TECHNICAL ASSISTANCE REPORT

GEORGIA

Cyber Risk: Regulation, Supervision and Testing

December 2024

Prepared By
Emran Islam, Rangachary Ravikumar and Michelle Monsees

Authoring Departments:

Monetary and Capital Markets

The analysis and policy considerations expressed in this publication are those of Monetary and Capital Markets department.

International Monetary Fund, IMF Publications
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430 • F. +(1) 202.623.7201
publications@IMF.org
IMF.org/pubs

Contents

Figures

Tables

Annexes

Acronyms and Abbreviations

CISS	Critical Information Systems Subject
CISO	Chief Information Security Officer
DGA	LEPL Digital Governance Agency, Ministry of Justice of Georgia
D-SIBs	Domestic Systemically Important Banks
FSSC	Financial Sector Supervisory Committee
GRAPE	General Risk Assessment Program
IMF	International Monetary Fund
MCM	Monetary and Capital Markets Department
NBG	National Bank of Georgia
ORMG	Operational Risk Management Guideline
PPP	Public Private Partnership
PT	Penetration Tests
TA	Technical Assistance

Preface

At the request of the National Bank of Georgia (NBG) to help enhance Georgia's cyber risk regulation, supervision and testing framework, a Monetary and Capital Markets (MCM) Department technical assistance (TA) mission visited Tbilisi, Georgia during June 24 - 28, 2024. The mission focused on (i) an assessment of NBG's cyber risk regulation, (ii) an assessment of cyber risk supervisory arrangements of NBG, (iii) assisting in the development of a cyber testing framework, and (iv) assisting in the development of a methodology for cyber exercising and stress testing.

The mission had met with Aleksandre Ergeshidze, Head, Specialized Risks Department, Nanuli Chkhaidze, Head of Cyber Risk Supervision Division and her team. In addition, the mission met with other departments within the NBG, select banks and representatives of the Banking Association of Georgia.

This report presents the mission's assessment and main conclusions. The mission thanks the senior management of the NBG and the officials for their excellent cooperation and productive discussions.

Executive Summary

At the request of the National Bank of Georgia (NBG), an MCM technical assistance mission aided in strengthening their cyber risk regulation and supervision, and testing. Georgia's financial sector is bank-dominated, and three large banks account for the majority of financial sector assets. The institutional arrangement for Information and cybersecurity is governed by the Information Security Act, 2021, national cybersecurity strategy Computer Emergency Response Team and focus on critical information systems subject (CISS). The NBG has taken certain steps, like amending the law, introducing cyber incident reporting, and issuing cloud outsourcing guideline, in line with recommendations made as part of the recent FSAP assessment.

Cyber risk regulations including incident reporting requirements are in place, but gaps remain. The NBG has not formulated a financial sector focused cybersecurity strategy. Cyber risk regulation does not cover ICT aspects and even for cyber risk there are certain gaps regarding governance, risk management and testing arrangements. It is necessary to develop a new regulation after consulting the industry and require periodic gap assessments as one of the requirements. The timelines for compliance need to be proportional considering varying levels of preparedness among banks. The NBG should conduct outreach sessions with the Board and the senior management of banks to sensitize them on cybersecurity matters.

Cyber risk supervision practices need improvements and focus more on supervisory priorities. The cyber risk supervision team should be augmented with 2 to 3 additional staff to strengthen supervisory effectiveness. Developing a supervisory manual is a priority to achieve consistent outcomes from onsite examinations. Leveraging technology, offsite supervision activities need to be strengthened. Forming a working group with participation from the supervisory policy department will help in achieving better outcomes in the development of regulations.

Information sharing practices within the financial sector require strengthening and further clarification is required in terms of incident reporting. While information sharing in a limited way is already in place, steps need to be taken to make it a systematic process. Existing arrangements within the DGA or the Banking Association could be leveraged for this purpose, which promote public private partnership (PPP). Providing regulatory clarity in terms of classifying cyber incidents will bring about consistent outcomes.

Cyber testing and exercises are an area where significant improvements are needed. Current regulatory requirements on testing and supervisory practices of conducting exercises leave scope for improvement as it lacks coverage on vulnerability scans, testing arrangements, remediation etc. Considering the varying levels of preparedness and resources among banks, development of a comprehensive testing framework will help in strengthening cyber preparedness of the financial sector.

Recommendations

Number	Recommendation	Reference Paragraph(s)	Priority1
Cyber Risk Regulation and Supervision			
1.1	Develop a financial sector focused cybersecurity strategy incorporating key elements with an outlook for 3 to 5 years	14	MT
1.2	Revise and update the cyber risk management regulation by addressing gaps and converting it into a technology risk management guideline	15	MT
1.3	Consult the industry before finalizing the regulation	16	NT
1.4	Require a gap assessment within six months of issuing the regulation along with a road map for implementation with milestones and timelines.	16	MT
1.5	Provide a differentiated timeline for full implementation by prioritizing implementation among top 3 banks followed by longer timeline for other banks	16	NT
1.6	Sensitize the Board and the senior management of banks by conducting outreach programs to explain the rationale, expectations and provisions of the revised regulation.	17	MT
1.7	Develop a supervisory manual based on the Toolkit shared and aligned with the proposed regulation	28	MT
1.8	Review the activities carried out by the cyber risk supervision team and streamline the processes to ensure primacy for supervision activities	27	NT
1.9	Augment the compliment of staff in the cyber risk supervision team by inducting two to three generalist supervisors with exposure on assessing governance and risk management aspects.	25	NT

[1] Near term(NT): < 12 months; Medium term(MT): 12 to 24 months; Long term(LT): > 24 months.

1.10	Ensure independent quality assurance of supervisory reports before its finalization.	25	NT
1.11	Expand the scope of supervision activities in alignment with the revised regulation and ensuring the same team assess ICT and Cyber risks.	27	MT
1.12	Constitute a small working group drawing members from supervisory policy department to develop the new regulation and comprehensive testing framework.	26	NT
1.13	Consider setting up a Standing Committee on Cyber to better harness cybersecurity skills available within the NBG	26	MT
Cyber Testing, Exercises, Stress Testing			
2.1	Develop a comprehensive testing framework with a suite of possible tests, scenarios, processes, and expected outcomes that could be applied proportionally	38	MT
2.2	Encourage the financial sector to voluntarily share information among themselves by leveraging the PPP working group and / or the Banking Association.	39	NT
2.3	Collaborate with the industry to develop information sharing protocols and frameworks and play a catalyst role.	39	MT
2.4	Strengthen the cyber incident reporting framework by clearly defining severity of incidents and incorporating the recommendations of the cyber incident reporting framework	40	NT

I. Cyber Risk Regulation and Supervision

A. Background

1. Georgia has strengthened its legal and institutional arrangements for cybersecurity in recent times. The Information Security Act (ISA) of 2012 has been amended in 2021 grouping the CISS into three categories (Tier 1: state agencies, institutions, LEPLs[2] (other than religious organizations) and state enterprises; Tier 2: – electronic communication companies; and Tier 3: banks, financial institutions, and other entities of private law) and designating the LEPL Operating Technical Agency (OTA, under the State Security Service of Georgia) for the first two tiers and the LEPL Digital Governance Agency (DGA) for the third tier as responsible agencies. The Information Security Act of Georgia 2021 also lays out penalties that could be levied for serious and persistent non-compliance as well as the need for accreditation of agencies that conduct information security audits and penetration tests. The Georgia CERT, under the DGA, is responsible for responding to cyber incidents, gathering, and providing threat intelligence and increasing cybersecurity preparedness among all CISSs.

2. Georgia has been publishing National Cybersecurity Strategies and the third such strategy for the years 2021-24 has been published. The first strategy covered the year 2013-15 followed by the second strategy for the years 2017-18. The third strategy has four goals and ten objectives as indicated in Table 1.

Table 1 – National Cybersecurity Strategy – 2021-24

Goals	Objectives
Bolster the development of cyberculture among information society and organizations, to support resilience to threats and incidents in cyberspace	Ensure school pupils' and students' safe and secure functionality in cyberspace by developing necessary skills and raising the level of education among them
	Raise awareness among information society and organizations to ensure their safe and secure functionality in cyberspace
Sustainability of cybersecurity governance system and enhancement of the public-private cooperation	Create and develop a national-level system to timely identify, report and effectively respond to cyber incidents and cyber threats
	Develop an effective system to combat cybercrime
	Provide support in enhancing information sharing on modern trends and best practices available for treating cyber threats and implementing international standards through established communication platforms

[2] Legal Entities of Public Law

Strengthening cyber capabilities and development of strong cyber workforce	Increase the level of knowledge and qualification of experts representing cybersecurity industry
	Strengthen the national cyber capabilities through the means of technical provision
Strengthen Georgia's position as a net contributor to international cyber security at an international scale	Strengthen international support/co-operation in particular to support information sharing about threats and incidents
	Participate in international cybersecurity trainings and exercises, and share knowledge and experience to contribute to the global cybersecurity agenda
	Strengthen bilateral and multilateral international partnerships

The NBG has been entrusted with implementing certain aspects of the objectives with reference to the financial sector.

3. The NBG itself is identified as a CISS under Category I under the oversight of the OTA The NBG also has the responsibility to identify and recommend CISS within the financial sector to the DGA under Category III. The NBG has identified three domestic – systemically important banks (DSIBs) as Category III so far. The DGA has been designated as the responsible agency for the Category III (CIIIs), and hence there is an apparent overlap of responsibilities between the NBG (as prudential supervisor) and the DGA. None of the other institutions supervised by the NBG have been identified as CIII and hence are not overseen by the DGA.

4. Georgia's financial sector is dominated by banks, which account for 96% of the financial sector assets. Three DSIBs account for the major portion of the assets. Smaller banks face resource constraints in implementing cybersecurity risk management regulation.

5. In the recently conducted FSAP assessment, a desk-based review of cyber risk regulation and supervision produced some recommendations. A summary of recommendations and actions taken by NBG is given in Table 2.

Table 2 – FSAP recommendations on cyber risk and action taken

FSAP Observations	Action Taken
The key role of the NBG in declaring a bank or financial infrastructure as a critical information system should be well articulated in the amendments to the law on information security.	The law has since been amended. The NBG has been given powers to identify CIII within the financial sector. Once declared as CIII, such

	entities fall under the oversight of the DGA as well.
Given limited staff resources in charge of cyber risk, the NBG is advised to strengthen the offsite framework for cyber risk supervision and automate the compliance monitoring process. The initiatives taken by the authorities to automate incident reporting and information sharing mechanism are welcome.	Cyber incident reporting framework has been put in place. Two types of reports are collected – one is detailed report on major incidents and the other is a summary report covering all incidents. Other off-site supervision activities are limited and there is potential to leverage technology in strengthening off-site supervision.
The NBG is encouraged to articulate the information / cybersecurity baselines for the use of cloud (including for hosting core banking system), and continuously monitor compliance.	Cloud outsourcing guideline has since been issued.
It would be also useful to enhance the frequency and sophistication for cyber preparedness testing exercises in the short term and develop a testing framework strategy in the medium term.	Current TA is to address this.
Having in place an arrangement for rotating external auditors assessing cyber preparedness or conducting penetration tests, and periodically reviewing the quality of such audit reports would further enhance the utility of such exercises.	Information systems and cybersecurity management audit guideline for commercial banks issued in 2022.

6. An earlier technical assistance (TA) mission assisted the cyber risk supervision team in building capacity. In the year 2023, a virtual TA mission delivered several sessions on cybersecurity covering both regulatory as well as supervisory aspects. Discussion of select case studies facilitated reinforcement of learnings.

B. Cyber Risk Regulation

B.1 Assessment

7. The National Bank of Georgia (NBG) has issued regulations covering cybersecurity management framework to commercial banks. ICT is covered under “Regulation of the National Bank of Georgia on the Management of Operational Risks at Commercial Banks (Operational Risk

Management Guideline or ORMG)" issued in 2014 and cyber risks are covered under "Regulation of the National Bank of Georgia on Cybersecurity Management Framework of Commercial Banks" issued in 2019. Rules for exchanging information about operational risk events issued in June 2023 facilitate information sharing among commercial and micro banks. The NBG also has issued the Guideline for the Use of the Cloud Outsourcing Services by the Financial Organizations (Cloud guidelines) in August 2023. The Audit Manual for Information Systems and Cyber Security Management Framework in Commercial Banks issued in May 2022 defines the requirements for the audit ('audit') process of information systems and cybersecurity management in commercial banks, the competence, impartiality and operation of the information systems and cybersecurity management framework in commercial banks. A summary table of extant regulations is given in Annex-2.

8. The NBG has issued regulations covering cyber risk management framework and audit manual to micro banks. In the year 2023, the NBG issued the cyber risk management framework regulation along with the audit manual to micro banks mandating baseline requirements.

9. Cyber risk regulation do not currently apply to supervised entities other than commercial and micro banks. In terms of applicability of cybersecurity regulations, currently these apply only to commercial banks and micro banks and all other supervised entities are not covered by the scope of application.

10. The DGA's remit extends to the three DSIBs and their regulatory expectations are based on ISO 27000 family of Standards whereas the regulation issued by the NBG is based on the NIST framework. The DGA is responsible for monitoring the cybersecurity preparedness of Category III (CIIIs) across sectors as per ISA 2021 – including the three DSIBs supervised by the NBG. There are separate audit requirements by both authorities and the difference in their respective regulatory approaches pose challenges to these DSIBs in terms of compliance. The DGA is also operating the Georgia CERT and provides threat intelligence and assistance in dealing with cyber incidents. The DGA does not have remit on banks other than the designated DSIBs and as such does not provide threat intelligence and incident handling assistance to these banks.

11. The mission reviewed the extant regulation vis-à-vis the model regulation developed as part of the cyber risk supervision toolkit and shared the findings with the authorities. Taking into account the recent updates of the NIST cybersecurity framework, ISO 27001:2022 and DORA, it would be important for the NBG to update its existing regulation and bringing it closer to international best practice standards. The cybersecurity management framework regulation should address ICT aspects and also cyber risk. Many regulators have issued a comprehensive technology risk management guideline factoring both ICT and cyber risk matters and do not directly mention any standard / framework. The review comments provided are given in Annex-1.

B.2 Recommendations

12. The NBG should develop a well-articulated cybersecurity strategy for the financial sector. The National Cybersecurity Strategy issued by the Government prioritizes a set of actions for the country as a whole. The role of the NBG in implementing the action plans under the strategy is rather limited and mostly in the capacity of a partner. A financial sector focused cybersecurity strategy could help in articulating the goals and objectives of the NBG for the next three to five years and might provide a clear

direction to the financial sector. The mission recommends the development of a financial sector cybersecurity strategy considering key components of a robust cybersecurity framework, duly approved by the top management of the NBG.

13. There are several factors that warrant development of a comprehensive technology risk management guideline in the near term. The extant regulation does not address ICT issues in detail, there are gaps as regards cybersecurity aspects and the current approach of leveraging NIST standards explicitly poses challenges to the supervised entities in terms of compliance, particularly in the light of the DGA's regulatory expectations based on ISO standards. Governance and risk management components in the regulation needs to improve. Having said this, although the extant regulation does not specify that all financial institutions are subject to cybersecurity management framework, the NBG does "indirectly" supervise them in terms of the online identification and verification of clients, implementation of which must be agreed with NBG. Another example is when the institution wants to join the open banking and submits a request to the NBG, there are minimal security requirements that are imposed.

14. It is important to engage with the industry in developing the new regulation and recognize differences in the levels of preparedness of large banks vis-à-vis smaller banks and banks and non-banks. The NBG needs to consult the financial sector while finalizing the revised regulation thereby providing an opportunity to the industry to provide their insights and to gain their commitment. The meetings with banks as well as Banking Association indicated that the levels of preparedness among large and other banks differ significantly marked by resource constraints. It is a good practice to require a gap assessment from the financial sector participants along with a road map for full implementation with milestones and timelines. The NBG needs to provide a differentiated timeline for gap assessments as well as full implementation based on the size, complexity, interconnectedness, and systemic relevance of institutions.

15. Cyber risk has become critical for the financial sector and Boards and senior management need to play an active role in its management. The NBG has a role in sensitizing the Boards of supervised entities. It is therefore necessary to sensitize the Board and the senior management of banks and other supervised entities by conducting outreach programs to explain the rationale, expectations, and provisions of the revised regulation immediately after its finalization. This will contribute to Boards playing an active role in strengthening the cyber preparedness of not only the institutions but also the sector as whole.

C. Cyber Risk Supervision

C.1 Assessment

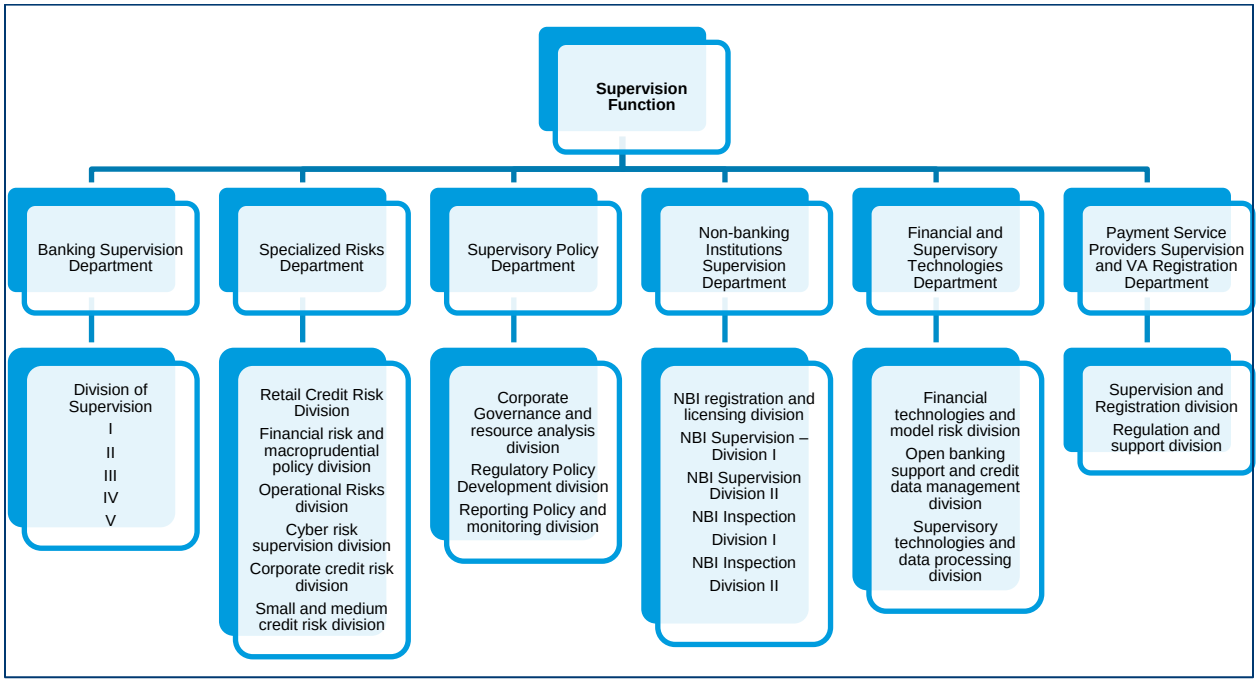
16. The NBG prepares and publishes supervisory strategies setting out strategic priorities. The current strategy is for 2023-25. The NBG has identified five high level strategic priorities for 2023-25, which are further broken down into action plans with timelines and milestones. The supervisory strategy apparently is developed in a bottom-up approach considering the priorities of various supervisory functions and aggregating them. Actions plans include cybersecurity related items as well. The strategic priorities are given in Table-3.

Table 3: STRATEGIC PRIORITIES FOR 2023-2025

1. IMPROVEMENT OF FINANCIAL SECTOR RISK MANAGEMENT FRAMEWORK AND PROACTIVE RESPONSE TO OUTCOMES 2. PROMOTION OF COMPETITION IN THE FINANCIAL SECTOR 3. PROMOTION OF FINANCIAL INNOVATION AND DEVELOPMENT OF SUPERVISORY TECHNOLOGIES 4. APPROXIMATION TO INTERNATIONAL STANDARDS 5. STRENGTHENING THE SUPERVISORY FUNCTION OF THE NATIONAL BANK AND INCREASING TRANSPARENCY

17. Banking supervision is organized as vertical as well as horizontal functions and the cyber risk supervision team is part of the horizontal function under the specialized risks department. The organization structure of the supervision function is given in Figure 1. The vertical function handled by banking supervision department has a staff compliment of 32, with a potential to increase it to 40 eventually. The horizontal function handled by the specialized risks department has a staff compliment of about 30. The operational risk division and cyber risk supervision division work collaboratively as their work areas overlap.

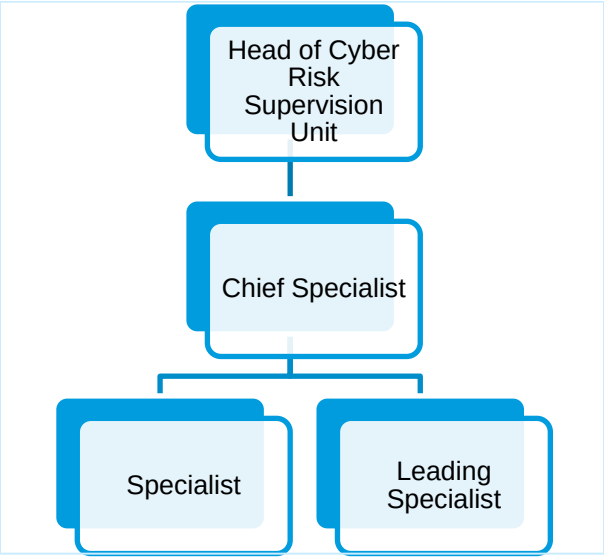
Figure 1 – Organization Structure of Supervision Function



18. The cyber risk supervision unit currently has four staff members, and the organization structure as well as work areas attended by the unit is given in Figure 2. The unit is scheduled to conduct one onsite examination this year. About 30% of the unit's time is spent on product reviews and approvals/no objection. One resource is dedicated to managing cyber incident reporting. Another resource is primarily focused on keeping the registry of products (from initiation to no objection/approval) and analyzing the submitted products (new or changed ones). The licensing applications from digital banks and micro banks

are maintained by the third team member as well as analyzing the penetration test reports. Governance and risk management aspects are generally handled by the unit head, as other resources are technical resources focused on a narrower work area. Banks and Micro Banks are allocated among the team members with all the DSIBs falling under the responsibility of the unit head.

Figure 2 – Organization Structure of Cyber Risk Supervision Unit and Work Areas



Work Areas attended to:

- Onsite and offsite supervision of cyber risk
- Product approvals/ no objection
- Licensing of digital banks, etc.
- Outsourcing – Cloud arrangements
- Cyber incidents
- External Audit reports
- Pen Test reports
- Policy formulation
- Coordination with operational risk division
- Coordination with DGA

19. Onsite examination is conducted in collaboration with the operational risk division and contains usual steps. As a practice, onsite examinations are planned in agreement with the vertical function. A questionnaire is sent for gathering pre-examination information about six weeks prior to the examination. The information is then analyzed to identify high risk areas and prepare a risk profile. Onsite visits are carried out by all the four members of the unit, typically for a week. The examination is focused on operational risk aspects as well as cyber risk aspects and hence conducted by a joint team drawn from operational risk and cyber risk units. The examination report contains two sections – one focused on operational risk and the other focused on cyber risk. The supervisory action plan is agreed upon and followed up. The team also is supplemented by an examiner from the vertical function.

20. Quality assurance of the examination reports is handled by the same team and needs additional independent review. The examination reports are finalized by the examination team. As the entire team gets involved in the examination processes as well as onsite visit, quality assurance activities are rather weak with a lack of independence. The report is seen by the horizontal function head – i.e., head of specialized risks department – but more from an overall perspective.

21. The cyber risk examination process is not supported by a supervisory manual. The examination team assesses various aspects of cyber risk management based on individual experiences and collective wisdom. There is no supervision manual developed for this work area.

22. The Financial Sector Supervisory Committee (FSSC) is headed by the Governor and the Vice Governor and departmental heads are members. The Board of the NBG does not directly get involved in Banking Supervision as per the legal mandate. The supervision function is headed by a Vice

Governor, who reports to the Governor. Major changes in the regulations and supervisory arrangements are overseen by the FSSC. However, there are no standard cyber agenda items or reports covering threat landscape, major incidents, progress in implementing the regulation, major supervisory findings and cyber awareness of the sector that go to the senior management leading to supervisory priorities being fixed more on a bottom-up approach.

23. Cyber risk assessment is integrated with the overall risk assessment through General Risk Assessment Program (GRAPE) framework and operational risk and cyber risk together is given a weight of 5%. The outcome of the examinations carried out are factored while scoring the operational risk and cyber risk elements as part of the GRAPE framework. This is done in consultation with banking supervision divisions – a vertical function. The discussion with the team indicates that this is a high priority work.

24. Offsite supervision activities and use of technology within the supervision activities are rather limited. Currently offsite information processed by the unit include one off collection of cybersecurity strategies, data relating to compliance with cloud outsourcing guidelines, pen test reports, audit reports, product review related information and some inputs from the operational risk division. There is an ISAC portal for reporting the cyber and operational incidents from commercial and digital banks. MISP is another instance, in testing mode, where systemic banks share technical details about cyber threats. The unit does not collect information on key risk indicators or gap assessment with reference to regulations and currently does not have dashboards or digital risk profiles prepared for the supervised entities, which could be very useful for the senior management. Further, the incident reports are facilitated by the Fintech unit using some Suptech solution – primarily leveraging Tableau for visualization. There is an opportunity to look afresh in leveraging technology to further strengthen the supervisory function more meaningfully.

C.2 Recommendations

25. There is an urgent need to augment the current composition (e.g., 2-3 extra staff members) and complement of staff in the cyber risk supervision team. Given the work areas attended to by the team, the current complement of staff is inadequate. The composition of the team also leaves scope for improvement as there is a need to augment the team by inducting two to three generalist supervisors with exposure on assessing governance and risk management aspects. The Unit Head is currently engaged in assessing all governance and risk management aspects relating to cyber as other team members are technical staff, responsible for all the three D-SIBs, and heads each of the cyber risk examinations leaving little time to focus on policy development, staff capacity building and quality assurance. The activities arising on account of the current TA also is expected to demand quality time from the team over short to medium term. There is a need to strengthen the quality assurance process by ensuring independence of the function.

26. Constituting a small working group with participation from the policy development unit will assist in developing the new regulation as well as testing frameworks. Developing regulation and testing framework benefits from a collegial approach and forming a small working group with representatives from the Supervisory Policy Department will help achieve better results. To harness the cybersecurity expertise available within the NBG, the authorities may also consider constituting a Standing Committee on Cybersecurity drawing members from other supervisory units and Payment System, Internal Security,

IT, and Risk Management departments to discuss issues relating to the emerging threat landscape, technological developments, supervisory tools that could be used and policy approach. Such an arrangement will bring the available expertise in a single forum and contribute to further strengthening of cybersecurity both within the NBG and in the financial sector.

27. The cyber risk supervision team carries out multiple activities and there is a need to review the activities to ensure primacy for supervision activities. Work areas attended to by the team (Fig-2) are many and some of the activities like product approvals/no objection, licensing and incident reporting consume significant supervisory attention. This has an impact on the frequency and quality of onsite and offsite supervision activities. New regulation when developed will demand aligning the supervisory activities and increase the scope to ICT and cyber risks.

28. Developing a supervisory manual based on the Toolkit shared and aligning with the proposed regulation will contribute to strengthening cyber risk supervision. It is important to develop a supervisory manual in alignment with the proposed regulation to ensure supervisory consistency. It will also help new staff joining the team to get suitable guidance in carrying out various supervisory activities.

II. Testing, Exercises and Stress Testing

D. Testing, Exercises, Information Sharing and Incident Reporting

D.1 Assessment

29. The desk-based review of cyber regulation and supervision as part of the recent FSAP assessment recommended developing a testing framework. The recommendation mentioned that it would be useful to enhance the frequency and sophistication for cyber preparedness testing exercises in the short term and develop a testing framework strategy in the medium term. The NBG requested the current TA keeping this recommendation in mind.

30. The current regulation requires banks to carry out penetration tests (PT) on an annual basis and share the reports with the cyber risk supervision team, upon their request. In terms of Article 8 of the cybersecurity framework regulation, (i) management of the banks is obliged to regularly check the efficiency of the organization's cyber security / information security program, (ii) the organization shall conduct annual self-assessment of cyber security, (iii) the banks shall conduct a penetration test at least once a year, which includes all the information systems of the bank that are connected to the network and (iv) the commercial bank shall conduct an annual independent audit of all components of the Bank's Cyber Security Management Framework. The information security audit must include risks associated with confidentiality, integrity and availability of systems.

31. PT reports and Audit reports are reviewed by the cyber risk supervision team and critical findings are followed up with the banks. Two of the staff are dedicated to reviewing the PT and Audit reports and such reviews focus significantly on technical aspects.

32. The NBG usually does not conduct cyber exercises. However, it has coordinated such exercises with other local or foreign agencies. Recently, the Banking association, NBG, commercial banks and DGA took part in such exercise organized by USAID CIDR program. Similarly, 5 years ago, the World Bank also organized an exercise for the NBG and commercial banks. Bankers Association also mentioned that they conduct cyber exercises periodically considering realistic scenarios.

33. DSIBs mentioned that they conduct red team testing – a form of threat intelligence-based testing – periodically and such exercises are useful in strengthening their defensive capabilities. DSIBs, however, indicated that skillsets for conducting such testing exercises is limited within Georgia and the DGA requires such testers to be accredited before they conduct such exercises. The smaller banks are not yet ready for such advanced testing frameworks. Banks in their meeting with the mission team conveyed that exercises and tests are more useful for cyber preparedness and provide deeper insights.

34. As part of the mission, the mission team made a detailed presentation on ‘Testing and Exercising’ sharing international best practices. The presentation covered various types of testing that could help in strengthening cyber preparedness of the financial sector including vulnerability scanning, penetration testing, scenario-based testing – market-wide, desktop, simulations and crisis management, and red team testing. The presentation also covered a few examples across various types of testing.

35. Information sharing practices in the financial sector gives scope for further improvement. Currently, the three DSIBs have access to the information shared through the MISP platform. Smaller banks do not get access to this resource. Similarly, threat intelligence sharing, and specific inputs shared by the DGA is available only for the three largest banks. Three DSIBs indicated that they do share information among themselves but are not keen in sharing information with other banks citing lack of reciprocity and costs involved as the reasons. Currently, the CISO forum is not active in the jurisdiction.

36. The Banking Association as well as the DGA mentioned certain forums run by them, which could be a potential candidate for facilitating information sharing among banks. The DGA runs a Public-Private Partnership (PPP) platform with members in their individual capacities who are capable and willing to contribute to strengthening cybersecurity in the country. Banking Association on the other hand mentioned that they have earned the trust of the member banks and are able to run CISO forums or any other form of information sharing initiatives. Both the options offer an opportunity to further strengthen the information sharing initiatives.

37. Incident reporting requirements established by the NBG has prescribed a reporting template and expects banks to define the category of the incidents themselves. The reporting template is informative and compares well with industry best practices. However, requiring banks to categorize incidents gives discretion to banks having potential to inconsistent classifications across banks. Banks suggested that clear definitions by the NBG could be of help.

D.2 Recommendations

38. Current regulatory requirements on testing and exercises are limited and there is a need to develop a comprehensive testing framework with a suite of possible tests, scenarios, processes, and expected outcomes that could be applied proportionally. The NBG and banks realize the importance of testing and exercises and are eager to strengthen the practices. One of the common themes during the discussion is how three DSIBs and rest of the banks differ in terms of financial, technical, and human resources. Thus, considering proportionality becomes a key element. By developing a comprehensive framework, banks could choose right kind of tests and exercises to suit their needs.

39. It is important for the NBG to play a catalyst role in encouraging the financial sector to voluntarily share information among themselves by leveraging the PPP working group and / or the Banking Association. The banks, the Banking Association and the DGA recognize the importance of information sharing as well as challenges in doing so. The smaller banks are craving for such an initiative. The NBG needs to develop an information sharing protocol and without directly participating in such initiatives, encourage the regulated entities in voluntarily sharing information.

40. There is a need to strengthen the cyber incident reporting framework by clearly defining severity of incidents and incorporating the recommendations of the FSB's cyber incident reporting framework. The incident reporting template is fit for purpose but regulatory clarification on classification of incidents will improve the consistency of reporting by banks.

Annex – I An Assessment of NBG's Cyber Risk Management Regulation vs Model Regulation

I. General

Topic	**Georgia**	**Model Regulation elements that are missing**
Authority	Article 15 of the Organic Law.	
Objective	No text	
Applicability	Commercial banks – both domestic and branches of commercial banks	
Regulatory approach	Proportionality covered; integrated with overall risk management framework	
Effective Date	April 1, 2019	
Reporting compliance to the supervisor	No text explicitly	Recommends this for ongoing monitoring.

II. Governance and oversight

Topic	**Georgia**	**Model Regulation**
Role of the Board of Directors and Senior Management	Article 8 – Management of the Bank is obliged to regularly check the efficiency of the organization's cyber security / information security program	Clear expectation from the Board and senior management. - Requisite experience - Appointment of CIO/CISO - IT/Cyber strategy - Risk tolerance / risk appetite - Tone from the top and culture - Accountability and responsibility - Resources / financial / human / technical

		- Training and awareness - Review - Independent audit - Promptly informing the Board
Policies, Standards, and Procedures	A cybersecurity framework is to be prepared; Broadly aligned with NIST's identification, Protection, Detection, Response and Recovery. Revised NIST framework's governance focus yet to be reflected. Risk Identification: people aspects not in focus.	Three lines of defense approach; Incorporating industry standards and best practices; (though this is covered under ORF regulation)
Management of information and IT assets	Covered under Article 3. Broadly in line with the model regulation. Emphasis on critical infrastructure related aspects; Role of management regarding information security policy, meeting legal and regulatory requirements, and including cyber risk as part of risk management given in this section. Threat intelligence, business impact analysis or risk assessment, risk tolerance / appetite given here.	Need for reviewing the inventory periodically. Keep track of software licenses.
Management of third party services	Covered as part of Identification – Management	No mention about list of third parties;

		Exit strategy not mentioned;
Competence and Background Review	Not clearly articulated.	Job description, background checking, etc.
Security awareness and training	Part of Article 4: Protection.	Board level training or awareness not explicitly mentioned. Training program to be reviewed periodically for its relevance.
Budget for cybersecurity	Not clearly articulated.	Separate cybersecurity budget other than overall IT budget; Training also needs to be budgeted.
Audit	No mention about internal audit function. Mentioned as part of Article 8 – independent audit – annually.	Need for internal audit function that is qualified and trained. High risk observations to be reported to the Board.

III. Technology and Cyber risk management

Topic	**Georgia**	**Model Regulation**
Risk Management framework	Article 2 focuses on cyber risk framework. Discusses NIST's five domains briefly.	Technology and cyber risk management framework. Risk assessment, risk treatment, and risk monitoring, review and reporting. Documentation. Result of the risk management process to be submitted the Board.
Risk assessment	Covered to some extended under Article 3.	

Risk treatment	Mainly mentioned in Article 6, that too with reference to incidents.	Commensurate to criticality and risk tolerance. Insurance Risk acceptance
Risk monitoring, review and reporting	Not covered in detail. Metrics only with reference to incidents.	Developing metrics, Frequency of monitoring and review, reporting.
Project management, system acquisition, SDLC, SRA, system design and implementation, system testing and acceptance, secure coding, devsecops, APIs	Being a cyber security regulation, not covered.	Useful to cover these either in cyber risk guidelines or IT risk guidelines.

IV. IT Services management

Topic	**Georgia**	**Model Regulation**
IT service management framework	Not covered explicitly	Useful
Documentation	Not covered explicitly	Documentation is an important control.
Physical controls	Covered under Article 4 – Access Control	Could be made more comprehensive
Software management	Covered under Article 4 – data protection – requires software development and testing environments to be segregated.	Development, testing and production needs to be segregated. SaaS related controls.
Configuration management	Article 4 – information security processes and procedures. More or less in alignment.	Review could be included.
Technology refresh management	Not covered explicitly.	Important element.

	ORF regulation under information systems covers some aspects of it.	
Patch management	Not covered explicitly	Important element
Change management	Not covered explicitly	Importance element
Incident management	Covered as part of Article 6.	Scope for further improvement.
Post incident review and lessons learned	Article 6 – Improvement	
IAM	Article 4 – Access control covers this. Least privilege covered under 'protective technologies.	Policy elements missing. User access reviews. Privilege access.
Network management	Network segregation – covered under Article 4 – protection.	Scope for further improvement. No mention of firewall in the entire regulation. NAD, isolating web browsing from endpoints, DDoS protection, risk assessment.
Virtualization security management	Separate cloud guidelines.	Scope for inclusion.
Data security and privacy	Separate data protection law and DGA present. Covered under data protection in Article 4.	Scope for improvement
BYOD	Covered under identification	
Secured disposal	Not covered	

V. Cyber security operations.

Topic	Georgia	Model Regulation
Cyber threat intelligence and information sharing	Covered under Article 3 – identification.	
Cyber event monitoring and detection.	Covered under Article 5 – discovery.	
Cyber incident response, management and reporting	Covered under response (Article 6) and restoration (Article 7)	
Incident reporting	NBG has incident reporting framework	

VI. Response and recovery

Topic	Georgia	Model Regulation
System availability	This is shown as one of the audit priorities in Article 8	Important to emphasize resilience as part of the regulation.
BCP/DR	In Article 3, BCP is mentioned in connection with critical service delivery. Article 7 of the ORF regulation covers testing aspects.	Scope for improvement. Whether there is a separate business continuity regulation?
Testing DR	Not explicitly covered. Article 7 of the ORF regulation covers testing aspects.	Important aspect
Backup and recovery	Mention in Article 4 – d (iv)	Important aspect
Data center	Not covered	Important aspect

VII. Scanning, Testing, Exercising, and Remediation

Topic	Georgia	Model Regulation
Vulnerability scan	No mention	Important aspect
Penetration testing	Article 8 – once a year	Can be elaborated.

Incident response exercises	Article 6 – e. Improvement	Can be elaborated.
Remediation management	Not covered in detail	Important topic

VIII. Independent Assurance

Topic	**Georgia**	**Model Regulation**
Technology risk audits	Annual independent audit – Article 8 Also, NBG has a separate regulation on Audit.	

IX. Outsourcing and Technology service provider management

Topic	**Georgia**	**Model Regulation**
Governance	Some coverage at different places. (Article 3, Article 4) Article 8 and 9 of the Operational Risk Management framework regulation discusses outsourcing in reasonable detail.	Whether you have an outsourcing guideline separately? If not needs further improvement.
Risk Assessment	Article 8 and 9 of the Operational Risk Management framework regulation discusses outsourcing in reasonable detail	
Vendor contract	NBG's power to collect information in ORF regulation	
Regulatory oversight	Power to audit not mentioned in regulation	
Vendor competency	Covered in ORF regulation	
Cloud computing	NBG has a separate cloud outsourcing guidelines.	

Annex- II Summary Table – Extant Regulations

N	Name of document	Type of document	Description of document	Approval date
1	Cybersecurity Management Framework of Commercial Banks	Regulation	Developed based on NIST Cybersecurity Framework (previous version). Additional requirements are annual SWIFT audits and penetration tests.	Approved by Decree N. 56/04 of March 22, 2019
2	Information systems and cybersecurity management audit guideline for commercial banks	Regulation	This guideline complements the NBG's Cybersecurity management framework. The audits (internal and/or external) should be conducted on annual basis. NBG should be informed before the audit starts. The same group of auditors is allowed to conduct audits only 2 consecutive years. After 2 years audit team should be changed. The audit findings should be represented in the report. The action plan based on the audit report should be prepared and shared with NBG.	Approved by the decree №48/04 May 2, 2022
3	Guideline for the Use of the Cloud Outsourcing Services by the Financial Organizations	Regulation	Currently, this guideline covers only commercial banks and microbanks critical and/or important functions. The guideline represents sort of harmonized requirements regarding the cloud usage from following authoritative sources: EBA cloud recommendations, NIST cloud computing, ESMA guideline for cloud outsourcing, ISO/IEC 27002:2022 relevant provisions regarding cloud.	Order N195/04 of the President of the National Bank of Georgia August 1, 2023
4	Cybersecurity management framework for microbanks	Regulation	This Regulation is the same as 1st and 2nd regulations (cyber framework and audit guidelines). Instead of making changes into the existing regulations (1 and 2) the decision was made to approve this as a separate regulation for microbanks.	Order №165/04 of the Acting president of NBG June 30, 2023
5	The information sharing requirements for operational risk events	Regulation	The requirements are obligatory for commercial banks. NBG operates the dedicated ISAC portal for relevant responsible users from commercial banks. The incidents, including cyber incidents, should be reported on this portal along with notifying us	Order №139/04 of the Acting President of NBG, 26 June, 2023

			per email and filling the relevant incident forms.	
6	Incident form 1	Template	If the incident falls under the category of immediate reporting, the bank should send the relevant information to us per email within the 24 hours, and the indicated form should be filled in within one week. This initial information related to incident and the form should be uploaded also on ISAC portal.	Annex of the Order №139/04 of the Acting President of NBG, 26 June, 2023
7	Incident form CSSFID-BBB-QQ-YYYYMMDD	Template	This form serves for all incidents including the immediate ones	
8	Registry of cybersecurity requirements for digital banks	Registry of requirements	This registry represents the key requirements and mandatory documentation which should be provided to us by the applicant organization which intends to be licensed as a digital bank. The timelines for implementing and developing documents and related processes are also indicated in this Registry.	Not approved in form of the official framework
9	Rule on Inclusion in Open Banking	Regulation	Article 4 of this regulation defines the security preconditions for applicants intending to join the open bank. Article 5 defines requirements for continuous security assurance.	Order №80/04 by President of NBG, 3 May, 2023
10	Cybersecurity checklist for nonbanking financial institutions	Checklist	This checklist combines both cyber and operational risks related topics. The Cybersecurity tab includes 7 thematic tabs, each of them requesting from a supervised entity relevant information and documents.	Not approved, need to be agreed with the nonbanking supervision department
11	Cybersecurity inspection checklist	Checklist	This checklist is developed mainly for inspection purposes. We request from banks to send the documents based on that list. It is developed based on Cybersecurity framework and practice as well.	Not approved

12	IS Questionnaire for new and changed products	Checklist	Based on the information provided in this checklist and additional documents, we will obtain reasonable level of assurance that the software/application or system that is supposed to ensure the secure and proper functioning of the product has been properly tested, meets business and information security requirements, and is also compatible with the Bank's existing IT with infrastructure.	Not approved, but agreed with banks, obligatory from 1st of January 2024