INTERNATIONAL MONETARY FUND

IMF Country Report No. 20/262

# NORWAY

## FINANCIAL SECTOR ASSESSMENT PROGRAM

## TECHNICAL NOTE—CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

August 2020

This Technical Note on Cybersecurity Risk Supervision and Oversight for the Norway FSAP was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed on July 7, 2020.

**Disclaimer:**
This document was prepared before COVID-19 became a global pandemic and resulted in unprecedented economic strains. It, therefore, does not reflect the implications of these developments and related policy priorities. We direct you to the **IMF Covid-19 page** that includes staff recommendations with regard to the COVID-19 global outbreak.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

**International Monetary Fund**
**Washington, D.C.**

INTERNATIONAL MONETARY FUND

# NORWAY

## FINANCIAL SECTOR ASSESSMENT PROGRAM

July 24, 2020

# TECHNICAL NOTE

## CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

This Technical Note was prepared in October 2019, before the global intensification of the COVID-19 outbreak. It focuses on Norway's medium-term challenges and policy priorities and does not cover the outbreak or the related policy response, which has since become the overarching near-term priority.

Prepared By
**Monetary and Capital Markets Department**

This Technical Note was prepared by IMF staff in the context of the Financial Sector Assessment Program in Norway. It contains technical analysis and detailed information underpinning the FSAP's findings and recommendations. Further information on the FSAP can be found at http://www.imf.org/external/np/fsap/fssa.aspx

# CONTENTS

# Glossary

| | |
|---|---|
| BCBS | Basel Committee on Banking Supervision |
| BCM | Business Continuity Management |
| BFI | Financial Infrastructure Crisis Preparedness Committee |
| CCP | Central Counterparty Clearing |
| CERT | Computer Emergency Response Team |
| CS GRC | Cybersecurity Governance, Risk and Compliance |
| COBIT | Control Objectives for Information and Related Technologies |
| CPMI | Committee on Payments and Market Infrastructure |
| CLS | Continuous Linked Settlement |
| CSOC | Cybersecurity Operations Center |
| EBA | European Banking Authority |
| EEA | European Economic Area |
| ENISA | European Union Agency for Cybersecurity |
| ESRB | European Systemic Risk Board |
| EU | European Union |
| FI | Financial Institution |
| FIRST | Forum of Incident Response and Security Teams |
| FMI | Financial Market Infrastructure |
| FSA | Financial Supervisory Authority (Finanstilsynet) |
| FSB | Financial Stability Board |
| FS-ISAC | Financial Information Sharing and Analysis Center |
| IBO | Interbank Settlement Function |
| ICT | Information and Communication Technology |
| IMF | International Monetary Fund |
| IOSCO | International Organization of Securities Commissions |
| ISAE | International Standard on Assurance Engagements |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| MoU | Memorandum of Understanding |
| NBO | Norges Bank Settlement System |
| NFCERT | Nordic Financial Computer Emergency Response Team |
| NIST | National Institute of Standards and Technology |
| NorCERT | Norwegian National Computer Emergency Response Team and Cyber Center |
| NorSIS | Norwegian Center for Information Security |
| NSM | Norwegian National Security Authority |
| OSSAT | Operational Security Situational Awareness Telco |
| PFMI | CPMI-IOSCO Principles for Financial Market Infrastructures |
| RAV | Risk and Vulnerability Analysis |
| RTGS | Real-Time Gross Settlement |

| | |
|---|---|
| SARC | Security Architecture Function |
| SLA | Service Level Agreement |
| SREP | Supervisory Review and Evaluation Process |
| SRM | Sectoral Response Institution |
| SRV | General Risk Assessment (= simplified SREP) |
| VDI | National Warning System for Digital Infrastructure (VDI) |
| WOCS | Workshop Operational Cyber Security |

# EXECUTIVE SUMMARY

**The Norwegian financial system has a long history of incorporating new technology.** Norway is at the forefront of digitization and has tight interdependencies within its financial system, making it particularly vulnerable to evolving cyber threats. Norway is increasingly a cashless society, with surveys and data collection suggesting that only 10 percent of point-of-sale and person-to-person transactions in 2019 were made using cash.[1] Most payments made in Norway are digital (e.g., 475 card transactions per capita per annum)[2] and there is an increase in new market entrants providing a broad range of services. Thus, good cybersecurity is a prerequisite for financial stability in Norway.

**Norway has matured and advanced public and private platforms for threat intelligence, information sharing, and response and recovery.** Financial institutions (FIs) and Financial Market Infrastructures (FMIs) use existing threat intelligence and crisis management platforms to test and increase their cyber-resilience. Finanstilsynet (FSA) and Norges Bank benefit from the threat intelligence for the identification of, and response to, changes in cybersecurity threat patterns in the financial sector. Cybersecurity incident reports are an additional tool for the FSA and Norges Bank to understand the level of cyber-resilience of the financial sector and to respond to cyber-attacks in a timely and coordinated manner.

**Further improvements in the collection, sharing and handling of information on cybersecurity incidents are recommended**. Clear qualitative and/or quantitative thresholds, as well as clearer processes and formats on the reporting of cybersecurity incidents, could ensure that the FSA (in its role as supervisor) and Norges Bank (in its role as overseer with a mandate for financial stability and efficient payment systems) are informed in a timely and adequate manner, allowing for effective corrective measures when needed. Norges Bank would also benefit from information sharing agreements on cybersecurity incident reports with the FSA and a clear crisis management framework on how to maintain financial stability should systemic cybersecurity incidents occur. Finalizing the ongoing effort to identify critical nodes in the financial sector as part of the implementation of the new Norwegian Security Law, informed by the financial sector map, will support financial stability considerations, as well as risk-based supervision and oversight.

**Cybersecurity risk regulation and supervisory practice are generally sound.** The FSA has adequate expertise and regulatory tools to fulfill its responsibilities as cybersecurity risk supervisor. However, the authorities are encouraged to issue additional enforceable guidance to the supervised institutions on ICT/cybersecurity risk. Key topics that have not been covered by existing guidelines are the designation of independent chief information security officer or equivalent; IT/cybersecurity awareness; identity and access rights management; security event logging and monitoring; malware prevention; and security reviews. The planned implementation of the European Banking Authority's (EBA) "Guidelines on ICT and security risk management" would solve this issue. The FSA should also implement a more structured, risk-based approach on regular inherent cybersecurity risk and

[1] Norway's Financial System: Overview Report, 2019, Norges Bank.

[2] Norway's Financial System: Overview Report, 2019, Norges Bank.

control maturity assessments of supervised institutions, supported by adequate tools. This can help to avoid blind spots in assessments over time and can, combined with the usage of intrusive on-site examination techniques, increase the level of assurance regarding the cyber-resilience of the financial sector. Further clarification could be added to the role of ICT/cybersecurity risk assessments in the overall supervisory assessment of an institution and on the influence on decisions regarding supervisory measures.

**Cybersecurity risk oversight should be intensified, and more emphasis should be given to critical service providers.** Norges Bank's oversight team is already aware of the importance and criticality of cybersecurity risk to interbank payments systems. However, intensive cybersecurity training of overseers, combined with a structured, comprehensive cybersecurity oversight approach and adequate tools, would increase the capabilities and effectiveness of the oversight function. Given the importance of a small number of service providers for interbank payment systems, the oversight function should use its existing legal powers (codified in the license terms) to seek greater assurance and transparency from critical service providers, for example by performing or mandating cybersecurity audits regularly. Additionally, clear communication of expectations by Norges Bank to the market, supplementing the CPMI-IOSCO guidance, would increase the cyber-resilience of inter-bank payment systems.

**The oversight function should be given adequate independence and resources to conduct thorough oversight of the Norwegian RTGS system (NBO)**. Currently the oversight function observes how Norges Bank's three lines of defense (i.e., operations, risk management and internal audit) operate with regard to NBO. But it is not empowered to conduct its own independent and intensive oversight of NBO, which includes setting clear oversight expectations and conducting independent assessments. Additionally, the oversight function has the same reporting line as the operators of NBO, which may raise conflict of interest issues. The oversight function should be given enough independence and support to fulfill its oversight mandate towards all interbank payment systems, including NBO, thereby reducing legal and operational risks and ensuring a level playing field between all interbank payment systems.

**The operation of NBO by Norges Bank benefits from strong cybersecurity and operations units and is well supported by risk management and internal audit.** Controls are well developed, and the mission team supports internal plans to reach the envisaged higher cyber maturity levels of NBO. However, to avoid conflicts of interests and in line with international best practice, parts of the cybersecurity risk management function could be integrated into the Norges Bank bank-wide risk management function in the future, rather than operating within the first line cybersecurity functions.

**The risk management and internal audit functions of Norges Bank should strengthen its activities on the external service providers.** Considering the criticality of external service providers for the operations of NBO, the risk management and internal audit functions within Norges Bank should intensify their direct cooperation with their counterparts in risk management and internal audit at the external service providers. Furthermore, internal audit of Norges Bank could obtain stronger assurance on the cyber-resilience of the external service providers by executing its right to audit.

| Table 1 Norway: FSAP Key Recommendations | | |
|---|---|---|
| **Recommendations and Authority Responsible for Implementation** | **Reference** | **Timing[1]** |
| ***Cybersecurity Risk Supervision (Finanstilsynet)*** | | |
| Establish clear qualitative and/or quantitative thresholds, as well as clearer processes and formats, on the reporting of cybersecurity incidents. | 49, 50 | I |
| Supplement the 2003 regulation on the use of information and communication technology with more detailed guidelines, enacted by the FSA, that provide detail on the implementation of principles and set out minimum requirements. | 54 | ST |
| Follow a more structured approach for cybersecurity risk supervision. This should include a clear description of how off-site supervision on cybersecurity should be conducted, and how assessments influence the overall risk assessments of institutions by the general supervisors. | 53 | ST |
| Increase the intrusiveness of on-site cybersecurity risk inspections. | 55 | MT |
| ***Cybersecurity Risk Oversight (Norges Bank)*** | | |
| Supplement the CPMI-IOSCO guidance with more detailed expectations of Norges Bank regarding cybersecurity risk oversight of FMIs. | 57 | I |
| Follow a more structured and comprehensive process for cybersecurity risk oversight. This includes utilizing a portfolio of tools and techniques to assess cybersecurity risk against set expectations, reaching clear conclusions and identifying specific remedial measures or thematic findings to inform future action. | 58 | I |
| Establish, operationalize and exercise an incident reporting and a crisis management framework to maintain financial stability against potential systemic cybersecurity incidents. | 66 | ST |
| Train Norges Bank overseers in cybersecurity, to strengthen the oversight function's capabilities to conduct effective cybersecurity risk oversight. | 61 | ST |
| The oversight function should be given enough independence to conduct thorough oversight of the Norwegian RTGS system (NBO). | 59 | ST |
| Finalize the financial sector risk map, in collaboration with the FSA and Ministry of Finance. | 51 | ST |
| Use the existing legal power of the oversight function to seek greater assurance and transparency from critical service providers for interbank payment systems. | 60 | ST |
| Strengthen intrusiveness of the interactions of Norges Bank's risk management and internal audit functions with NBO's external service providers to seek greater assurance and transparency. | 62 | MT |

[1] I Immediate (within 1 year); ST Short term (within 1–2 years); MT Medium Term (within 3–5 years)

# INTRODUCTION[3]

**1. This note reviews Norway's financial sector cybersecurity risk[4] supervision and oversight.** This includes the role of Finanstilsynet (Financial Supervisory Authority of Norway, FSA) and Norges Bank in the areas of cyber threat intelligence collection, financial sector and cyber mapping, cybersecurity risk related information sharing, cybersecurity risk regulation and supervisory/oversight practices, as well as response and recovery capabilities of critical financial sector participants and public sector agencies (with focus on the FSA and Norges Bank).

**2. The basis for the review of the Norwegian cybersecurity risk supervisory and oversight approach was derived from regulatory good practice.** As there are no binding international regulatory standards on cybersecurity risk management, the mission team used regulatory good practice as the basis of this report. For cybersecurity risk supervision of financial institutions (FIs) the following benchmarks were used: the FSB Stock take of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices; the World Bank Group Financial Sector's Cybersecurity: A Regulatory Digest; the BCBS Cyber-resilience: Range of practices; the IMF Departmental Paper on Cybersecurity Risk Supervision and the G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector. The CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures ("CPMI-IOSCO Guidance") is the basis of recommendations on the oversight of cybersecurity risk in financial market infrastructures (FMIs).

**3. The note focuses on the review of the supervisory and oversight frameworks for systemically important FIs and FMIs in Norway**. The review is based on questionnaire answers provided by the FSA, Norges Bank and 9 systemic FIs and FMIs, and interviews with both authorities and supervised FIs and FMIs, the study of relevant national laws and reports published by the authorities, as well as documentation of work conducted by the Norges Bank and the FSA. Interviews with selected financial institutions and financial market infrastructures informed the assessment of the effectiveness of the Norwegian regulatory framework and supervisory assessments with regards to cybersecurity risk.

[3] Prepared by Frank Adelmann (IMF) and Emran Islam (IMF external expert).

[4] Cybersecurity, cybersecurity risk, and cyber-resilience are widely but imprecisely used terms. In this note we use the Financial Stability Board's Cyber Lexicon definition of cybersecurity ("Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved"), which is broad and considers cyber incidents irrespective of their cause, and where "cyber" relates to the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Thus, for all practical purposes, the term cybersecurity is the same as information security that has been broadly used for some time. Similarly, cyber-resilience can be considered a new term referring to the existing concept of business continuity management but with a focus on cyber threats.

# CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

## A. Threat Landscape, Information Sharing, and Cyber Network

**4. The Ministry of Justice and Public Security is responsible for coordinating civilian cybersecurity, including the implementing of the Norwegian Security Act.** This responsibility includes developing and following up with national strategies and the identification of cross-sectoral issues, such as improving the cooperation and flow of information related to cyber incidents. In January 2019, the government presented a national strategy for digital security and a national strategy for digital security expertise. The Ministry of Justice and Public Security is responsible for the overall implementation of the 2018 Norwegian Security Act in the civilian sector, as well as the agency management of the Norwegian National Security Authority (NSM). The implementation of the Norwegian Security Act in the finance sector is the responsibility of the Ministry of Finance.

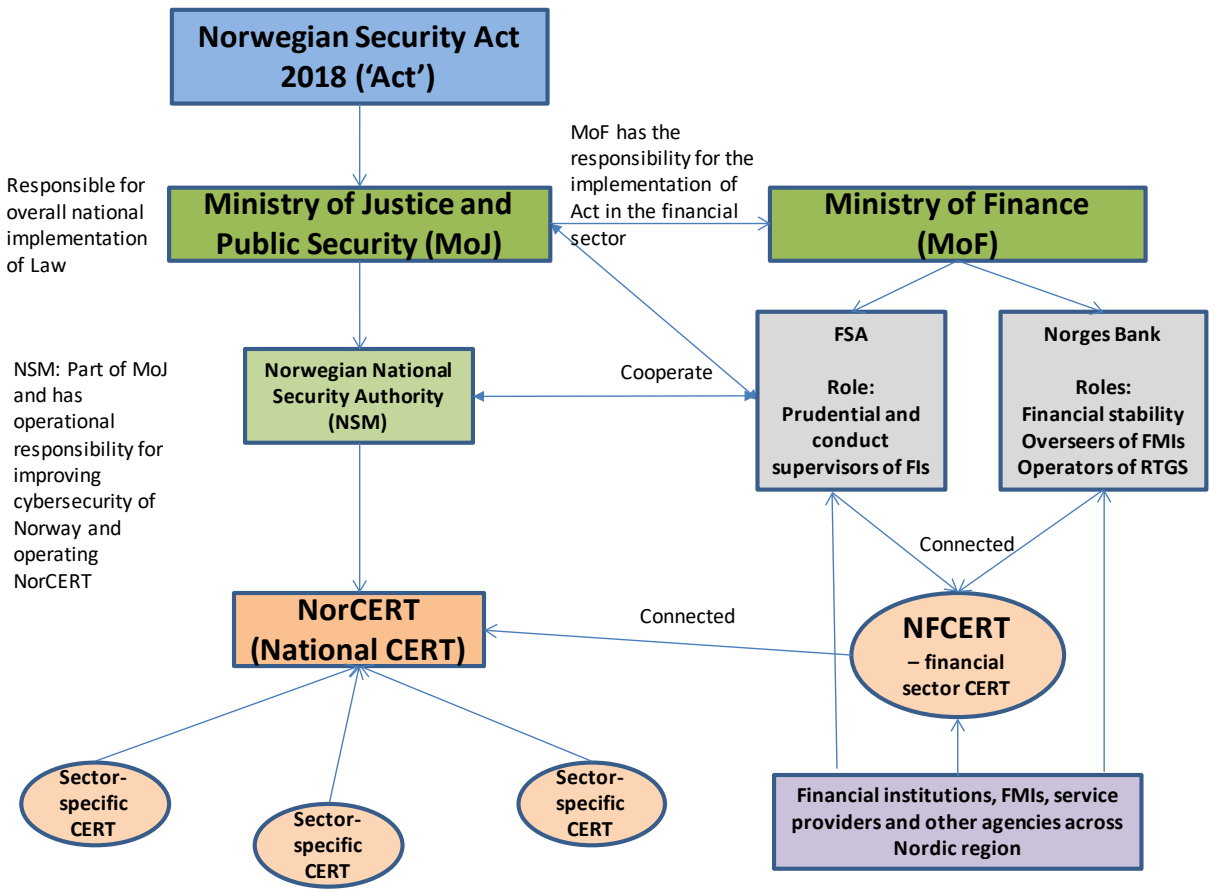
**5. The central public threat intelligence function is the Norwegian National Computer Emergency Response Team and Cyber Center (NorCERT).** In addition to its involvement in information collection and sharing, NorCERT helps to handle serious cyber-attacks against Norway's most important institutions and businesses and operates and organizes a national sensor network on the internet that detects data breach attempts against critical businesses across all sectors. NorCERT is connected to a range of sector-specific CERTs, including the Nordic Financial Computer Emergency Response Team (NFCERT), which is the dedicated financial sector CERT.

**6. NorCERT is run by the Norwegian National Security Authority (NSM).** NSM is the national cross-sectoral specialist organization for cybersecurity and the national warning and coordination body for serious cyber-attacks on critical infrastructures. The purpose of NSM is to counter threats to the independence and security of vital national security interests, primarily espionage, sabotage or acts of terrorism. Among other tasks, NSM gathers and analyses cybersecurity risk related information, develops security measures, fosters national and international cooperation, monitors information systems and conducts oversight and inspections for critical infrastructures, as defined by the ministries in line with the 2018 National Security Act. Additionally, the NSM uses intelligence sourced from the NorCERT and the sector-specific CERTs to produce a threat landscape report of Norway. NSM is the regulatory agency for the Norwegian Security Act 2018, and as such provides guidance to the act and conducts oversight and inspections of companies that have assets relevant to the act ("critical national assets"). In 2019, NSM has set up a National Cyber Security Center, where the FSA and NFCERT participate along with other public and private institutions. NSM reports to the Ministry of Justice and Public Security.

**7. NFCERT is a private not-for-profit threat intelligence information-sharing network for the entire Nordic financial sector.** The Nordic Financial Computer Emergency Response (NFCERT) helps its members to gather threat intelligence and to work together when responding to cyber threats and handling cybercrime. Its overarching goal is to strengthen the Nordic financial sector's resilience to cyber-attacks. NFCERT was founded in June 2017, based on the previous national CERT for the financial industry in Norway (FinansCERT Norge AS) and governed and paid for by its members. It connects stakeholders of all Nordic countries, including FIs and FMIs, supervisors,

overseers, police and public CERTs. NFCERT gathers and shares technical information, including cyber events and incidents without naming the institutions affected.

**Figure 1. Simplified Structure of Norwegian Regulatory and Threat Intelligence Landscape**



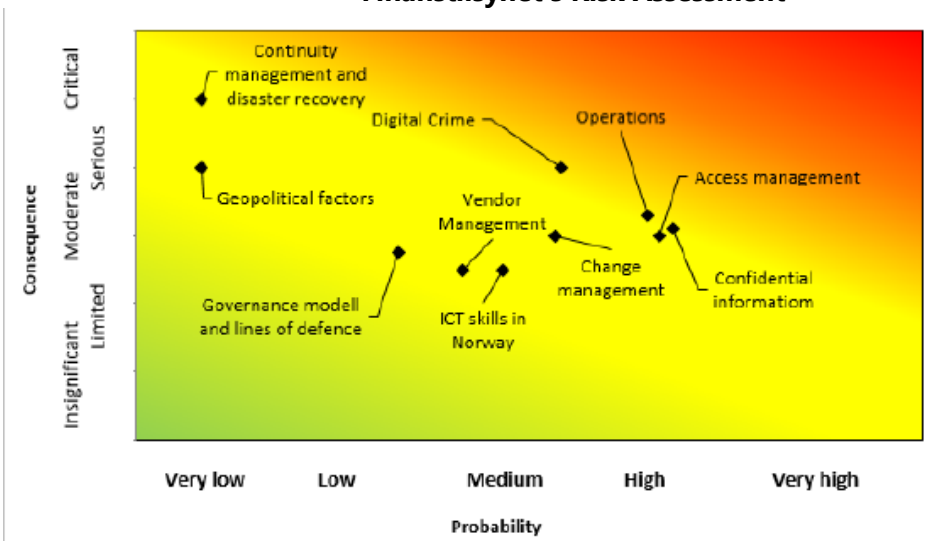

Source: IMF Staff.

**8. The FSA and Norges Bank cooperate with other public and private sector agencies to analyze cybersecurity threats to the financial sector**. The main cooperating agencies are NFCERT, the Ministry of Justice and Public Security, NSM and the NorCERT.

**9. The FSA and Norges Bank monitor the financial sector threat landscape in their respective areas of responsibility.** The FSA gathers threat intelligence about the financial sector through reports of NSM (including NorCERT), NFCERT and the European Union Agency for Cybersecurity (ENISA) and through questionnaires and meetings with selected FIs and FMIs on cyber-related matters and through cyber incident reports. Norges Bank has its own cybersecurity unit that gathers threat intelligence, mainly to ensure the cybersecurity of the central bank itself, including NBO. The Norges Bank cybersecurity team also cooperates with national and international threat intelligence providers, including information sharing networks with other central banks.

**10. FIs and FMIs must report material cybersecurity incidents to the FSA.** According to the Regulations on Use of Information and Communication Technology of 2003, FIs and FMIs must report all incidents to the FSA that lead to a material reduction in functionality because of breach of confidentiality, integrity or availability of ICT systems and/or data. The FSA reports severe incidents, with possible impacts on the proper functioning of the financial sector, to the Ministry of Finance and Ministry of Justice and Public Security simultaneously. Depending on the severity of the incident, the FSA can also alert the Financial Infrastructure Crisis Preparedness Committee (BFI), which is comprised of public financial authorities, private FIs and FMIs, major service providers to the financial industry and NFCERT. In each BFI meeting, one the agenda point is a walkthrough of severe incidents in the financial sector. In 2018, 189 IT-related incidents were reported to the FSA, approximately the same number as in 2017. In 2018, 5 of them were defined as security incidents, while in 2017 the number of security incidents was 10. None of the incidents were considered critical. A cross-sectoral framework for managing ICT security incidents has been established for critical infrastructures in parallel with regulations provided by the Norwegian Security Act 2018. At the time of the mission, it was not fully decided which FIs and FMIs will fall under the cross-sectoral system for reporting ICT security incidents. Final decisions in this regard were expected by end of 2019 and may be coordinated with the "critical national assets" that each ministry is responsible for identifying under the Norwegian Security Act 2018.

**Figure 2. Key Threats Identified in the 2018 Risk and Vulnerability Analysis**




Source: FSA.

**11. FMIs, subject to the oversight of Norges Bank, must report material cybersecurity incidents also to the Norges Bank.** Norges Bank is fully responsible for overseeing two interbank payment systems (NICS and NBO), which must report incidents to Norges Bank. In the case of other FMIs, Norges Bank shares the oversight with the FSA and other international authorities, so all authorities are informed about cybersecurity incidents. Depending on the severity of the incident,

Norges Bank can activate Norges Bank's internal crisis coordination function (BØS) for crisis situations with a financial stability impact.

**12. Based on threat intelligence gathered, the FSA prepares and publishes an annual risk and vulnerability analysis (RAV) of the financial sector's use of IT.** The yearly RAV report contains findings, observations and lessons learnt of supervisory activities, including those from cyber incident reports, and notifications of new payment services and changes in existing services received. It shares the supervisor's understanding of the cyber threat landscape and cybersecurity risk control expectations. Next to ICT and cyber, the report also covers observations in the monitoring of outsourcing contracts and new developments in the regulatory framework. Figure 2 shows key threats identified in the 2018 RAV.

**13. Norges Bank also regularly reports on cyber risk developments.** Norges Bank covered latest developments on cybersecurity and the payment system in its 2019 annual report on financial infrastructure and in a special feature in its 2018 Financial Stability Report. The 2019 report on financial infrastructure focused on red team testing to strengthen the cyber resilience of FMIs and key ICT service providers. A special feature in the Financial Stability Report 2018 highlights the importance of cybersecurity, identifies contagion channels and possible consequences for the financial system as well as several high-level measures to mitigate cyber risk to financial stability.

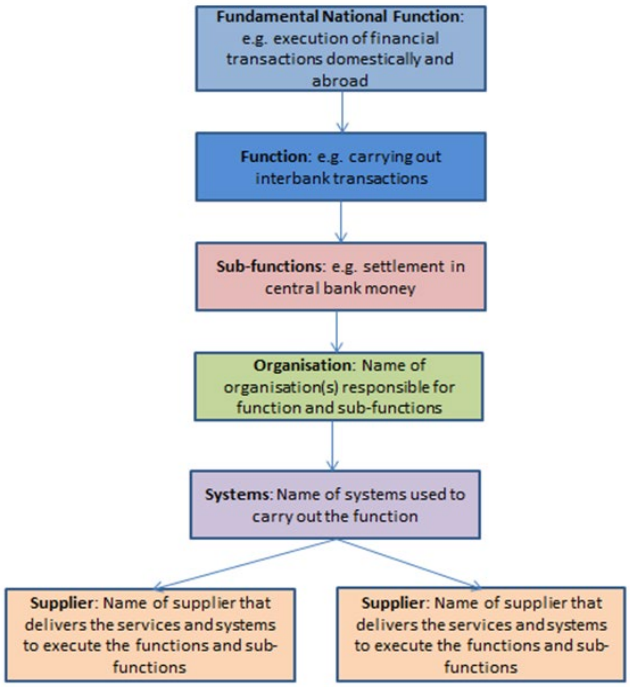
**14. Norges Bank has created a first draft of a financial sector mapping to identify critical financial infrastructures and information systems.** The mapping is based on the new Norwegian Security Act that came into force on January 1, 2019. To identify which financial infrastructures, information systems and assets in the public and private sector fall under the National Security Act's purview, each ministry had to identify so-called "Fundamental National Functions" (and "sub-functions") in its area of responsibility. Fundamental National Functions are services, production and other activities where an adverse impact will have consequences for the government's ability to preserve national security interests. The Norwegian Ministry of Finance defined three fundamental national functions in its remit:

- The ability to finance the public sector;
- Securing the ability to deliver financial services; and
- Preservation of the constitutional duties of the Ministry of Finance.

Within these fundamental national functions, critical national objects, infrastructures and information systems had to be identified. In this regard, the Norwegian Ministry of Finance has initiated a dialogue with Norges Bank and FSA about which objects, infrastructures and systems of the financial sector should fall within the scope of the Security Act. At the time of the mission, a financial sector map drafted by Norges Bank was shared with the mission team. This draft map has, however, not been discussed with and approved by the FSA and the Ministry of Finance. Figure 3 illustrates the structure of the draft financial sector map produced by Norges Bank.

**15. In 2018, Norges Bank and FSA carried out a joint survey on outsourcing that identifies critical service providers in the financial system.** The survey shows concentrations for critical systems and hardware. Norges Bank highlighted this risk in its 2019 Financial Infrastructure report.

**Figure 3. Structure of Draft Financial Sector Map Produced by Norges Bank**




Source: IMF Staff.

## B. The FSA's Supervisory Practice

**16. The FSA is the main supervisor for the Norwegian financial sector.** It supervises cybersecurity risk of banks, finance companies, mortgage companies, e-money institutions, payment institutions, insurers, pension providers, insurance intermediaries, investment firms, securities fund management companies, managers of alternative investment funds, regulated markets (including stock exchanges), securities depositories, real estate agencies, debt collection firms, external accountants and auditors. Cybersecurity risk of Norwegian branches of banks with their head office in another EEA state are, however, primarily supervised by the supervisory authorities of the country in which their head office is situated. However, for the significant branches, the FSA can participate in inspections covering ICT and cybersecurity risk related topics.

**17. The FSA participates or attends as an observer in several international committees dealing with cybersecurity risk supervision.** It collaborates with:

- the EU Agency for Network and Information Security (ENISA), which develops general recommendations on cybersecurity and contributes to the development of regulations and guidelines;
- working groups of the European Banking Authority (e.g., Task Force IT);

- working groups of the European Central Bank (e.g., SecuRe Pay - retail payment security);
- the IT Supervisory Group which fosters global supervisory collaboration on IT risk in the financial sector; and
- the Financial Information Sharing and Analysis Center (FI-ISAC), a forum where the financial sector, prosecuting authorities and CERTs share information on cybercrime.

**18. The FSA is a member of the European Supervisory Authorities, as stipulated in the EEA agreement.** Therefore, guidelines on cybersecurity published by European authorities are normally implemented in Norwegian supervisory practice. The application of the guidelines is typically announced on the FSA's website.

**19. On January 1, 2019, a new Norwegian Security Act covering cybersecurity entered into force, replacing the Security Act of 1998.** While the old law had several detailed requirements on information security, the new law is principle-based and requires a reasonable level of security without being prescriptive. The law covers the state, county and local government as well as municipal bodies. In addition, each Norwegian ministry was made responsible to decide which private businesses are crucial for the Norwegian society and shall therefore be subject to the law. Businesses covered by the law must regularly conduct cybersecurity risk assessments and implement cybersecurity controls, based on the results. The law also enforces closer interaction and information-sharing between authorities and public sector agencies.

**20. In 2003, the FSA published a regulation on the use of information and communication technology (ICT), which is the most relevant regulation to the financial sector on cybersecurity related risks.** The regulation covers both FIs and FMIs, is non-descriptive and outlines very broad principles on the following topics:

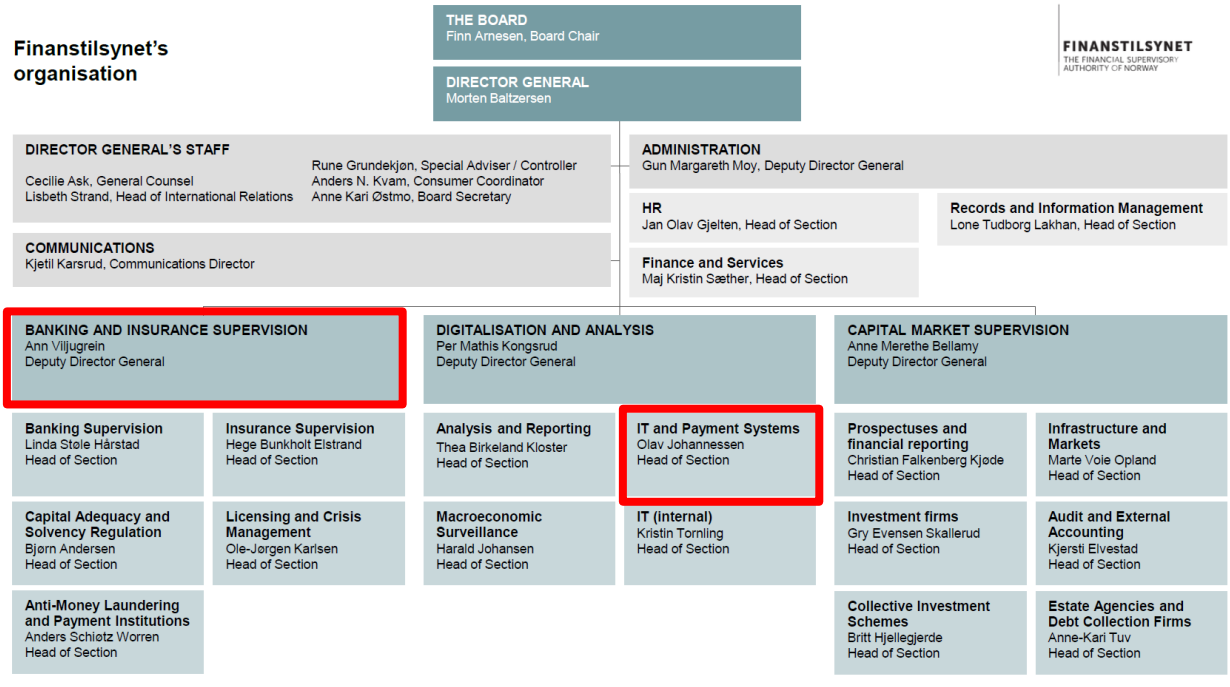
- Planning and organization;
- Risk Analysis;
- Quality;
- Security;
- Development and procurement;
- System maintenance;
- Operation;
- Problem and change management;
- Disruption of operations and contingency management; and
- Outsourcing.

When conducting supervisory assessments, the FSA uses this regulation as a basis for its conclusions.

**21. Cybersecurity risk supervision is conducted by the FSA's IT and payment systems division in the Digitalization and Analysis department, established in 2019 (see figure 4).** The departments for Banking and Insurance Supervision and Securities and Infrastructure are informed about the results of cybersecurity risk assessments and include these into the overall risk assessments of financial institutions. Both departments can be involved in on-site visits but are otherwise hardly involved in the execution of the assessments. The IT and payment division is staffed with 11 FTE.

**22. Information requests and cybersecurity risk assessment criteria can be institution-specific or thematic.** According to the FSA, a risk-based supervisory methodology for cybersecurity risk has been established, based on international supervisory standards. Typically, institution-specific information requests are sent out to selected institutions, with focus on cybersecurity governance, policies and procedures. Supervisors assess the information received and organize on-site visits (1-3 days), where the submitted information is verified. On the response and recovery capabilities, a standardized questionnaire was sent out in 2018 to all Norwegian banks and significant branches. The information received is planned to be subject of on-site visits for selected institutions. Based on the outcomes, a compilation report is planned to be written. For ICT risk assessments (including cybersecurity risk) COBIT is the preferred technical good practice framework used by supervisors, next to NIST, ISO and the CPMI-IOSCO guidance.

**Figure 4. Organizational Chart of the FSA**




Source: FSA.

**23. On-site visits are mainly focused on policies, routines and based on interviews, documentation and incident reports.** The FSA sees the three lines of defense within the

supervised institutions, as well as external auditors, as being responsible for testing the maturity and effectiveness of cybersecurity related controls in an intrusive manner. The FSA can perform on-site inspections on a deeper technical level but is typically not making use of this.

**24. The FSA and Norges Bank work together closely in cybersecurity risk supervision and oversight.** Each authority extends invitations to the other to attend relevant supervisory and oversight meetings on cybersecurity related issues, for FMIs that fall within the purview of both authorities. Norges Bank is also regularly invited by the FSA to participate in relevant cybersecurity related on-site visits.

**25. IT service providers are not subject to the same regulation and supervision as licensed banking and payment system participants.** This means that the FSA cannot impose requirements directly on the IT service providers. The FSA is, however, free to conduct assessments and inspections of vendors and service providers as part of the assessment or inspections of supervised entities. The EBA guidelines on Outsourcing Arrangements[5] are applied by the FSA, which also enforce the right to audit and access for supervisors. Supervisory measures in case of information/cybersecurity related shortcomings at the vendor/service provider are directed to the licensees that are responsible for monitoring their IT service providers.

## C. Norges Bank's Oversight Practice

**26. Norges Bank and the FSA are the authorities responsible for the oversight and supervision of FMIs in Norway.** Norges Bank is the supervisory authority for certain interbank systems under the Payment Systems Act. The supervision of interbank systems means that Norges Bank is a licensing authority and has a right and an obligation to require changes if the interbank system is not arranged in accordance with the Payment Systems Act and license terms.

**27. Norges Bank fully oversees two interbank payment systems according to the Norges Bank Act (NICS and NBO).** As part of its oversight, Norges Bank can obtain information and require NICS and NBO to make changes that increase the efficiency and security of the systems. Norges Bank can also give advice and makes recommendations to the Ministry of Finance and other relevant authorities when, in the Bank's opinion, action is deemed necessary and Norges Bank itself does not have instruments at its disposal. Additionally, Norges Bank's oversight of international FMIs that are important for the financial sector in Norway takes place through participation in international oversight colleges.

**28. Other Norwegian FMIs (e.g., CSDs, CCPs and banks operating payment systems) are supervised by the FSA and overseen by Norges Bank, concurrently.** Both authorities jointly supervise and oversee Norwegian FMIs under two publicly disclosed cooperation arrangements, which establish the nature of tasks, cooperation, and division of responsibilities. The cooperation arrangements do not provide for joint supervision, but both the FSA and Norges Bank closely work together in oversight and supervision.

[5] These guidelines only apply for credit institutions, investment firms and payment and electronic money institutions.

| Table 2. Norway: FMIs Subject to Supervision and Oversight | | | |
|---|---|---|---|
| **FMI** | **Operator** | **Norges Bank's role** | **Other designated authorities** |
| Norges Bank's settlement system (NBO) | Norges Bank | Supervision (Norges Bank's Supervisory Council) and oversight | Supervision: Norwegian National Security Authority. |
| Norwegian Interbank Clearing System (NICS) | Bits AS | Licensing and supervision | |
| DNBs settlement bank system | DNB Bank ASA | Licensing and supervision | Licensing and supervision of the bank as a whole: Finanstilsynet and Ministry of Finance. |
| SpareBank 1 SMNs settlement bank system | SpareBank 1 SMN | Oversight | Licensing and supervision of the bank as a whole: Finanstilsynet and Ministry of Finance. |
| CLS | CLS Bank International (CLS) | Oversight in collaboration with other authorities | Licensing: Federal Reserve Board<br>Supervision: Federal Reserve Bank of New York.<br>Oversight: Central banks whose currencies are traded at CLS (including Norges Bank). |
| Norwegian securities settlement system | Verdipapirsen tralen ASA (VPS) | Oversight | Supervision: Finanstilsynet. |
| VPS's central securities depository (CSD) function | VPS | Oversight | Licensing: Ministry of Finance<br>Supervision: Finanstilsynet. |
| SIX x-clear's central counterparty system | SIX x-clear Ltd. | Oversight in collaboration with other authorities | Supervision: Swiss financial supervisory authority.<br>Oversight: Swiss National Bank, Finanstilsynet and Norges Bank. |
| LCH's central counterparty system | LCH Ltd. | Oversight in collaboration with other authorities | Supervision: Bank of England<br>Oversight: EMIR College and Global College (including Norges Bank). |
| EuroCCP's central counterparty system | EuroCCP N.V. | Oversight in collaboration with other authorities | Supervision: Dutch central bank<br>Oversight: EMIR College (including Norges Bank). |
| Source: 2019 Financial Infrastructure Report, Norges Bank. | | | |

**29. Norges Bank assesses the FMIs that are subject to supervision and oversight in accordance with principles drawn up by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO)**. The FSA is also a member of IOSCO, so supervision takes into consideration the CPMI-IOSCO principles, alongside other regulations and good practices. In the context of cybersecurity risk, Norges Bank's oversight is conducted against the CPMI-IOSCO guidance on cyber resilience for financial market infrastructures ("CPMI-IOSCO guidance"), published in June 2016. The CPMI-IOSCO guidance is principles-based and mostly non-prescriptive, therefore allowing FMIs and Norges Bank a degree of flexibility in implementation and oversight, respectively. In terms of international engagement, the Norges Bank participates in the cyber systemic risk working group of the European Systemic Risk Board (ESRB).

**30. The Guidance requires FMIs to establish and implement a cyber resilience framework.** The Guidance covers the following topics:

- Cyber governance;
- Identification;
- Protection;
- Detection;
- Response and recovery;
- Testing;
- Situational awareness; and
- Learning and evolving.

**31. Norges Bank relies on FMIs completing self-assessments against the CPMI-IOSCO guidance as the basis of its oversight.** The self-assessment helps inform Norges Bank's assessment process. In addition, cybersecurity is on the agenda of the bi-annual meetings with FMIs. In both oversight and supervision meetings, Norges Bank focuses on the FMIs' approach to cybersecurity, particularly on how the FMIs protect themselves against potential cyber-attacks and their preparedness (including business continuity planning) for potential incidents. The FSA normally attends these meetings. Together with FSA, Norges Bank has also participated in individual ICT on-site visits. In terms of the supervisory approach of the FSA towards FMIs, the same approach is taken for FMIs as set out above with regards to other types of financial institutions.

**32. IT service providers are not subject to direct oversight by the Norges Bank.** However, as recommended in the 2015 FSAP Technical Note on Oversight and Supervision of financial market infrastructures, the Norges Bank has requested NBO and NICS to obtain a self-assessment from its critical service providers against Annex F, which are the oversight expectations for critical service providers. These expectations focus on five key areas: risk identification and management; information security; reliability and resilience; technology planning; and communication with users. Additionally, Norges Bank has the right to access and audit the critical service providers of NICS and

DNB Settlement Systems as part of their licensing term. This right has, however, not been executed to date.

**33. Norges Bank and the FSA are considering using red team testing as a means of gaining assurance on the cyber resilience of its FMIs and other financial institutions and critical service providers.** In its 2019 Financial Infrastructure Report Norges Bank and in the RAV 2018 the FSA announced that it will invite the financial industry, the FSA and other relevant authorities to a dialogue that will serve as the basis for an assessment on the suitability of the Threat Intelligence-based Ethical Red teaming Framework (TIBER-EU), published by the ECB in 2018. This tool, which sets out the methodology to conduct simulated cyber-attacks on financial institutions, is being considered as a tool to strengthen the oversight of FMIs and to assess the resilience of FMIs including their critical service providers, which are considered as a key concentration risk to financial stability. At the time of the mission, Norges Bank and the FSA had collectively sent a letter to various authorities and financial institutions, financial market infrastructures and significant service providers, inviting their views on the adoption of TIBER-Norway.

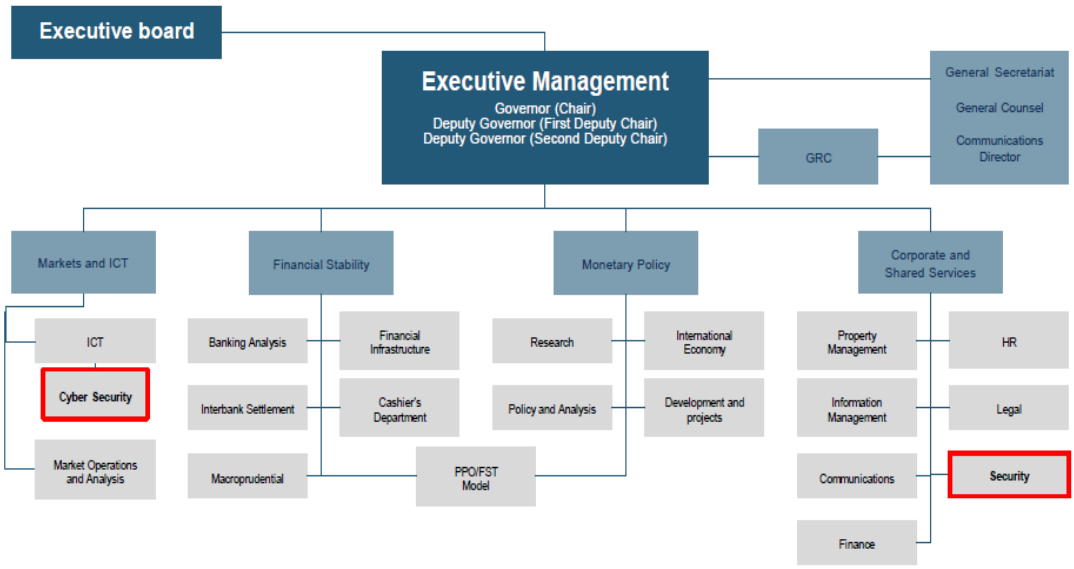
**34. Cybersecurity risk oversight is conducted by the Financial Infrastructure Division (see figure 5).** The department is staffed with 8 FTE, who are responsible for oversight of all the FMIs in scope, but without dedicated cyber specialists. To fill this void, the department works closely with the IT department, which provides technical expertise and insight, and the Security Department, which provides strategic overview, threat assessments and national security insight.

**35. In addition to oversight, Norges Bank has a key role in operating NBO, the Norwegian RTGS system.** NBO outsources the operations of its critical infrastructure to EVRY, SIA, and Vermeg. Within Norges Bank, the Interbank Settlement function (IBO) is responsible for the daily operations of NBO and reports to the Head of Financial Stability. The oversight function for NBO also reports to the Head of Financial Stability.

**36. From a cybersecurity perspective, there is a dedicated cybersecurity unit that is responsible for ensuring the cybersecurity of Norges Bank, including protecting the operational activities of NBO within Norges Bank.** This unit, comprised of 14 FTEs, is tasked with delivering Norges Bank's IT and Cyber Strategy and Vision, which is: "No threat actor with purpose and ability must be able to, unhindered and unseen, perform a successful cyber operation against Norges Bank". The cybersecurity unit is made up of the Security Architecture (SARC) function, which is responsible for protecting Norges Bank; the Cybersecurity operations center (CSOC), which conducts detection and response activities; and the Cybersecurity Governance, Risk and Compliance (CS GRC) function, which conducts cyber risk management activities and acts as the second line of defense.

**37. Norges Bank collaborates with a broad range of external partners**, for example NFCERT, Norwegian National Cybercrime Centre, National Cyber Security Centre, Operational Security Situational Awareness Telco (OSSAT), Workshop Operational Cyber Security (WOCS), Financial Services—Information Sharing and Analysis Centre (FS-ISAC) and Central Bank's Heads of Security Organization (37 central bank and the Bank for International Settlements).

**Figure 5. Organizational Chart of Norges Bank**




Source: Norges Bank.

**38. Norges Bank's risk management (GRC) function plays an instrumental role in monitoring, managing and reporting the cybersecurity risks related to NBO, which includes the risk borne from its external service providers.** From a risk perspective, the key cybersecurity risk is borne from the level of resilience of NBO's service providers. In this respect, Norges Bank's IBO function interacts with its providers, which includes discussing performance against SLAs, obtaining key performance indicators, reviews and reports conducted by the providers, etc. The risk management functions (GRC and CS GRC) review these outputs indirectly. On a quarterly basis, the risk management function (GRC) supports IBO in performing a risk review for NBO. The review is also supported by the ICT department including the Cyber Security Section, CS GRC, and Norges Bank Security. The heads of these units and the head of the Cyber Security Section meet to discuss risks related to NBO and its providers. A quarterly risk-report that includes risks of NBO and the observations of the oversight function is prepared for the Head of Financial Stability. The report is discussed in the management meeting for the Financial Stability Department, where the oversight function attends. Furthermore, a bi-annual risk-report for the central banking operations that includes cyber-security risks related to NBO is presented to the Executive Board.

**39. Norges Bank Security and Crisis Management are responsible for the implementation of the Norwegian Security Act 2018 in the organization and supporting its implementation in the financial sector.** It is the bank's single point of contact towards the national security and intelligence agencies, the security contacts in the ministries, and maintains Norges Bank's formalized security cooperation with other Central Banks and the Bank for International Settlements. Norges Bank Security has coordinated the mapping of the financial sector to identify critical financial infrastructures and information systems, as part of identifying the "Fundamental National Functions" that the Norwegian Security Act 2018 will cover. This has included development of new methodology for structuring functions, institutions, systems and suppliers in a national security

context. Norges Banks Security also provides the holistic strategic threat intelligence capability of the bank; and training, planning, electronic systems and external coordination for crisis management across the organization. As part of the latter it facilitates Norges Bank and the financial sector's participation in the national exercise "Digital 2020."

**40. Norges Bank's internal audit function (i.e., third line of defense) conducts an audit of NBO at Norges Bank every three years**. This includes a review of how the different functions within Norges Bank interact with its providers and manage the outsourcing relationship. Although the contractual terms permit Norges Bank's internal audit function to conduct an audit of its providers (e.g., EVRY), this right has not been used. Internal audit relies on external IT audits (e.g., ISAE 3402) conducted by its suppliers, as a source of assurance.

## D. Response and Recovery Capabilities

**41. Cybersecurity incidents in the financial sector are followed-up by the FSA and Norges Bank.** The FSA gathers and analyses cybersecurity incidents of the entire financial sector (excluding inter-bank payment systems), while Norges Bank oversees solely incidents in inter-bank payment systems. The same distribution of tasks applies for the supervision and oversight of emergency preparedness solutions.

**42. Each institution in the financial sector has an independent responsibility for ensuring acceptable risk in its own business.** This includes, among other things, the responsibility for secure and stable operating solutions, good backup and emergency solutions and actively contributing to a robust financial infrastructure. Assessment of the business continuity management of FIs and FMIs are conducted as part of the supervisory assessments and on-site visits, and through oversight assessments against Principle 17 of the PFMIs and the CPMI-IOSCO Guidance. The FSA has conducted a thematic review, on the response and recovery capabilities of critical institutions it supervises, supported by a detailed questionnaire.

**43. To effectively detect and manage cyber-attacks in the financial sector from a technical perspective, several cooperation platforms have been established.** NSM operates the national response function for serious cyber-attacks against critical infrastructures and is responsible for organizing and operating the national warning system for digital infrastructure (VDI). VDI is a network of sensors located in public and private businesses that own critical infrastructure. Information from the sensors contributes to a national capability for early detection and verification of coordinated and targeted attacks. NorCERT and NFCERT also collect cybersecurity incident related information and ensure that all relevant parties receive the correct warning information and are enabled to take the necessary action.

**44. The Financial Infrastructure Crisis Preparedness Committee (BFI) is responsible for coordinating measures to prevent and resolve severe crisis situations.** The FSA is the manager and secretariat for BFI. In the event of a serious incident, the FSA would be responsible for invoking the BFI, as well as informing the Ministry of Finance. The BFI consists of participants from Norges Bank, the FSA, Ministry of Finance, NFCERT, Finans Norge, Evry ASA, Nets A/S, major FMIs and FIs as

well as of additional observers from the telecommunications, power and postal sectors, NSM and the securities and brokerage sector. The BFI was established in 2000 and typically holds three regular meetings a year.

**45. BFI organizes and follows up on results of emergency drills and desktop exercises.** An important task for BFI is to carry out annual emergency drills, to ensure that the communication channels between critical financial sector participants work effectively, and to hold an annual desktop exercise with the participants, based on realistic scenarios. Exercises are conducted to better prevent and manage extreme but plausible scenarios. In an exercise, the BFI facilitates institutions to discuss a scenario, its consequences and possible measures that can be taken. It maps out potential mitigation actions and debates effective solutions to the simulated problem. The responsibility for developing scenarios and managing the desktop exercise is rotated between the financial sector participants annually. The follow-up discussions aim to address identified sectoral weaknesses and find appropriate solutions. One scenario focused, for example, on the lack of availability of a card payment network, leading to the potential use of an offline card solution and its operational capacity in a crisis. Furthermore, a communication plan for the public and other authorities is worked out, and annual reports on the work of the BFI are prepared.

**46. In the event of a serious incident within an inter-bank payment system, the Norges Bank would be informed.** Depending on the severity of the incident, the Director of Financial Stability would invoke BØS, the internal crisis coordination function for incidents with a financial stability impact, or the bank-wide crisis group, which would thereafter liaise with the relevant stakeholders.

**47. NSM is mandated to gather cross-sector incident information of all businesses subject to the new Norwegian Security Act.** The basis of cybersecurity incident reporting is the framework for managing ICT security incidents from 2017, targeted at critical public and private businesses and sectoral response institutions (SRM). It describes a systematic approach to managing ICT security incidents across businesses and sectors to ensure an effective national sector-wide handling capacity. The framework does not include dealing with the consequences of cybersecurity incidents. This is handled by other regulations and emergency procedures. It therefore does not replace incident reporting regulations and guidelines published for the financial sector. According to the framework, critical businesses are required to receive, evaluate and disseminate information from and to their responsible SRM. The MoF has appointed the FSA as SRM for the financial sector in Norway and exercises its role in collaboration with NFCERT, according to agreed information exchange rules.

# REVIEW AND RECOMMENDATIONS

## A. Threat Landscape, Cyber Network, and Information Sharing

**48. The public and private threat intelligence gathering and sharing in Norway is mature and advanced.** According to interviews with FIs, FMIs and the authorities, NFCERT delivers valuable information and support amongst the existing CERTs and thereby helping the financial sector in combatting cybercrime. Both FIs and FMIs are closely involved in NFCERT and it is widely considered to be of major importance for a successful cooperation within the national and wider Nordic financial sector. The regulators also benefit from information shared through this platform. NorCERT complements the threat intelligence needed by the FSA and Norges Bank, to conduct effective cybersecurity risk supervision and oversight, with additional cross-sectoral intelligence.

**49. However, incident reporting and follow up could be improved.** Although an incident reporting scheme has been established by the FSA since 2003 according to which incidents should be reported with undue delay, concrete criteria for incidents to be reported and defined processes with established timelines are missing. The FSA intends to comply with the EBA Guidelines on major incident reporting, which contain such criteria. The implementation of these guidelines has, however, been delayed and would not cover all institutions under the supervision of the FSA. The cybersecurity incident reporting of supervised and overseen institutions is a key component of understanding the threat landscape of the financial sector, and a key trigger for risk-based supervisory and oversight actions as well as crisis management plans. Some institutions indicate that they only report incidents after knowing the root cause, sometimes leading to reports 10 business days after the incident happened. Other institutions, however, immediately report all incidents that are considered critical according to their internal classification scheme. The current incident reporting scheme does not necessarily ensure a timely reaction in case of a serious incident with possible contagion effects to the wider financial sector.

**50. Clear qualitative and/or quantitative thresholds as well as better defined processes and formats on the reporting of cybersecurity incidents should be implemented.** Qualitative and quantitative thresholds for incident reporting (such as the duration of downtime, the internal risk classification of the incident or the importance of systems affected), would ensure a common understanding in the financial sector on which incidents should be reported to the supervisor and overseer and would avoid having critical information being withheld. Based on the criticality of incidents, clear reporting processes and timelines should be communicated to the financial sector. This incident reporting guidance should be consistent with the new framework for managing incident reporting established by NSM. Norges Bank's cybersecurity incident reporting scheme should benefit from the same kind of clarification. The FSA and Norges Bank should collaborate and exchange information on cybersecurity incidents in a way that allows both authorities to fulfill their responsibilities (FSA as supervisor and Norges Bank as overseer, operator and responsible authority for financial stability), thereby avoiding inefficient parallel, independent reporting regimes.

**51. Norges Bank should finalize the sector map, in collaboration with the FSA and Ministry of Finance.** Norges Bank's draft financial sector map gives a good overview of critical functions, organizations, systems and service providers in the Norwegian financial sector. The finalized financial sector map will help both, Norges Bank and the FSA, to get an overview of all potential systemic risks from key nodes, interconnections and critical service providers; to detect contagion channels relevant for financial stability; to inform the risk-based supervisory and oversight approach of the FSA and Norges Bank; and for enhancing common tools and initiatives for critical players in the financial sector (e.g., crisis coordination and red-team testing).

## B. The FSA's Supervisory Practice

**52. The ICT supervisors of the FSA seem to have adequate expertise and capacity to conduct effective cybersecurity risk supervision.** Cybersecurity risk regulation and supervisory practice are generally sound. The FSA has good regulatory tools to fulfill its responsibilities as cybersecurity risk supervisor. Off-site and on-site assessments are conducted regularly in a risk-based manner. The RAV report is very valuable and gives a detailed overview on the state of cybersecurity in the financial sector.

**53. Cybersecurity risk supervision should, however, follow a more structured approach.** This should include a clear description on how off-site supervision on cybersecurity should be conducted, and how assessments influence the overall risk assessments of institutions, conducted by the general supervisors. The FSA's IT and Payments Systems division, in charge of cybersecurity risk supervision, has the required skills for cybersecurity risk assessments of banks and has conducted very valuable cybersecurity risk assessments on the financial institutions it is supervising in the past. However, there are no manuals guiding the specialized ICT/ cybersecurity risk supervisors on how to conduct a consistent assessment of a firm's ICT or cybersecurity risk profile (inherent risk) and its ICT or cyber control maturity level, ensuring a minimum level of cybersecurity in the financial sector and preventing blind spots in the off-site assessments, over a defined period. The manuals should consider the criticality of the institutions for the financial sector and be supported by efficient tools that support the efficiency of the supervisory assessment (e.g., structured questionnaires for information gathering). They should furthermore clarify how the assessments should influence the overall operational risk assessment of institutions as part of the overall supervisory review process (SREP or SRV).

**54. The 2003 Norwegian regulation on the use of information and communication technology (ICT) should be supplemented by more detailed guidelines enacted by the FSA.** The FSA has not yet published outcome-focused rules that provide detail on the implementation of principles, and baseline expectations that set out minimum requirements that will form the basis for a robust cybersecurity framework of FIs and FMIs. Guidelines to key topics covered by international good practice on cybersecurity risk management, such as designation of independent chief information security officer or equivalent; IT/cybersecurity awareness; identity and access rights management; security event logging and monitoring; malware prevention; and security reviews, have not been issued by the FSA. To solve the issue, the FSA plans to work with the EBA guidelines on ICT and security risk management (finally published in December 2019) and the NSM

cybersecurity principles. When working with these guidelines, the FSA should ensure that these are communicated in a way that ensures enforceability of supervisory actions when needed.

**55. The intrusiveness of on-site cybersecurity risk inspections should be increased.** The FSA has been conducting valuable on-site visits in supervised institutions, summarized in official letters and followed-up by the specialized ICT and cybersecurity specialists. Although there is a detailed ICT security inspection manual that is highlighting intrusive testing procedures for key areas of cybersecurity, in practice on-site inspections are typically less intrusive. Typically, inspections are limited to short (1-3 days) on-site visits with longer preparation phases, focusing on policies, documentation and governance arrangements. Having more intrusive checks on the accuracy and consistency of information provided by the institutions and on the effectiveness of cybersecurity controls implemented, could increase the level of assurance to the cyber-resilience of the sector and improve the supervisor's understanding of supervised institution. The finalized financial sector map can highlight critical nodes where the FSA can focus its efforts with more intrusive inspections, thereby obtaining greater assurance of cyber-resilience in the financial sector.

## C. Norges Bank's Oversight Practice

**56. Norges Bank, in its oversight and operational capacities, has rightly identified cybersecurity as a major risk to financial stability, and undertaken several initiatives to prioritize its work in this area.** Norges Bank has correctly identified concentration risk from service providers as a financial stability risk; has initiated processes to explore tools (e.g., TIBER-Norway) to further enhance the cyber resilience of the financial system; and in its operational role, has set a clear vision, strategy and implementation plan to improve NBO's cyber resilience. However, there is room for significant improvement in its cybersecurity risk oversight process. Although the FMIs under Norges Bank's oversight mandate had provided a self-assessment against the CPMI-IOSCO guidance, there was no request for supporting documentation, and minimal review and follow-up. The focus of oversight was limited to bi-annual meetings, and there was a lack of scrutiny on the level of maturity of the FMIs. In this regard, there are several steps Norges Bank can take to improve its oversight, as set out below.

**57. The basis for cybersecurity risk oversight of FMIs, which is the CPMI-IOSCO guidance, should be supplemented by more detailed expectations of Norges Bank.** The Norges Bank uses the principles-based CPMI-IOSCO guidance for its oversight of FMIs. However, Norges Bank has not set out clearly to the FMIs under its purview outcome-focused expectations and baseline minimum requirements in addition to the broad CPMI-ISOCO principles. The Norges Bank should clearly articulate expectations in relation to governance, identification, protection, detection, response and recovery, testing, situational awareness and learning and evolving, based on international good practice. Where the Norges Bank shares its oversight responsibilities with the FSA, it should collaborate with the FSA to determine appropriate expectations and requirements. By setting clear expectations, Norges Bank will: (i) provide its overseen FMIs with detailed steps on how to operationalize the CPMI-IOSCO guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time; (ii) establish a clear basis against which it can assess the FMIs it is responsible for; and (iii) provide the basis for a meaningful

discussion between the FMIs and the overseers. When establishing these expectations, the Norges Bank should ensure that these are communicated clearly to the FMIs.

**58. Cybersecurity risk oversight should follow a more structured and comprehensive process.** This includes utilizing a diverse portfolio of tools and techniques to assess against the set expectations, culminating in clear conclusions and identifying specific remedial measures and/or thematic findings that can lead to future action. A more structured and intrusive approach would allow Norges Bank to gain greater assurance on the FMIs and their critical service providers. This should be supported by an adequate number of staff and a toolkit for cybersecurity assessment, which may include, but are not limited to, questionnaires, self-assessments, desktop reviews of documentation, on-site inspections and walkthroughs, threat-based penetration testing (e.g., TIBER-Norway) and technical reviews ("deep dives") on key risk areas. The use of external experts could be considered. The toolkit and assessment process will allow Norges Bank to develop clear conclusions and identify concrete remedial measures that can lead to future action. In this regard, the mission team supports the outreach to the financial sector to assess the value of the establishment of a threat-led penetration testing framework for Norway ("TIBER-Norway"), as a tool to test critical FMIs and critical service providers. Generally, when drawing a key conclusion, the overseers should summarize observed practices and achievements, and identify gaps or shortcomings against expectations as they emerge from the facts gathered. Overall, the output of assessments should provide value, support decision making and generate feedback that lead to significant and sustained improvement.

**59. The oversight function should be given adequate independence to conduct thorough oversight of NBO.** The oversight function observes how Norges Bank's three lines of defense (i.e., operations, risk management and internal audit) operate with regard to NBO. But it is not empowered to conduct its own independent and intensive oversight of NBO. Sound cybersecurity risk oversight should entail, amongst other things, an evaluation of whether the three lines of defense for NBO function effectively to identify, monitor and mitigate cyber risk. Additionally, the oversight function has the same reporting line as the operators of NBO, which may raise conflict of interest issues. The oversight function should be given sufficient independence and support to fulfill its oversight mandate towards all interbank payment systems, including NBO, thereby reducing legal and operational risks and ensuring a level playing field. Legal risks could be caused by other FMIs going to court, claiming unequal treatment in oversight practices. Operational risks could arise from ineffective cybersecurity controls for NBO, not identified by the oversight or internal control functions, based on unmitigated conflicts of interests. This independent and more intensive oversight should allow the oversight function to set its own oversight expectations for NBO and conduct its own independent assessments.

**60. The oversight function in Norges Bank should use its existing legal power to seek greater assurance and transparency from critical service providers to interbank payment systems.** The structured oversight approach (supported by an adequate toolkit), should cover all critical nodes identified in the financial sector mapping, including critical service providers, ensuring that all critical nodes have a high level of cybersecurity maturity.

**61. Norges Bank should provide its overseers with further training on cybersecurity, to strengthen their capabilities to conduct effective cybersecurity risk oversight.** The oversight department is staffed with 8 FTE, who are responsible for oversight of all FMIs, but without cybersecurity specialists. As cybersecurity has not traditionally been an area of focus for overseers of FMIs, there is a shortage of expertise that combines oversight of FMIs and cybersecurity globally. Norges Bank should therefore provide its staff with intensive training on cybersecurity. Building in-house capacity will enable the oversight function to oversee its own FMIs more effectively and enhance Norges Bank's contribution to oversight conducted jointly with the FSA (e.g., VPS) and other international authorities and colleges (e.g., LCH EMIR College and Global College). Meanwhile, the oversight should continue to leverage off expertise provided by the IT department, which facilitates cross-fertilization of skills and rationalization of resources.

**62. The risk management and internal audit functions within Norges Bank should increase intrusiveness regarding NBO's service providers, to seek greater assurance and transparency.** Norges Bank uses its three lines of defense (i.e., operations, risk management and internal audit) to identify, mitigate, monitor and report risk related to NBO, as operated within Norges Bank. However, as NBO has outsourced its infrastructure to critical service providers, Norges Bank should consider using its risk management and internal audit functions to interact more directly with the risk management and internal audit counterparts at the critical service providers of NBO, rather than relying solely on the reports from the providers. The internal audit function should also use its existing right to audit the critical service providers. This will allow Norges Bank's risk management and internal audit functions to gain a better understanding of the risk and control environment at the critical service providers. NBO is classified as a "critical national asset" under the Norwegian Security Act 2018. This entails that suppliers (service providers) to the infrastructure are also bound by the Security Act. Norges Bank could in this regard also use the formal requirements provided by the Security Act to follow up the critical service providers.

**63. Norges Bank's internal cybersecurity approach (first line of defense) is advanced, with a clear vision, strategy and implementation plan to increase its level of cyber maturity.** Norges Bank should continue to build on its well-established first line of defense in cybersecurity and advance towards implementing its strategic goals and aspirational level of maturity. However, Norges Bank could incorporate the CGRC unit (the dedicated cybersecurity risk management function) within the GRC function (i.e., Norges Bank's overall risk management function), to ensure independence for the second line cybersecurity activities, in line with international good practice.

## D. Response and Recovery Capabilities

**64. Cooperation on the response to and recovery from successful cyber-attacks in the financial sector of Norway is advanced.** NSM, NFCERT, SRM and BFI help the financial sector to quickly, effectively and in a coordinated manner respond to cyber-attacks. Regularly conducted emergency drills and desktop exercises from BFI and the Ministry of Justice (for example the exercise "Digital 2020"), which test crisis communication and response capabilities, are good tools to

enhance cyber-resilience on a financial sector level. The 2018 thematic review of the FSA suggested adequate preparedness of critical supervised institutions. After the finalization of the financial sector mapping, the FSA should, however, verify that the current crisis management bodies, emergency drills, desktop exercises and supervisory activities focused on response and recovery capabilities, cover all critical nodes of the financial sector. Some of these might be in different jurisdictions and not be fully supervised by the FSA. In this regard, the FSA should use its role as SRM to extend checks on response and recovery capabilities of all identified critical nodes in the financial sector and increase international cooperation on crisis management with countries that host critical nodes not directly supervised by the FSA (such as branches of foreign banks that are critical to the Norwegian financial sector).

**65. However, there are gaps in the collaboration on incidents with potential financial stability implications.** Financial connectedness and operational dependencies can function as contagion channels when serious incidents occur. The Norwegian financial system is interconnected, both through banks and FMIs' exposure to one another and through extensive use of common systems and shared service providers. This may increase cybersecurity risk and amplify the effects of shocks and disruptions. The consequences may become more serious if public and market confidence in banks and the financial system erodes. Norges Bank's Financial Stability Report 2018 describes possible channels through which cyber risks affect financial stability (disruptions at an individual bank, payment system disruptions and disruptions among critical ICT service providers). Currently, Norges Bank does not have adequate processes and protocols to identify and respond to cybersecurity incidents with a potential systemic impact. The missing collaboration with the FSA on cybersecurity incident reporting, which receives most cybersecurity incident reports for the financial sector, might prevent a timely activation of crisis management procedures in Norges Bank. Furthermore, it is unclear how cybersecurity incidents that are shared with or reported to Norges Bank are analyzed for a potential impact on financial stability and thereafter escalated (e.g., to BØS). Norges Bank is part of the FSA-led BFI structure. BFI is, however, only activated in cases which may severely impact the Norwegian financial infrastructure, and its activation is not necessarily based on a financial-stability-related criteria.

**66. Norges Bank should establish, operationalize and exercise a crisis management framework to maintain financial stability against potential systemic cybersecurity incidents.** Specifically, Norges Bank should take a structured approach to cybersecurity incident analysis and responses, based on cybersecurity incident information sharing agreements with the FSA, and incorporate this into existing crisis management structures. Norges Bank could take the following structured approach:

- Establish information sharing agreements with the FSA on cybersecurity incidents and establish common, clear criteria and processes for cybersecurity incident reporting.
- Establish criteria, thresholds and analytical processes to determine whether a cybersecurity incident impacts financial stability. Norges Bank may leverage off its work on identifying critical nodes in the financial sector map and conduct analyses on how such incidents could transmit through the financial system.

- Additionally, outcomes from international research and working groups can help in defining those processes (such as the cyber systemic risk working group of the European Systemic Risk Board in which Norges Bank participates).
- Based on the cybersecurity incident information sharing and analyses, Norges Bank should leverage and strengthen existing internal structures (e.g., BØS) to ensure that it can respond to cybersecurity incidents and potential crisis situations, in a timely manner and with clear escalation paths and communication protocols – internally and externally. The crisis coordination should consider domestic and international systems and institutions that may be impacted.
- Norges Bank should regularly test and exercise this cybersecurity risk related crisis management framework, to ensure it is prepared for a real crisis and is effective. The Digital 2020 initiative, led by the Ministry of Justice, may be an opportune time to exercise.