INTERNATIONAL MONETARY FUND

IMF Country Report No. 23/135

SWEDEN

FINANCIAL SECTOR ASSESSMENT PROGRAM

April 2023

TECHNICAL NOTE ON CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

This Technical Note on Cybersecurity Risk Supervision and Oversight for the Sweden 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 March 16, 2023.

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

SWEDEN

FINANCIAL SECTOR ASSESSMENT PROGRAM

March 16, 2023

TECHNICAL NOTE

CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

Prepared By
Monetary and Capital Markets Department

This Technical Note was prepared by Mr. Nick Strange, short-term consultant, under the supervision of Tommaso Mancini-Griffoli, in the context of the Financial Sector Assessment Program in Sweden. 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
BIS	Bank for International Settlements
CERT	Computer Emergency Response Team
CIISI-EU	Cyber Information and Intelligence Sharing Initiative
CPMI	Committee on Payments and Market Infrastructure
CMBCG	Cross-Market Business Continuity Group (UK)
CMORG	Cross-Market Operational Resilience Group (UK)
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECRB	Euro Cyber Resilience Board
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESRB	European Systemic Risk Board
EU	European Union
FI	Finansinspektionen
FIDI-FINANS	Forum for Information Sharing on Information Security in the Financial Sector
FMI	Financial Market Infrastructure
FMV	Swedish Defense Materiel Administration
FRA	National Defense Radio Establishment
FSC	Financial Stability Council
FSPOS	Financial Sector's Public-Private Cooperation Group
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
MSB	Swedish Civil Contingencies Agency (Myndigheten för Samhällsskydd och beredskap)
	Riksgälden
SNDO	Swedish National Debt Office
NCSC	National Cyber Security Centre
NFCERT	Nordic Financial CERT
NIS	Network and Information Security (Directive)
NIST	National Institute of Standards and Technology
POR	Principles for Operational Resilience (BIS)
PTS	Swedish Post and Telecom Authority
PFMI	CPMI-IOSCO Principles for Financial Market Infrastructures
RTGS	Real-Time Gross Settlement
SAMFI	Cooperation Group for Information Security
SREP	Supervisory Review and Evaluation Process
TIBER	Threat Intelligence-Based Ethical Red teaming

EXECUTIVE SUMMARY

Sweden's financial sector is highly digitalized and interconnected, and the related technological developments heighten cyber threats and vulnerabilities. The cyber threat landscape has evolved, with many Swedish financial institutions victims of Distributed Denial of Service (DDoS) attacks. Wider, more destructive attacks are likely in the near future.

The National Institute of Standards and Technology (NIST) Cyber Security Framework (Identify, Protect, Detect, Respond and Recover) has been adopted as an organizing framework by supervisors in Finansinspektionen (FI). Our recommendations follow this framework:

Identify

Sweden is well-served with agencies engaged with cybersecurity, but the roles and responsibilities of each in respect to the cyber security of the financial sector should be clarified and barriers to sharing information resolved. At a high level, the Swedish Civil Contingencies Agency (Myndigheten för Samhällsskydd och beredskap (MSB) is responsible for coordinating the work on cyber risk across the whole of society. A National Cyber Security Strategy was published in 2017 identifying high-level strategic priorities, supported by an action plan for 2019–2022, reported on annually. The national strategy is not sector-specific. A financial sector cyber security strategy has been under development and was disclosed as a plan on united action within the financial sector for the Financial Stability Council's (FSC's) December 2022 meeting. This and other work in train under the FSC will begin to address the questions about roles and responsibilities and information sharing, but we recommend that the Swedish authorities (including the Government and the Riksdag) (i) allocate clear responsibilities for cyber security risk management and interagency cooperation in the financial sector; and (ii) identify and address barriers to information sharing between government agencies, the financial authorities, and the private sector. We welcome the decision to establish a permanent forum under the NCSC where operational information can be exchanged between authorities with participants from the private sector.

It is important that the financial sector engages with and helps to shape the activities of the NCSC. We recommend the National Cyber Security Centre (NCSC) should engage fully with the financial sector, ideally as a case study. The information sharing forum referred to above, which includes the financial authorities and private sector firms, should drive greater engagement.

Cyber incident reporting frameworks are in place, as are some, limited, information sharing fora, but there is still an appetite from financial institutions to receive more information on threats and incidents. In its role as Sweden's Computer Emergency Response Team (CERT-SE), MSB receives notification of cyber incidents, as does the supervisory authority, Finansinspektionen (FI) and the Riksbank in its capacity of overseer of financial market infrastructure (FMI). Public-private information sharing fora exist in which the major banks and FMI providers

participate. However, our interviews with financial institutions revealed an appetite for timely threat intelligence from the agencies and financial authorities. We recommend that MSB, and in due course the NCSC, should produce regular cyber threat intelligence reports available to all financial institutions. We also recommend that the authorities should routinely draw on incident reporting and other sources to identify trends and common threats and report back to financial institutions, encouraging further engagement.

The information that the Riksbank and FI receive from regulated firms about essential services and material outsourcing arrangements should be organized in a database and analyzed so that concentrations and dependencies can readily be identified. Operators of essential services must identify themselves with the help of criteria in the national Network and Information Security (NIS) Act and in regulations[1] issued by MSB. Regulated firms are required to inform their supervisor if they are entering into a material outsourcing arrangement with a third party. This information could be used to identify concentrations and dependencies on a limited number of suppliers, but no such aggregation takes place either in Riksbank or FI. We recommend that FI should establish and maintain a central database of such essential service providers and outsourced third-party arrangements and use the data to analyze and identify concentrations. The resulting register will most likely be of a very sensitive nature and will need to be managed accordingly.

Respond and Recover

Contingency plans and crisis protocols should be established for large-scale cyber-attacks impacting the Swedish financial sector. General crisis manuals are available as a reference for the Riksbank and FI in the event of a cyber incident, but we understand that work is underway to further develop the financial sector crisis documentation to include more specific details regarding cyber-attacks. The first cyber security crisis management exercise was held in the Autumn of 2021 under instruction from the Financial Stability Council involving the Ministry of Finance, Riksbank, FI and the Riksgälden (Swedish National Debt Office (SNDO) with representation up to a senior level. This raised questions on what actions should be taken, when the crisis occurs within the financial sector but does not stem from companies having traditional financial problems and the traditional tools thus are ineffective. Defining how information sharing should be conducted was another issue that the authorities encountered during the exercise. We strongly support the need for further cyber crisis management exercises and recommend that the financial authorities and relevant government agencies formalise an operational and cyber incident response framework and exercise it regularly. We further recommend that the authorities consider extending cyber exercises to include participants from the private sector.

[1] MSBFS 2018:7 (now MSBFS 2021:9)

Regulation and Supervision

The financial authorities should prepare for enactment of the EU Digital Operational Resilience Act (DORA) by identifying the gaps and inconsistencies that will arise as a result of that Act in domestic regulation and guidelines. There is little specific mention of cyber risk in current legislation, either domestic or at the EU level, instead general provisions must be interpreted in a cyber risk context. It is expected that DORA will help consolidate what is currently a fragmented regulatory landscape for ICT and cyber risk management. We recommend that the financial authorities undertake a detailed review of domestic legislation and regulations to identify and address gaps and inconsistencies.

Supervisory review work on cyber risk is risk-based, grounded in legislation, and aligned to the NIST Cyber Security Framework, but ICT resource constraints will need to be addressed. ICT risk continues to be a prioritized risk for FI and several important reviews have been carried out in recent years, in particular thematic work based on the NIST framework. Recognizing the need for materially more resources in FI's ICT Competence Centre, particularly as its remit was expanded to cover markets, insurance, and the Protective Security Act, the budget for cyber risk supervision resource was increased from five to 18. However, it is proving difficult to recruit appropriately skilled individuals and in any case the scale of the required recruitment would be burdensome to the small existing team. FI has the power to appoint and instruct an auditor (i.e., an external specialist) to audit (review) a financial firm under its supervision but has not yet used this power. Other jurisdictions have found this a useful way to (i) augment limited internal resources and (ii) access highly specialized skills that would be uneconomic to retain in-house. We recommend that FI should investigate innovative means by which supervision resource can be augmented through secondments and increased use of existing powers to appoint auditors.

Table 1. Sweden: 2022 FSAP—Key Recommendations			
Recommendations	**Paragraph Reference**	**Responsible**	**Timing[1]**
Threat Intelligence and Information Sharing			
The Swedish authorities (including the Government and the Riksdag) should allocate clear responsibilities for cyber security risk management and interagency cooperation in the financial sector.	20	The Swedish Authorities	I
The Swedish authorities (including the Government and the Riksdag) should identify and address the barriers to information sharing between government agencies, the financial authorities, and the private sector. We welcome the decision to establish a permanent forum for sharing operational information between the authorities and the private sector.	21, 22	The Swedish Authorities	ST
The NCSC should engage fully with the financial sector as its role is developed	23	NCSC	I
MSB, and in due course the NCSC, should produce regular cyber threat intelligence reports available to all financial institutions.	24	MSB	ST
The authorities should routinely draw on incident reporting and other sources to identify trends and common threats and report back to financial institutions, encouraging further engagement.	25	The Swedish Authorities	ST
Essential services, critical infrastructure and outsourcing			
FI should establish and maintain a database of essential service providers and outsourced third party arrangements and use such information to identify concentrations and dependencies.	31	FI	I
Cyber incident management			
The financial authorities and relevant government agencies should formalise an operational and cyber incident response framework and exercise it regularly.	36	The Swedish Authorities	ST
The financial authorities and relevant government agencies should consider extending cyber exercises to include participants from the private sector.	37	The Swedish Authorities	MT
Regulatory Framework			
The financial authorities should undertake a detailed review of domestic legislation and regulations to identify and address gaps and inconsistencies, if any.	42	The financial authorities	ST
Oversight and Supervision			
FI should investigate innovative means by which supervision resource can be augmented such as secondments and increased use of existing powers to appoint skilled persons “auditors”.	50, 51	FI	I
[1] I Immediate (within 1 year); ST Short term (within 1-2 years); MT Medium Term (within 3−5 years)			

INTRODUCTION

1. Sweden's financial sector is highly digitalized, and the participants are increasingly interconnected. With technological development and digitalization, the cyber threats and vulnerabilities increase. Technology is advancing in all areas of banking and finance. Artificial intelligence and machine learning applications are in development for credit and market risk management. Adoption of cloud-based software and infrastructure services has accelerated as a result of the pandemic leading to new operational risks. Central to all these is a safe and secure payment system. Sweden has become increasingly dependent on electronic means of payment and cash-free. The percentage of people paying in cash for their last purchase has fallen from 39 percent in 2010 to less than 10 percent in 2020[2] and many businesses now no longer accept cash as a means of payment. The *Swish* instant payment app-based system, a cooperative venture between the six largest banks in Sweden, is now the preferred means of peer-to-peer payments, with nearly 8 million private users at the end of February 2022 and 260,000 companies signed up.[3]

2. The cyber threat landscape too has evolved. Over the past few years, many Swedish financial institutions have become victims of Distributed Denial of Service (DDoS) attacks that have flooded online services and websites with traffic causing them to become unreachable and inoperable for short periods of time. The authentication and signing service BankID, a common way to prove identity in digital environments in Sweden, suffered from a large DDoS attack on May 2020 which led to a four-hour outage and a further attack in 2021 leading to a one-hour outage. Much wider, more destructive attacks are likely in the near future as tools and techniques once only available to nation states become freely available on the Dark Web. Evidence of this has already been seen with increasingly sophisticated ransomware attacks. The authorities use a range of sources, including third-party threat intelligence providers, to inform them of the financial sector's changing exposure to cyber threats.

3. This note focuses on the supervisory and oversight frameworks for financial institutions (including banks, insurers and FMIs). This note sets out an assessment of the work of the Riksbank (the Swedish central bank and an authority under the parliament (Riksdag)), FI (the Swedish Financial Supervisory Authority) and the SNDO (the resolution authority) in the areas of cyber threat intelligence gathering, information sharing, financial sector mapping, cyber security risk regulation and supervisory and oversight practices, as well as the response and recovery capabilities of critical financial sector participants and public sector agencies. The review is based on questionnaire answers provided by the Ministry of Finance, the Riksbank, FI and the SNDO, and interviews with the authorities and supervised financial institutions, the study of relevant national laws and reports published by the authorities, as well as documentation of work conducted by the Riksbank and FI. Interviews with selected financial institutions and FMIs informed the assessment of

[2] Cash free – not problem-free (riksbank.se)

[3] Swish - About Swish

the effectiveness of the Swedish regulatory framework and supervisory assessments with regards to cyber security risk.

4. The basis for the review of cyber security supervision and oversight was derived from international standards and regulatory good practice. As there are no binding international regulatory standards on cybersecurity risk, the mission team used guidance material developed by standards-setting bodies and regulatory good practice as the basis of this note. For cybersecurity risk supervision of financial institutions (FIs) the following benchmarks were used: BCBS '*Principles for Operational Resilience* and the revision of the *Principles for the Sound Management of Operational Risk'* (both March 2021) and BCBS *Cyber-resilience: Range of practices* (December 2018); the FSB's *'Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices'* and Discussion Paper on *'Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships'* (November 2020) the World Bank Group's '*Financial Sector's Cybersecurity*: *A Regulatory Digest;'* the EBA's *'Guidelines on ICT and Security Risk Management'* and *'Guidelines on Outsourcing Arrangements.'* EIOPA's *'Guidelines on ICT Security and Governance'* and *'Guidelines on outsourcing to cloud service* providers;' 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'* (June 2016), is the basis of recommendations on the oversight of cybersecurity risk in FMIs.

CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

5. This note sets out our understanding of current arrangements, our assessment of those arrangements and our recommendations. The National Institute of Standards and Technology (NIST) Cyber Security Framework (Identify, Protect, Detect, Respond and Recover) has been adopted as an organizing framework by supervisors in FI. Where meaningful, our recommendations follow this framework. Under the NIST category "Identify" we cover 'Threat Intelligence and Information Sharing' and 'Essential Services, Critical Infrastructure and Outsourcing.' Under the NIST category 'Respond and Recover,' we focus on 'Cyber Incident Management.' The remaining two sections: 'The Regulatory Framework' and 'Supervision and Oversight' are not limited in coverage to specific NIST categories and so stand alone.

A. Threat Intelligence and Information Sharing

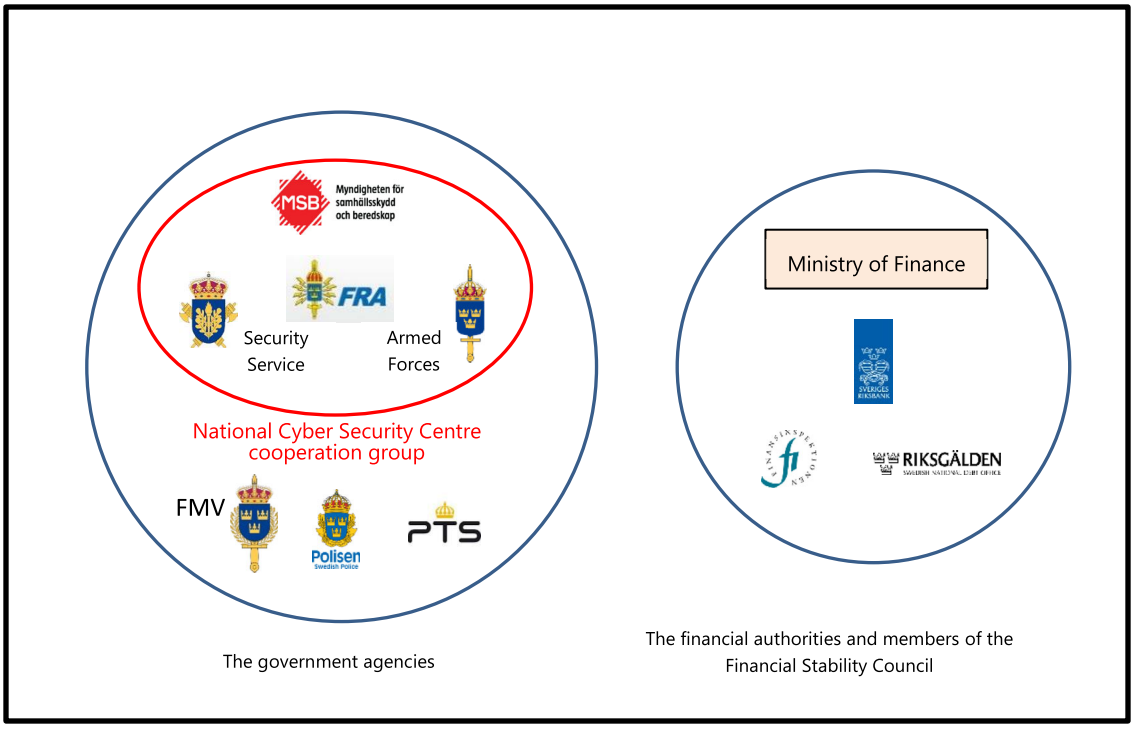
Current Arrangements

6. The Swedish Civil Contingencies Agency (MSB) is responsible for coordinating the work on cyber risk across the whole of society. The MSB is responsible for issues concerning civil protection, public safety, emergency management and civil defense where no other authority has responsibility. Responsibility refers to measures taken before, during, and after an emergency or crisis. MSB reports to the Swedish Government, from whom it receives its instructions. MSB hosts a

website[4] offering guidance on information and cyber security and management, accessible by all. Until recently, MSB hosted an 'Interagency Cooperation Group for Information Security (SAMFI)' bringing together the public authorities with a particular responsibility in the field of information and cyber security including the National Defense Radio Establishment (FRA), Swedish Defense Materiel Administration (FMV), the Swedish Armed Forces, The Swedish Post and Telecom Authority (PTS), the Swedish Police and the Swedish Security Service. We understand that this group no longer exists, and its role subsumed into the NCSC. MSB is also the single point of contact for CERT-SE, Sweden's national CSIRT (Computer Security Incident Response Team). CERT-SE supports governmental authorities, regional authorities, municipalities, enterprises, and companies. CERT-SE's broader responsibilities are to:

- Respond promptly when IT incidents occur by spreading information, and where needed, work with the coordination of measures and partake in work to remedy or mitigate the consequences of the incident/s.
- Cooperate with authorities that have specific tasks in the field of information security.
- Act as Sweden's point of contact for equivalent services in other countries and develop cooperation and information exchanges with them.

Figure 1. Agencies and Authorities with an Interest in Cyber Security



[4] Informationssäkerhet.se - Support for systematic work with information security in organizations (informationssakerhet.se)

7. The Swedish Government published a national cyber security strategy in 2017. The strategy is not sector-specific, but is regarded as an important common starting point for the work to develop information security in society as a whole. The main aims of the strategy are to help to create the long-term conditions for all stakeholders in society to work effectively on cyber security, and raise the level of awareness and knowledge throughout society. The strategy sets out a number of priorities for Government:

- Securing a systematic and comprehensive approach in cyber security efforts;
- Enhancing network, product and system security;
- Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents;
- Increasing the possibility of preventing and combating cybercrime;
- Increasing knowledge and promoting expertise; and
- Enhancing international cooperation.

8. A Comprehensive Information and Cyber Security Action Plan has been prepared for the years 2019-2022, addressing in particular the establishment of a Swedish National Cyber Security Centre. In 2018 the Swedish Government asked the public authorities with particular responsibility in the field of information and cyber security to develop and prepare a comprehensive information and cyber security action plan. MSB has been charged with the responsibility to coordinate annual reports on the plan, setting out progress on each of the strategic priorities identified in the national cyber security strategy. The 2020 and subsequent reports focus in particular on the development of the NCSC.

9. The NCSC's aim is to strengthen Sweden's overall ability to prevent, detect and manage hostile cyber threats. In accordance with the Swedish Government's decision in December 2020 to establish the center, it will gradually be developed in the coming years. The cyber security center's mandate is to:

- Coordinate the work to prevent, detect and manage cyber-attacks and other IT incidents;
- Provide advice and support on threats, vulnerabilities and risks; and
- Be a national platform for cooperation and information exchange with private and public actors in the cyber security area.

10. By 2023, the center is expected to develop in the following areas:

- Targeted and coordinated warnings about threats and cyber-attacks;
- Coordination of the support to preventive protective measures, for example cyber security assessments and mapping of operational preparedness in the event of IT incidents;
- Exchange of knowledge, skills and information and cooperation with public and private actors, for example on detection, vulnerabilities, threats, risks, analysis, tools, and methods, as well as international cooperation; and
- Provision of skills enhancement initiatives, for example exercises and training of identified target groups.

11. The cyber security center is to regularly report to the Government on its activities, and in 2023 the Government will decide on its continued direction. In form, the NCSC consists of in-depth cooperation between several Swedish authorities: The National Defense Radio Establishment (FRA), the Swedish Armed Forces, the Swedish Civil Contingencies Agency (MSB) and the Swedish Security Service (Säkerhetspolisen). Within the center, temporarily housed at MSB, the participating agencies are gradually co-locating staff and coordinating their efforts to prevent, detect and manage cyber-attacks, and other cyber incidents, and provide support regarding threats, vulnerabilities, and risks.

12. The Riksbank, the SNDO and FI have developed coordinated action plan for strengthening the cyber security in the financial sector. The Financial Stability Council (FSC), a forum for representatives from the government, FI, SNDO and the Riksbank to discuss matters pertaining to financial stability, has increasingly discussed matters regarding cyber security in the Swedish financial sector. In 2021, the Riksbank and FI decided to develop a Sector Specific Cyber Security Strategy for the financial sector after a discussion at the FSC meeting in June that year. It was later decided that the efforts in this regard should be given a more operational orientation through developing a coordinated action plan. This plan was presented to the FSC at its meeting in December 2022.No draft of the action plan was made available at the time of our review, but it is understood that the following areas were to be covered:

- Establishing a permanent forum where operational information can be exchanged between government agencies such as the Security Service and the FRA with participants from the financial sector;
- Establishing a forum to develop and distribute threat assessments, currently expected to be hosted within the National Cyber Security Centre, subject to MSB's approval;
- Considering the role that the Norwegian NFCERT5 might play in the Swedish cyber security ecosystem; and
- Setting out a broad range of actions to increase knowledge about cyber threats and incidents in the financial sector and financial sector authorities.

13. At the FSC meeting in June 2022, the Riksbank, the SNDO and FI took stock of their work in this regard. A new permanent forum for information sharing and the development and distribution of threat assessments is established under the auspices of the NCSC. NFCERT will likely play an important part in information sharing with midsize and small financial institutions that will not be a part of the NCSC forum. The FSC has no legal powers to enact recommendations arising from the strategy but can discuss the need to take certain actions that are within the legal powers of the financial authorities. Wider proposals would require government action.

14. The Riksbank and FI each receive information about domestic cyber threats and incidents from regulatory reports, other government agencies and external suppliers. As an FMI itself through its provision of RIX-RTGS, the Riksbank receives incident reports and also

[5] The NFCERT organization provides threat intelligence to financial institutions in Norway and Denmark. Participation in this initiative would be an alternative to setting up a similar mechanism for the Swedish financial sector.

subscribes to external threat intelligence information from a range of outsourcing providers. FI's most important source of information is event reports, required by regulation from payment services providers (with defined thresholds)[6] and from other regulated firms under general guidelines regarding reporting of events of material significance (no defined thresholds). FI also receives information through regular operational risk assessments and routine supervisory dialogue with the institutions under supervision. The Riksbank also receives information through its representation in different forums on a national level with peers in the financial industry and national security authorities. FI receives financial institutions' reported incidents under the NIS directive from the Swedish Civil Contingencies Agency (MSB), the local CERT-SE. General threat reports from different antivirus vendors are received by both authorities. Incident information and other cyber threat intelligence is shared within the Financial Stability Council.

15. The Riksbank and FI both participate in regional (Nordic) and international fora where cyber incident sharing takes place. The EU´s Cybersecurity Strategy, adopted in 2020, provides common ground for cooperation, as does the Digital finance package containing inter alia a Digital finance strategy and a regulation on digital operational resilience in the financial sector (DORA).

16. The Riksbank does not routinely share with, or receive information from, other jurisdictions but is represented in different forums on international levels, for example with the Euro Cyber Resilience Board (ECRB). The Riksbank is recorded as attending two of the five meetings that the ECRB has held since it was established in March 2018. At the ECRB meetings commercial threat intelligence providers, Europol and the European Union Agency for Cybersecurity (ENISA) deliver presentations on the latest cyber threat landscape and the outlook for ECRB members. In early 2020 the ECRB launched a Cyber Information and Intelligence Sharing Initiative (CIISI-EU).

17. FI receive information from ENISA and the European Systemic Risk Board (ESRB). There is also cooperation on the Nordic level, for example within the Nordic-Baltic central bank meetings on payment and settlement systems. In addition, FI shares and receives information on cyber incidents with/from supervisory colleges and is the only Nordic country represented on the Cybersecurity & Operational Resilience sub-group of the Senior Supervisors Group for international supervisors.

18. Following a decision by the Riksdag, FI has had responsibility for crisis preparedness in the Swedish financial sector since 1995. In 2021 a state inquiry proposed a new structure for the Swedish civil defense; ten different sectors are created consisting of several authorities with one authority designated as the sector-lead. The inquiry proposed that a sector for financial services should be created consisting of the SNDO and FI, the latter as the sector lead. As an authority under the parliament, the Riksbank is not a permanent member of the sector but will work very closely with it. FI will be tasked with cooperating with the Riksbank and the MSB regarding

[6] Regulations and General Guidelines regarding activities of payment service providers (FFFS 2018:4).

crisis preparedness. This new structure entered into force on 1 October 2022 granting FI the responsibility to coordinate crisis preparedness and civil defense within the financial services sector.

19. Public-private information sharing is facilitated by the Forum for Information Sharing on Information Security in the Financial Sector (FIDI-FINANS) and The Financial Sector's Public-Private Cooperation Group (FSPOS). The meetings and information sharing with FIDI-FINANS are regulated by rules set up by the MSB. The operations of the FSPOS are governed by a three-year plan that is approved by the CEOs, Directors General or their equivalents of the participating organizations. The main goal of FSPOS is to strengthen financial infrastructure through cooperation and information sharing. The major banks, financial market infrastructure providers and insurers are represented on each, as are the financial authorities. FIDI-FINANS also has representatives from all the public authorities interested in information and cyber security.

20. In the private sector the major banks have established effective and swift communications between themselves about cyber incidents. Specifically, CISOs are meeting monthly to share information and knowledge and quickly calling each other when cyber incidents are discovered which may impact on other banks. Our interviews with financial institutions confirmed that this mechanism works well, with immediate CISO to CISO calls when needed. Smaller banks who are members of the Swedish Banking Association have meetings every two months where information is shared between themselves and the major banks on cyber issues.

Assessment

21. Responsibility for cyber risk management and interagency cooperation is spread across several different agencies and authorities, making coordination difficult. MSB has overall responsibility for cyber security risk coordination at a national level, but there are six other government agencies with a cyber-security mandate from government. Separately, the four financial authorities have an interest in setting a cyber security risk management strategy for the financial sector. Against this backdrop of multiple agencies and authorities with an interest in cyber security risk management we note a lack of clarity about each government agency and financial authority's specific responsibilities with respect to cyber security risk management. This is widely recognized, indeed the Riksbank raised concerns in the March 2021 Financial Stability Report[7] that "*…responsibility…is spread across several different authorities… This may make it difficult to coordinate the work on cyber risks affecting the financial sector.*" Riksbank's comments echo those made by Oliver Wyman in a wide-reaching report commissioned by FI to provide an external perspective on the Swedish ecosystem around cyber risk in the financial sector. Their report, published in August 2020[8] noted that "*…some uncertainty exists around how* [the functions required in a well-prepared cyber risk ecosystem] *within the financial sector are distributed.*"

[7] Financial Stability Report 2021:1 (riksbank.se)

[8] Combatting the Cyber Threat in Sweden (fi.se)

22. Despite this widespread recognition of the problem, no single authority or collection of authorities would appear to be charged with finding a solution. Any confusion of responsibilities will quickly become problematic in the event of a cyber incident affecting the financial sector at which time clarity of roles is essential and cooperation at a premium.

23. Barriers exist to sharing cyber security information between government agencies and the financial authorities. We were assured information sharing between the Riksbank and FI in respect of cybersecurity oversight works well, but wider communication and information sharing between the financial authorities and government agencies is inconsistent and subject to perceived legal constraints. Information sharing was noted as problematic during the FSC's cyber crisis exercise (see below). Information sharing between financial sector companies and the security authorities is to be covered in the Financial Sector Cyber Security Strategy. Information sharing between financial sector authorities will not be covered by the strategy. However, barriers have already been identified, for example concerns about sharing between financial authorities because of uncertainty as to whether the authority receiving the information will arrive at the same conclusions around information classification as the sending authority and uncertainty about the legality of information sharing both domestically and internationally.

24. Challenges also exist sharing cyber security information with the private sector. The working group for the Financial Sector Cyber Security Strategy has identified a need expressed by the finance sector to exchange operational information with security agencies. We welcome the decision to set up a permanent forum under the NCSC where operational information can be exchanged between authorities (such as the Security Service and the FRA) with participants from the financial sector.

25. We understand that, to date, there has been little or no direct involvement of the financial authorities in the planning for the NCSC. The national cyber security strategy is of critical importance to the financial sector, and vice versa, but no financial authorities are formally engaged in planning for or staffing the NCSC.

26. Our interviews with financial institutions revealed a lack of actionable and timely threat intelligence from government agencies that they can readily access. The MSB website sets out useful guidance material on general cyber risks and cyber security precautions accessible to all. However, the firms we interviewed told us that they turn to commercial threat intelligence providers and government agencies in other countries for actionable threat intelligence. This issue could be addressed by the forum noted above, which could develop and distribute threat assessments.

27. Firms have expressed an appetite for feedback from the Riksbank and FI summarizing reported incidents and about domestic cyber threats more generally. Our interviews with financial institutions revealed that despite providing cyber incident and other relevant information about cyber threats to the authorities, through incident reporting and routine supervisory contact, they did not receive actionable information about domestic cyber threats, trends etc. back.

Recommendations

28. The Swedish authorities (including the Government and the Riksdag) should allocate clear responsibilities for cyber security risk management and interagency cooperation in the financial sector. The financial authorities should work together to review the needs of the financial sector. The review should consider:

- The information, assistance and guidance the financial authorities need from the government agencies and from the NCSC when operational, and the roles and responsibilities they require of each of the government agencies during normal times and in the event of a cyber security incident;
- The roles of the individual financial authorities themselves during normal times and in the event of a cyber security incident—in particular who takes the lead in the event of a cyber incident, who leads on communication, who engages with other government agencies;
- An appropriate timeframe for action.

29. The Ministry of Finance should take responsibility at government level for taking forward recommendations arising from this review which are outside the scope of the financial authorities themselves.

30. The Swedish authorities (including the Government and the Riksdag) should identify and address the barriers to information sharing between government agencies, the financial authorities and the private sector: The financial authorities should work together to identify barriers to information sharing between the government agencies and the financial authorities, between the financial authorities themselves and with the private sector, and to set out proposals for how these barriers can be overcome. As some barriers have already been identified, these could be addressed without delay. For example: (i) legal 'gateways' should be established so that information about cyber-attacks can readily be shared between the financial authorities under defined circumstances; (ii) information classification schemes should be harmonized between agencies and, as part of the gateway agreements, undertakings given between agencies that the classification applied by one will be respected by all.

31. A permanent forum should be established for sharing operational information between the authorities and the private sector. We strongly support the establishment of permanent forum where operational information can be exchanged between authorities with participants from the financial sector. A model might be UK's Cross Market Operational Resilience Group (CMORG[9]), established by the Bank of England to lead sector-wide collective action on operational resilience.

[9] Operational resilience of the financial sector | Bank of England

32. The NCSC should engage fully with the financial sector as its role is developed. There are many ways in which cyber incidents could impact on Swedish society and supporting infrastructure. Society depends on the provision of food, clean water, sanitation, power, telecoms, but the financial sector will play a role underpinning each. It is therefore critical that the financial sector should engage with and help to shape the activities of the NCSC. Indeed, the financial sector should be a case study for NCSC to help define its future role and activities. The Swedish authorities may wish to reach out to established National Cyber Security Centers in Denmark,[10] Norway,[11] and the UK[12] for advice and support. In this context we note that the information sharing forum referred to above, which includes the financial authorities as well as private sector financial firms, should drive greater engagement.

33. MSB, and in due course the NCSC, should produce regular cyber threat intelligence reports available to all financial institutions. MSB, in its role as CERT-SE, has access to a wide range of cyber threat intelligence information from all sectors of the economy which could be packaged up to alert financial institutions and others about the general cyber threat landscape. Threat information should be actionable and timely. In due course this role could be taken over by the NCSC. By way of example, the UK NCSC produces weekly threat reports[13] setting out the latest cyber threat information which could be used as a reference point.

34. The authorities should routinely draw on incident reporting and other sources to identify trends and common threats and report back to financial institutions, encouraging further engagement. At present there is little incentive, other than good corporate citizenship, for financial institutions to report cyber incidents promptly because they see little in return. Effective incident reporting would see a two-way flow of information, with individual incidents reported to the authorities who would distil wider lessons for sharing back to the financial institutions.

B. Essential Services, Critical Infrastructure and Outsourcing

Current Arrangements

35. Operators of 'essential services' are required to ensure they have protective security measures in place over those essential services. Firms who are "operators of essential services" (OES) must identify themselves with the help of criteria in the national NIS Act and in regulations[14] issued by MSB. Criteria in the NIS Act are partly linked to the operator, and partly to the service provided. If the operator meets all the criteria, the operator must register as an OES to the sector-specific competent authority (FI). The operator must also establish an incident reporting

[10] Danish Centre for Cybersecurity (cfcs.dk)

[11] Norwegian National Cyber Security Centre

[12] National Cyber Security Centre - NCSC.GOV.UK

[13] Weekly threat reports - NCSC.GOV.UK

[14] MSBFS 2018:7 (now MSBFS 2021:9)

account by the MSB in its role as CERT-SE. The Protective Security Act also sets out criteria for identifying national critical infrastructures. Similar to the NIS Directive, the Protective Security Act tightens requirements for the security of IT systems at financial institutions.

36. Outsourcing and third-party risks have been a focus area for FI in recent years, and continue to be going forward. In common with those in many other jurisdictions, financial institutions in Sweden are looking to outsource more of their core operations, in particular to take advantage of the efficiencies of Cloud technology. Regulated firms are required to inform their supervisor if they are entering into a material outsourcing arrangement with a third party. In common with most regulators[15] FI take an indirect approach to supervision of outsourced arrangements and to third party risk by placing clear responsibility on the regulated firm to ensure the risks arising from the outsourced arrangement are managed appropriately. On the 22nd of June the government gave the Financial Supervisory Authority an assignment to draw up an action plan to strengthen control over the financial companies' outsourced operations. The task includes making proposals for legislative amendments that are required to achieve better control over the financial companies' outsourced operations.

37. Staff in FI's ICT Competence Centre are engaging with financial institutions to understand and assess their outsourcing arrangements. In 2021, as noted above, they undertook a review into how payment clearing operations were managing the risks associated with outsourcing. In FI's regular risk meetings that year, each bank was asked how many critical ICT third party providers they had and whether they had ensured that existing and new agreements include appropriate and proportionate ICT requirements, including cyber security. The ICT team are currently in discussions with the major banks and FMIs to understand the nature of outsourced arrangements in the wider Baltic area, against the backdrop of events in Ukraine. In 2022 a survey of outsourcing arrangements looking at how firms comply with the EBA guidelines is planned.

38. Riksbank, FI and SNDO currently gather information about essential services and material outsourcing arrangements. Information gathered through the Riksbank's oversight function is maintained in a document management system. Information about critical outsourcing arrangements is filed in FI's case management system. The SNDO asks for certain information in relation to banks' resolution planning on an annual basis in respect of critical functions.

Assessment

39. The financial authorities do not have a consistent and consolidated view of the dependencies and concentrations arising from outsourced essential services. The information that both the Riksbank and FI receive about outsourcing arrangements is not stored in a way which could readily be used to identify dependencies and concentrations. The information that SNDO holds is technically searchable as it is spreadsheet based. However, a central register of

[15] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper (fsb.org)

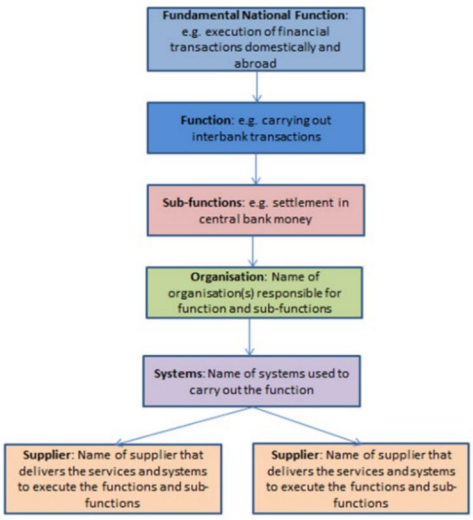
essential services, knowledge of which firms provide essential services and where outsourced third-party arrangements support those essential services would prove very valuable in the event of an incident involving one or more of those service providers, enabling the financial authorities quickly to identify the firms that would be impacted. The resulting register will most likely be of a very sensitive nature and will need to be managed accordingly.

Recommendation

40. FI should establish and maintain a central database of essential service providers and outsourced third party arrangements. A comprehensive and searchable database of essential services and material outsourcing arrangements would enable concentrations and dependencies to be identified and the associated risks to be understood and managed. This tool would be a fundamental building block for operational resilience, enabling scarce ICT and cyber security resources to be targeted towards the services, firms and supporting systems that matter most. At its simplest this register could be in the form of a spreadsheet, shared between the Riksbank and FI and starting with the category 1 firms. The information required by DORA about outsourcing arrangements would be a good reference point (description of services, service level agreements, data locations, access rights, exit strategies etc.).

41. At a more sophisticated level, a comprehensive financial sector map would help to clarify the providers of essential financial services, the dependencies on third party providers for those services and the systems they use. Norges Bank have set out a mapping model which could be applied to the Swedish financial system too.

Figure 2. Structure of Draft Financial Sector Map Produced by Norges Bank



Source: IMF Staff

C. Cyber Incident Management

Current Arrangements

42. The Financial Markets and Institutions Unit at the Ministry of Finance is responsible for handling financial stability matters related to any cyber related crisis affecting the financial sector. The Financial Stability Council has developed general crisis documentation which would be followed by the Riksbank and FI in the event of a cyber incident. Work is currently being conducted to further develop the crisis documentation to include more specific details regarding cyber-attacks. The Financial Stability department at the Riksbank has protocols to follow when a cyber incident occurs, including who to contact and what information the Riksbank expects from the banks and financial infrastructure systems.

43. During the autumn of 2021, a Cybersecurity crisis exercise was held coordinated by the Financial Stability Council. The exercise involved the Riksbank, FI, SNDO and the Ministry of Finance and was performed over two days. Each agency was represented by 8-10 employees up to head of department level. During the two days of the exercise, the agencies were required to manage a situation where large parts of the payment system were unavailable, leaving households, companies, and agencies without means of payment. The scenario started with a cyber-attack targeting a fictional clearing house for mass payments. The second day a critical third-party provider was attacked, and the effect of the attack spread to a fictional major Swedish bank. The exercise proved challenging, and to assist both, the Riksbank and the SNDO called in operational payments staff to advise how to keep payments moving. While the exercise was seen as very valuable, some questions were identified to be followed up:

- Defining the information that could and should be shared between authorities and with firms, other relevant stakeholders and the general public during a crisis, and how that information could be shared;
- Understanding the status of a financial company that is not in financial distress, but is unable to access their information and process transactions; and
- Identifying what actions could be taken by the authorities when the crisis occurs within the financial sector but does not stem from companies having traditional financial problems.

44. The financial authorities will take work forward to increase preparedness and resilience against future cyber threats by increasing their collective understanding of cyber threats and enhancing information with other relevant authorities and the private sector. Further crisis exercises on the topic of cybersecurity are planned to be undertaken in 2023.

Assessment

45. The financial authorities have no specific contingency plans or crisis protocols for a large-scale cyber-attack impacting on the Swedish financial sector. The recent cybersecurity crisis management exercise represented significant progress for the financial

authorities in understanding the challenges presented by cyber scenarios, but much remains to be done. Actions arising center on communication and cooperation under such circumstances and on identifying actions which each party could undertake to mitigate the impact of a cyber-attack.

46. The financial authorities have no current plans to extend cyber incident preparations to include participants from financial institutions. In the event of a cyber incident the authorities would not be operating in isolation from financial institutions. The reactions of financial institutions to a cyber incident may be unpredictable and hamper the authorities in their management of the situation. It is important that in times of crisis the public and private sectors can work together effectively.

Recommendations

47. The financial authorities and relevant government agencies should formalize an operational and cyber incident response framework and exercise it regularly. POR principle 3 proposes that business continuity exercises should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents. Participants should continue to include senior level decision makers so that they too are fully-prepared in the event of a significant cyber incident.

48. The authorities should consider extending cyber incident management exercises to include participants from the private sector. As an example, for many years the UK has run sector cyber simulation exercises (SIMEX)[16] involving both public and private sectors to explore the effectiveness of communication and coordination channels, and how the differing reactions of the financial sector to the scenario might impact on the sector as a whole. SIMEX rehearses the UK's Cross Market Business Continuity Group, an executive level group chaired by the Bank to enable the UK financial authorities (Bank of England, Prudential Regulation Authority, Financial Conduct Authority and HM Treasury) to interact with the sector during times of major operational disruption. CMBCG is therefore effectively the in-crisis parallel to the out-of-crisis CMORG, discussed above. Still in the UK, the Financial Policy Committee is piloting cyber stress testing,[17] a deeper form of simulation where participating firms are asked to demonstrate how they would recover payments under a pre-defined severe but plausible scenario.

D. The Regulatory Framework

Current Arrangements

49. The current legislative framework addressing cyber risks for the financial sector is fragmented with very few explicit mentions of cyber risk. In Sweden general provisions requiring financial entities to identify, measure, control, internally report and verify the risks

[16] Sector Simulation Exercise: SIMEX 2018 Report | Bank of England

[17] 2022 cyber stress test: Retail payment system | Bank of England

associated with their operations are set out in primary legislation.[18] Provisions that are to be applied to cyber risks are also found in EU legislation and guidelines, including the EBA guidelines on ICT and security risk management and on outsourcing arrangements. FI have issued regulations for the banking sector based on the EBA guidelines.[19] EIOPA has issued similar guidelines for insurance. The NIS directive governing security of network and information systems was implemented in Sweden in 2018 and the Swedish Civil Contingencies Agency (MSB) and FI have set out complementing provisions (MSBFS 2018:7 and FFFS 2014:5). In addition, the Swedish Protective Security Act, which came into force on 1 April 2019, places stricter cybersecurity requirements on financial institutions.

50. The recently adopted EU NIS2 Directive and Digital Operational Resilience Act (DORA) will help to address the fragmentation, in particular by standardizing reporting of ICT incidents. The NIS2-directive replaces the NIS-directive and lays down measures with a view to ensuring a high common level of cybersecurity within the European Union, requiring Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs). NIS2 also lays down cybersecurity risk management and reporting obligations for certain entities and lays down rules and obligations on cybersecurity information sharing.

51. The recently adopted DORA-regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience. Major ICT incidents will require reporting to the competent authority (in this case FI), who will provide details of the event to the EBA, ESMA or EIOPA as appropriate and the ECB who will assess and pass the information on. The precise definition of 'major' has yet to be determined, but it will be common across all EU countries. The scope of the DORA regulation is broad and covers all kinds of financial institutions. It sets out requirements in relation to:

- Information and Communication Technology (ICT) risk management;
- Reporting of major ICT-related incidents to the competent authorities;
- Reporting of major operational or security payment-related incidents to the competent authorities;
- Digital operational resilience testing;
- Information and intelligence sharing;
- Measures for sound management by financial entities of the ICT third-party risk;
- Contractual arrangements concluded between ICT third-party service providers and financial entities;
- The oversight framework for critical ICT third-party service providers when providing services to financial entities; and

[18] Securities Market Act (SFS 2007:528) (chapter 8 § 4, chapter 13 § 2 and chapter 20 § 1), Banking and Financing Business Act (SFS 2004:297) (chapter 6 § 2) and Insurance Business Act (SFS 2010:2043) (chapter 10 § 6)

[19] FFFS 2014:1 (governance, risk management and control at credit institutions), FFFS 2014:4 (management of operational risks) and FFFS 2014:5 (information security, IT operations and deposit systems).

- Rules on cooperation among competent authorities and rules on supervision and enforcement by competent authorities in relation to all matters covered by the Regulation.

52. As a regulation, the legislative act is directly applicable in all Member States when it will start to apply on 17 January 2025.

Assessment

53. Once DORA and the NIS2 Directive are fully applied there are likely to be inconsistencies between the new EU legislation and the Swedish legislative and regulatory framework which will need to be addressed. Swedish primary legislation, including the Protective Security Act, PSD2 (subject to upcoming review), DORA and NIS2 will all need to be considered and some aspects of the national legislation and domestic guidance may need revision in areas where they overlap with DORA and/or NIS2.

Recommendation

54. The financial authorities should undertake a detailed review of domestic legislation and regulations to identify gaps and address inconsistencies. The financial authorities are aware that such a review will be needed and has commenced this work. There is a two-year period from the Act being agreed before it comes into force, but there is much to be done as the review will require line by line assessment of domestic legislation and guidelines to ensure they are consistent with European legislation and the reissue of guidelines that are aligned.

E. Oversight and Supervision

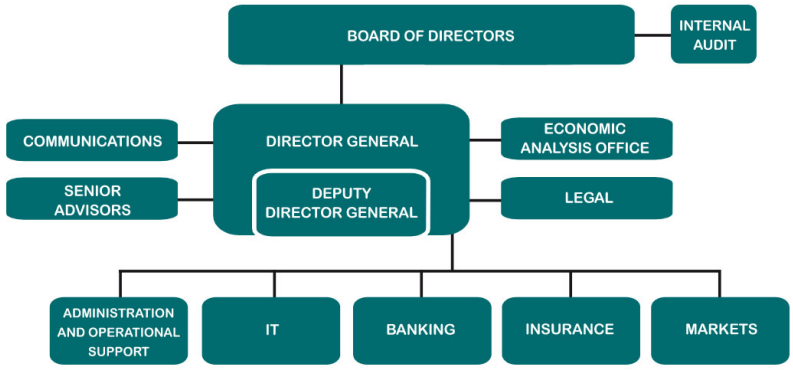
Current Arrangements

55. The Riksbank oversees the Swedish Financial Market Infrastructures (FMIs), while FI is the single integrated regulator covering the Swedish banking, securities and insurance sectors. The Ministry of Finance manages the governmental affairs on financial market matters. Oversight and supervision, including the supervision of cyber risks within the financial sector are delegated to FI. The Riksbank does not have a specific function or unit for the oversight of cyber risk in the financial system, but within the Riksbank's Markets and Infrastructure Division in the Department for Financial Stability, the team that oversees financial market infrastructures includes oversight of cyber risk. A second team works with the TIBER framework, covering banks as well as financial market infrastructure providers.

52. In FI, the Banking area (Operational Risk department) has the responsibility to supervise operational risk including payments, ICT and cyber risk management at banks, and credit and payment institutions. In October 2021, an ICT Competence Centre was established within the Operational Risk Department with an extended responsibility to supervise ICT and cyber risk management at all types of financial institutions, including the Insurance and Markets areas, meaning that the Banking area is responsible for all ICT and cyber risk supervision. The

supervisory responsibility of the Operational Risk department has also increased due to a new responsibility to supervise the Protective Security Act for financial institutions since December 2021.

Figure 3. Finansinspektionen Organization Chart



Source: Finansinspektionen

56. FI's supervisory review work on cyber risk is risk-based, grounded in legislation and aligned to the NIST Cyber Security Framework. A risk-based approach is applied by the staff in the ICT Competency Centre to direct scarce resources to where they judge the greatest risks are. Operational and cybersecurity risk supervisory reviews are based on the EBA SREP ICT Guidelines, mapped to the capabilities set out in the NIST Cyber Security Framework (Identify, Protect, Detect, Respond and Recover). Each year FI publish a memorandum setting out their most prioritized risks. ICT risk continues to be a prioritized risk area. Key cyber risk reviews in recent years include:

- In 2018 FI published a report[20] setting out conclusions drawn from the supervision of information and cyber security carried out related to banks in 2017 and 2018.
- In 2020 FI published a report21 setting out conclusions drawn from its supervision of the banks' continuity management during the years 2018 and 2019.
- In 2021 FI announced that they would look into how firms conducting payment clearing operations were managing the risks associated with outsourcing and how they maintained good internal governance and control of their operations. Additional reviews were carried out, including a thematic review across four large firms, looking at the process by which firms had identified which assets are critical and should be prioritized for protection from cyber-attack (NIST category: 'Identify').

[20] FI Supervision No. 9: Information and Cyber Security work in Banks

[21] FI Supervision 18 - Continuity management at banks

- In 2022 the ICT team plans to review how the largest firms protect themselves from attacks, ensure their operational reliability and monitor their subcontractors (NIST category "*Protect*").

57. Other reviews are planned for 2022. Some are subject to successful recruitment, while others may be deferred as a result of additional work necessary to follow up developments in the Ukraine and assess the potential impacts on the Swedish financial sector. Resources may also be diverted to look into individual events at firms when they have reported an incident (each member of the team is assigned to specific firms so supervisors know who to contact).

58. Supervisory review takes the form of a combination of regular meetings discussing ICT and operational risk reports, and onsite inspections into prioritized areas. FI supervisors receive and analyze operational and ICT risk reports from the banks 2–4 times per year depending on firm category. This information is used to drive specific risk-focused discussions in the regular supervisory meetings with the firm. For the supervisory priority areas onsite inspections are performed covering both the governance and the operational effectiveness of the ICT risk control framework. We were informed that onsite inspections typically involved two weeks onsite—the first taking the form of meetings, followed by a period of office-based analysis, then a second week onsite during which deeper testing was undertaken, including demonstrations of key systems and controls and testing to evidence their effectiveness.

59. Threat-led penetration testing under the TIBER-SE framework is a key financial stability and supervisory tool and has been performed at several of Sweden's major financial institutions. TIBER-EU (Threat Intelligence-Based Ethical Red Teaming) is a framework developed by the ECB from the UK's CBEST framework that makes it possible to test, in a standardized way, resilience to cyber risks among players in the financial system. The test (known as red team testing) involves the controlled simulation of a cyber-attack on an organization's employees, processes and technology. The test is not 'pass or fail,' but is aimed at identifying shortcomings so that resilience can then be improved. In 2019 the Riksbank adopted the TIBER-EU framework and published guidelines for Sweden's national adaptation, TIBER-SE. The main aims of TIBER-EU are:

- To strengthen resilience to cyber threats in the financial sector,
- To standardize and harmonize the implementation of red team testing within the EU,
- And to provide support for cross-border tests.
- Participation in the TIBER-SE program is voluntary but binding once agreed.

60. The budget for FI's ICT and cyber risk supervision resource has been increased but it is proving difficult to recruit appropriately skilled individuals. There are currently five experienced ICT and cybersecurity staff in the ICT Competence Centre with joint responsibility for supervising operational risks, ICT risks and national protective security across Banking, Markets and Insurance. The addition of the two departments and a general reprioritization of ICT and cyber risk

supervision led to a significant increase in budget for the ICT Competence Centre. Two groups are now budgeted within the Operational Risk Department, each to consist of 8 experts and one manager. Additional resource (3FTE) has been budgeted to support FI's additional responsibilities under the National Protective Security Act, but these will not be on the supervision side. Four new staff, two senior, have been hired and are expected to join the ICT competence center in the Summer. However, many of the positions are vacant at the time of our visit, including one manager position, as it is proving difficult for FI to attract candidates of the right quality in a highly competitive environment for ICT experienced hires.

Assessment

61. The supervisory approach adopted by the ICT Competence Centre has a sound base in EU and Swedish legislation and guidelines issued by FI for ICT risk management and control. Furthermore, the mapping to the capabilities in the NIST Cyber Security Framework (Identify, Protect, Detect, Respond and Recover) ensures that each of these important areas are covered over time in review work. The TIBER-SE threat-led penetration testing programme has been very well received by participant firms and covers the 'Protect' and 'Detect' NIST categories. In our interviews participants in the programme told us that they found the approach complimented rather than duplicated their own red team testing and that they had learned valuable lessons from the exercise.

62. Supervisory reviews are detailed and are generally found to be useful to the financial institutions we interviewed. In common with other regulators, it is challenging for FI to attract staff who are at the cutting edge of technological developments, and this kind of resource may not be needed full time. Resource constraints in the ICT Competence Centre limit the number of reviews which can be undertaken each year.

63. The significant increase in budget for the ICT Competence Centre in FI is welcome, but there are barriers to recruitment. The five staff in the ICT team are experienced and our interviews with financial institutions generally confirmed that they are well regarded by peers. However, significantly greater resources are needed to provide adequate coverage of this increasingly important area. With more staff the ICT team could accelerate coverage of larger firms and improve coverage of smaller firms. We therefore welcome the increase in budget allocation, increasing the headcount available to the ICT Competence Centre from five to 18. However, FI is not attracting sufficient numbers of appropriately skilled and experienced applicants to advertised roles, so recruitment is slow, with only four new staff due to join in the Summer.

Recommendations

64. FI should investigate innovative means by which supervision resource can be augmented such as secondments and use of existing powers to appoint auditors. Recruitment on the scale required will place a substantial burden on existing staff so we recommend that recruitment is phased and alternative resourcing investigated. Furthermore, technological advances in financial institutions can be difficult for regulators to keep up with. Other financial

authorities have found success in seconding in resource from industry and/or consultancy firms (an approach that has been successful in the UK) to augment staff numbers, refresh technical skills and bring in new skills.

65. Furthermore, FI has the power[22] to appoint and instruct an 'auditor' (i.e., an external specialist) to 'audit' (review) a financial firm under its supervision but has only used this power to a limited extent. Other jurisdictions have found this a useful way to (i) augment limited internal resources and (ii) access highly specialized skills that would be uneconomic to retain in-house. FI should consider increased use of this power.

[22] Chapter 13, section 9 of the Banking Act, Chapter 23, section 7 of the Securities Markets Law and Chapter 17, section 11 of the Insurance Business Act.