APPENDIX 3: FINANSTILSYNET'S MONITORING ACTIVITIES

Finanstilsynet will supervise institutions' compliance with the requirements for secure and robust ICT systems and assess their preparedness for handling critical situations in 2024.

Finanstilsynet's supervision of ICT and payment services – key areas

The supervisory activities are risk-based, and Finanstilsynet prioritises supervision of institutions that are of the greatest significance to financial stability and well-functioning markets. Finanstilsynet will assess ICT risk and review the institutions' annual risk assessments. Furthermore, Finanstilsynet will follow up the following topics:

- Institutions' overall management and control of ICT activities
- Control and monitoring of ICT service providers and outsourced ICT operations
- Preparedness, including testing of contingency solutions
- Work related to ICT/cybersecurity
- Institutions' control over access to systems
- Change management
- Institutions' payment services
- ICT solutions for detecting money laundering and terrorist financing

The use of new technology, major changes in the ICT field, and significant changes in the financial infrastructure are also relevant areas that will be monitored.

Work on payment systems

Finanstilsynet will monitor the robustness of payment solutions, ensuring that adequate emergency preparedness is established for these solutions and that the emergency preparedness of the electronic payment system is sound. The cooperation with Norges Bank related to the payment system and the financial infrastructure will continue.

Finanstilsynet will continue to monitor institutions compliance with the Regulations on payment services systems[1], including:

- Account servicing payment service providers' interfaces (APIs) for third party providers' access to accounts, according to the European Banking Authority's (EBA) opinion[2]
- Risks associated with payment services
- Compliance with the notification obligation for new or changed payment services

During the licensing processes, Finanstilsynet will ensure that institutions have well-documented procedures related to ICT and payment services.

[1] Lovdata: Regulations on payment services systems

[2] EBA calls on national authorities to take supervisory actions for the removal of obstacles to account access under the Payment Services Directive

Follow-up of incidents

Follow-up of ICT incidents is a prioritised part of supervisory activities. Finanstilsynet will closely monitor developments. It will assess whether institutions report incidents in accordance with the regulations and ensure that institutions identify the cause of the incident and implement measures to prevent recurrence. In the event of serious irregularities, Finanstilsynet will monitor the incident throughout its duration and continuously assess specific measures. Furthermore, it will follow up that both account servicing payment service providers and third party service providers report deviations related to account servicing payment service providers' interfaces (APIs) and that account servicing payment service providers correct the deviations and inform the third party service providers in accordance with PSD2. Identified vulnerabilities in institutions' ICT solutions will also be monitored. Finanstilsynet will continue its annual review of the largest actors' incident reporting.

Outsourcing of ICT activities

Finanstilsynet will follow up institutions' outsourcing of ICT operations. The follow-up includes institutions' notification to Finanstilsynet on new and amended agreements on outsourcing of critical or important ICT operations, in accordance with section 4c of the Financial Supervision Act and section 3 of the Notification Obligation Regulations[3]. Supervisory activities will include:

- Monitoring institutions' governance of outsourced ICT activities
- Ensuring that the institutions conduct risk analyses and a proper assessment of the outsourcing arrangement before entering into agreement
- Ensuring that contracts comply with regulations, particularly regarding inspection rights
- Ensuring that critical and important contracts are reviewed by the board
- Ensuring that outsourcing is otherwise properly managed within the institution, in accordance with section 2 of the ICT Regulations.

Emergency preparedness

The work of the Financial Infrastructure Crisis Preparedness Committee (BFI) will continue. BFI reviews incident scenarios, among other things, and assesses whether responsibilities during crisis situations are sufficiently clear. Emergency response exercises are also planned for 2024, and measures related to findings from previous exercises will be followed up. Certain incidents will be monitored more closely, especially with key actors in the financial infrastructure.

Finanstilsynet will participate in joint Nordic/Baltic activities related to preparedness and operational resilience. It will also participate in relevant contingency work initiated by other sectors and coordination within the national framework for handling ICT security incidents, including through the National Cyber Security Centre (NCSC), established by the Norwegian National Security Authority (NSM).

Finanstilsynet will align its preparedness work and handling of ICT security incidents with NSM's framework for handling ICT security incidents[4]. Finanstilsynet serves as the sectoral response environment (SRM) for the financial market area and fulfils this role in cooperation with the Nordic Financial CERT (NFCERT), according to agreement. The NSM framework forms the basis for the cooperation between Finanstilsynet and NFCERT.

Monitoring of the cyberthreat landscape

[3] Lovdata: The Notification Obligation Regulations (Norwegian only)

[4] NSM Framework for handling ICT incidents (Norwegian only)

Finanstilsynet will stay informed about institutions' use of ICT and developments in payment services, including specific trends related to:

- The cyberthreat landscape
- Digital crime
- Systemic ICT risk
- Work with emergency preparedness focused on digital vulnerability and digital security
- Institutions' organisation and follow-up of security work
- Changes in payment processing using new technology
- Cross-border activities

Together with Norges Bank, Finanstilsynet established a framework in 2021 for testing cybersecurity in the financial sector (TIBER-NO). The aim is to promote financial stability by increasing resilience against cyberattacks on critical functions in the Norwegian financial sector. This work is monitored by a steering group led by Norges Bank, with participation from Finanstilsynet.

Finanstilsynet will hold regular meetings with institutions and NFCERT. In addition, it will participate in the National Cyber Security Centre (NCSC), the European supervisory authorities' work on ICT security, and the European Systemic Cyber Group (ESCG) under the European Systemic Risk Board (ESRB).

In 2023, a project was initiated to assess systemic ICT risk in cooperation with Norges Bank. The aim is to establish a framework for mapping and assessing systemic ICT risk and to conduct annual assessments.

Consumer protection

Finanstilsynet will monitor that institutions establish digital solutions in compliance with regulations and that the solutions launched have built-in security and functionality in line with consumer expectations. The emphasis will be on institutions safeguarding their customers' security when using their solutions and services.

Finanstilsynet will also monitor that institutions do not share customer data without consent and that data do not fall into the hands of unauthorised third parties. Furthermore, it will ensure that institutions communicate with their customers in a safe and secure manner, such as not sending or requesting information about the customer or their engagement in emails or causing uncertainty by including links in email or SMS communications.

Finanstilsynet will monitor that consumers are given the option to protect themselves against adverse incidents, for example, by being able to block cards for online use.

Based on the requirement to report fraud involving payment services, according to section 2 of the Regulations on Payment Services Systems, Finanstilsynet will monitor the overall extent of fraud and, if necessary, individual actors. The quality of reporting will be followed up.

If incidents occur, Finanstilsynet will follow up that institutions provide customers with information on how they have been affected and how the institution or the customer can remedy the situation.

Finanstilsynet will continue to monitor that the banks fulfil their obligations concerning compliance with the provisions of the Financial Institutions Act[5] regarding cash offerings. It will also monitor that the banks have established solutions in line with the provisions of the Financial Institutions Regulations to meet increased demand for cash in a crisis situation[6].

[5] Lovdata: Financial Institutions Act

[6] Lovdata: Financial Institutions Regulations