priority, location, security /risk classification, asset group.

Developing a list of assets is the first step in classifying and protecting information assets.

The OSE must identity, classify and implement an inventory of IT processes and elements components of networks and information systems. The OSE releases updates and patches and establishes which are the networks and information systems affected by new security problems. For the identification of threats, vulnerabilities and risk the identification of assets, systems and organization processes should be presented on a list. A procedure for the

labeling and classification of information should be in place and the dates/ information should be used accordingly.

Ecosystems management has the following objectives:

- ecosystem mapping
- ecosystem relations

Ecosystem mapping has 4 major parameters: maturity (which are the technical capabilities of the involved parties related to cyber security), trust (reliability of involved parties), level of access of interested parties, and dependency (which are the critical activities for my organization).

The OSE has to elaborate and implement a procedure for the ecosystems relations which include the external relations between the networks and information systems and third parties. In this case agreements with third parties should be established and audit mechanism should be in place related to the supplier compliance with the security mechanisms. A list of this agreements should be kept.

In the figure below are presented the questions and evidence related to the governance and ecosystem and evidence that the IS auditor should obtain.

1.1 INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MANAGEMENT			
S/N	SECURITY MEASURES	QUESTIONS	EVIDENCE
1	Information System Security Risk Analysis	Is the key personnel aware of the main information security risks and the relevant mitigations?	Evidence of personnel attendance to the training (e.g. accepted invitation, date and agenda of training, signed participation list during the awareness workshop etc.).
		Is there a mechanism for ensuring that all security personnel use the risk management methodology and tools?	Guidance for personnel on assessing risks and list of risks and evidence of updates/reviews documented.
		Is the risk management methodology and/or tools, periodically reviewed, taking into account changes and past incidents?	Documentation of the review process and updates of the risk management methodology and/or tools. Time-table and overall plan of the review cycle.
2	Information System Security Policy	Is there an information security policy (ISSP) and an information security management system (ISMS) in place?	Documented ISS policy in place (dated and signed).

		Are there any certifications in place for specific security risk management standards?	Certification against information security risk management standards (for example ISO 27001), including scope statement.
		Are the information security processes reviewed at regular intervals, while taking into account violations, exceptions and incidents which affected other essential operators/ DSP?	Documentation of review process, taking into account changes and past incidents. Time-table and overall plan of the review cycle.
3	Information System Security Accreditation	Have the systems supporting essential services been regularly subjected to security scans and have they been integrated within the risk management framework of the organization?	Reports from past security scans and security tests.
		Are there policy/procedures in place for the performance of security assessments and security testing?	Documented policy/procedures for security assessments and security testing, which at least include: -which assets should be assessed, -under what circumstances, -the type of security assessments and tests, -frequency, -approved parties (internal or external), -confidentiality levels for assessment and -test results and the objectives security assessments and tests.
		Has the effectiveness of policy/procedures for security testing been evaluated?	List of reports about security assessment and security tests.
4	Information System Security Indicators	Are KPIs implemented in systems supporting essential services to be able to assess their effectiveness at all times?	Documentation of KPIs and mapping with the Critical Information System in which they are implemented.
		Are there any policy/procedures in place for the implementation of security indicators for testing the systems supporting essential services?	Policy/procedures for testing critical information systems, including when tests must be carried out, test plans, test cases, test report templates, desired KPI values.
		Are the aforementioned policy/procedures reviewed and updated?	Updated policy/procedures for testing critical information systems, review comments, and/or change logs.
5	Information System Security Audit	Is there an updated policy and/ or procedure for performing information system security assessments and audits of systems and assets supporting essential services?	Information security audit policy and/ or procedures, formally documented and regularly maintained.
6	Human Resource Security	Are the professional references of key personnel (system administrators, security officers, guards, et cetera) validated?	Documentation of checks of professional references for key personnel.
		Is training material on security issues provided to key personnel?	Evidence of personnel attendance to the training (e.g. Accepted invitation, date and agenda of training,

			signed participation list during the awareness workshop etc.)
		Is key personnel formally appointed in necessary security roles?	• List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles. • Organization's organigram in place, job descriptions signed by key personnel, relevant role trainings attended.
		Are the policies/procedures for the Human Resource security regularly reviewed and updated, taking into account possible changes?	• Comments or change logs of the policy/procedures. • Review time-plan versions of the policies/ procedures providing the changes that took place.
7	Asset Management	Are lists of critical assets and configurations of systems supporting essential services maintained?	Lists of centrally managed critical assets and critical system configurations managed and maintained.
		Is there a policy/procedures in place for asset management configuration control?	Documented policy/procedures for asset management, including roles, responsibilities, assets and configurations that are subject to the policy along with the objectives of the asset management
		Is the asset management policy regularly updated, based on changes and past incidents?	Up to date asset management policy/procedures, review comments and/or change logs.
1.2 ECOSYSTEM MANAGEMENT			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Ecosystem Mapping	Are the contract relationships with third parties properly documented and listed?	Lists of all contracts with third-parties
2	Ecosystem Relations	Are the security requirements included in the contracts with third parties?	Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks etc.
		Is a security policy for third parties in place?	Documented security policy for contracts with third parties.
		Is the security policy for third parties reviewed following incidents or changes?	Documented comments or change logs of the policy.
		Are there any residual risks associated to third parties and their services not addressed/mitigated?	• Vendor Risk Assessment/ Management policy/ procedure in place and maintained. • Documented amendment or termination of relationships with high-risk third parties.
		Is a periodic review and update performed to the security policy of third parties, taking into account past incidents, changes, etc.?	Documentation of review process of the ecosystem relations policy.

Figure 2: Governance aspects to take into account - Source: *ENISA Guidelines on assessing DSP and OES compliance to the NISD security requirements*

6. Costs related to the NIS Implementation

The implementation of NIS may involve expenditures for example: the acquisition of external audit services performed by CERT RO certified auditors at least at 2 years.

Costs on a longer period may be related to compliance with asset management, systems patching, maintenance, cost with personnel in order to ensure security, outsourcing of CSIRT (computer security incident response team) services on a certificated center or assurance and certification of an intern CSIRT.

According to the ENISA NIS Investment Report from December 2020, while low levels of investments cannot be sustained without adverse impact on the information security readiness, higher spending does not necessarily correlate with an associated improved maturity.

The below figure presents the Dedicated NIS Directive budget per sector

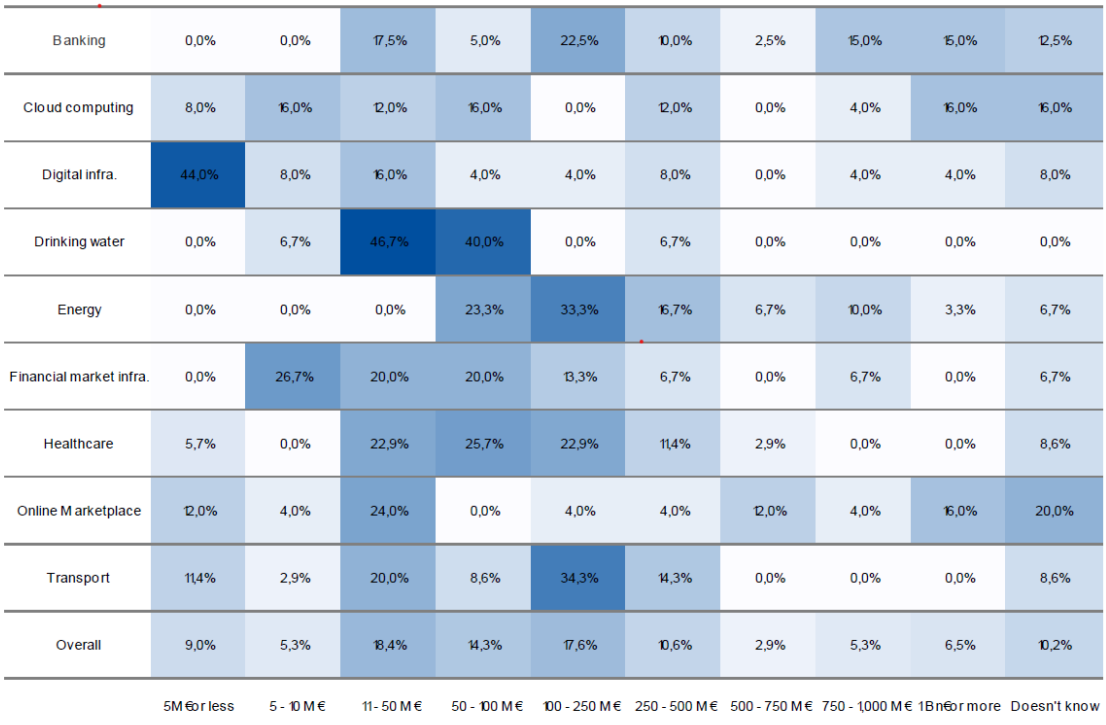

Figure 3: NIS implementation investment - Source: *ENISA -NIS Investment Report December 2020*

7. Benefits that may came with the NIS implementation

The following benefits can be achieved from the NIS implementation:

- Processes improvements on assuring information security and the information system for the provision of essential services, administration of current accounts and payment services.
- Compliance with National and European regulatory requirements and avoiding sanctions from competent Authorities at National level.
- Fulfillment of legal and reporting requirements.

Bibliography:

The above mentioned articles was made taking into consideration the (EU) Directive 2016/1148, Romanian Law no. 362/2018 , Order no 1323/2020 from November 9, 2020 related to the approval of Technical Rules on minimum requirements to ensure the security of the networks and information systems applicable to essential services operators , ENISA -NIS Investment Report December 2020, CISA Manual, Guidelines on assessing DSP and OES compliance to the NISD security requirements and the auditor experience.