INTERNATIONAL MONETARY FUND

IMF Country Report No. 23/280

ICELAND

FINANCIAL SECTOR ASSESSMENT PROGRAM

July 2023

TECHNICAL NOTE ON CYBER AND OPERATIONAL RESILIENCE, SUPERVISION AND OVERSIGHT

This paper on Iceland 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 June 21, 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

ICELAND

FINANCIAL SECTOR ASSESSMENT PROGRAM

June 21, 2023

TECHNICAL NOTE

CYBER AND OPERATIONAL RESILIENCE, SUPERVISION AND OVERSIGHT

Prepared By
Monetary and Capital Markets Department, IMF

This Technical Note was prepared by Nick Strange (IMF external expert) in the context of a Financial Sector Assessment Program (FSAP) mission for Iceland, led by Etienne B. Yehoue. 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
CBI	Central bank of Iceland
CERT-IS	Computer Emergency Response Team (Iceland)
Committee	Financial Stability Committee (of the CBI)
Council	Financial Stability Council
CPMI	Committee on Payments and Market Infrastructure
CSC	Cyber Security Council
CSO	Chief Security Officers
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECOI	Electronic Communication Office of Iceland
EEA	European Economic Area
eID	Electronic Identification system (Auðkenni),
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities & Markets Authority
FMI	Financial Market Infrastructure
FSA	Financial Supervisory Authority (now part of CBI)
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
MoF	Ministry of Finance and Economic Affairs (*Fjármála-og efnahagsráðuneytið*)
MoHESI	Ministry of Higher Education, Science, and Innovation *(Háskóla-, iðnaðar-og nýsköpunarráðuneytið)*
NBFI	Non-Bank Financial Institution
NCIP	National Commissioner of Icelandic Police
NF-CERT	Nordic Financial CERT
PFMI	CPMI-IOSCO Principles for Financial Market Infrastructures
POS	Point of Sale
PSD2	Payment Services Directive
RB	Reiknistofa bankanna
RTGS	Real-Time Gross Settlement
SEPA	Single Euro Payments Area
SREP	Supervisory Review and Evaluation Process
SURF	Samstarfsvettvangur Um Rekstaroryggi Fjarmalainnvida (a public/private collaboration forum on cyber matters)
TIBER	Threat-led Intelligence Based Ethical Red teaming

EXECUTIVE SUMMARY

The Icelandic financial system is large, concentrated and interconnected - banks and Non-Bank Financial Institutions (NBFIs) - domestically and internationally. There are 10 banks: 4 commercial banks and 6 savings banks, but the system is dominated by just three of the commercial banks (Arion banki, Íslandsbanki and Landsbankinn) that together account for 95 percent of banking assets. Cash use is declining as a percentage of point of sale (POS) transactions, leading to an increasing dependence on electronic payment means. The debit and credit cards used for most retail transactions rely on international communications with Visa and Mastercard.

The Icelandic financial sector has not experienced seriously disruptive cyber-attacks or operational issues in recent years, but threats are growing. The migration by the Central Bank of Iceland (CBI) of domestic payments to a new core payment system is almost complete, considerably enhancing its cyber resilience. However, in common with all jurisdictions, Icelandic financial institutions have seen increased levels of cyber-attacks, particularly Distributed Denial of Service (DDoS) and social engineering (phishing etc.) attacks. One major Icelandic bank' website was faked, allowing fraudsters to harvest log-in details and withdraw funds. Contingency planning, emergency preparedness and response in the finance sector must take note of the possibility of wider, more diverse and destructive attacks in the future.

Iceland's dependence on international connectivity for both debit and credit card systems introduces a significant vulnerability into the payment system. During the Icelandic banking crisis of 2008/9 Icelandic debit cards ran on domestic systems. The individual decisions by two major acquirers (now known as Teya and Rapyd) to rely on debit card processing by Visa and Mastercard have reduced the operational independence of the Icelandic financial system. CBI and relevant authorities are investigating alternative domestic retail payment solutions for use in the event of a significant disruption to the credit and debit card system. With cash as the only currently available fallback, CBI should work with payment system providers and retail stores to refine contingency plans and test how cash will be distributed and used in a crisis situation.

There is no dedicated cyber security strategy for the finance sector. The Ministry of Higher Education, Science & Innovation (MoHESI), responsible for centralised cyber security matters and coordination across sectors, published a revised Icelandic National Cybersecurity Strategy in February 2022 and a supporting action plan in November 2022, but this is not sector specific. Further, while the role of each of the authorities and institutions with respect to the cyber security may be gleaned from relevant legislation and/or implied by their wider role, there is no central document setting out how the cybersecurity of the financial sector is safeguarded**.** A clearly articulated strategy would provide guidance and context for more detailed actions to preserve the cyber and operational resilience of the sector, ensuring that the actions of the Ministry of Finance & Economic Affairs (MoF), CBI and other participants were aligned towards common goals. The authorities should work together to produce a financial sector specific cyber security strategy, clearly setting out the roles and responsibilities of each party.

The Financial Stability Committee (the "Committee") of the CBI has a broad remit which represents an opportunity to take a leading role in operational resilience with regard to cyber security risk mitigation. The Financial Stability Committee should consider developing a cyber and operational risk agenda in support of its broad financial stability objective, with appropriate involvement of the Financial Stability Council.

Internationally CBI participates in a number of information sharing fora, particularly across the Nordic region, while domestic arrangements are continuing to develop. The Icelandic Computer Emergency Response Team (CERT-IS) is part of the Electronic Communications Office of Iceland (ECOI), an independent body under MoHESI's administrative scope. CERT-IS has recently received additional resources and an expanded remit. The MoHESI leads the Cyber Security Council, an information sharing forum of different ministries and institutions (including CBI and MoF). Arrangements are in development for formal cooperation and coordination between the financial sector authorities and the private sector in relation to cyber risk matters through CBI's SURF (a public/private collaboration forum on cyber and operational risk matters where MoF and CERT-IS participate). We encourage the Icelandic authorities to continue to consolidate cyber security efforts and coordination across the administration, and to emphasize the importance of the services that CERT-IS offers to all sectors, and the financial sector in particular.

There is some confusion about who would lead the financial sector's response to a major cyber or operational incident. The Financial Stability Council (MoF and CBI) is tasked with formal contingency response for the finance sector. The common coordination plan for times of disruption is under collective revision at the level of experts in CBI's SURF. MoF and CBI should expedite the development and dissemination of the common coordination plan. By request of the CBI and SURF, CERT-IS recently led a cyber security scenario 'table-top' exercise exploring collaboration and coordination in the event of a ransomware attack. Financial institutions involved found it to be very valuable and there is an appetite for more. We also encourage CBI, SURF and CERT-IS to arrange further and regular cyber security scenario exercises to strengthen cooperation and coordination, expanding the range of financial institutions and government agencies involved.

Operational risk experts in CBI are experienced and well regarded by financial institutions, but more resources are needed to provide adequate coverage of this increasingly important area. CBI should gradually increase the resources for specialist supervision of operational, ICT and cyber risk at regulated firms and should use the power to appoint external auditors to augment its limited internal resources for cyber risk reviews.

The supervision of financial institutions' cybersecurity is highly dependent on self-assessments by the regulated entities themselves and independent reviews carried out by third parties. The lack of on-site visits and/or robust challenge to the assertions made in third party reports increases the risk that weaknesses are missed. CBI should commence on-site examination of operational, Information and Communication Technology (ICT) and cyber risk at regulated firms to obtain fuller picture on cyber preparedness, starting with the systemically important institutions and widening coverage as increased resources for specialist supervision allow. The planned introduction

of Threat-led Intelligence Based Ethical Red teaming (TIBER) penetration testing in Iceland will provide valuable additional insight into cyber risk vulnerabilities.

Many of the regulations governing ICT systems were summarised in the guidelines issued by the Icelandic Financial Supervisory Authority (FSA), but these cover legislation extant in early 2019. The supervisory guidelines on ICT systems should be subject to regular review and updating, in particular in respect of Payment Systems Directive 2, the Digital Operational Resilience Act (DORA) and the Basel Principles for Operational Resilience.

Supervisors conducted an exercise in 2019 to identify critical operations and critical third-party providers. CBI should regularly revise the list of critical operations and critical service providers for internal use and for presentation to the Financial Stability Committee and Financial Stability Council.

No formal summary or trend reports are created summarizing cyber and operational incidents and trends. CBI is encouraged to enhance its incident dashboard by summarizing cyber incidents and examining trends.

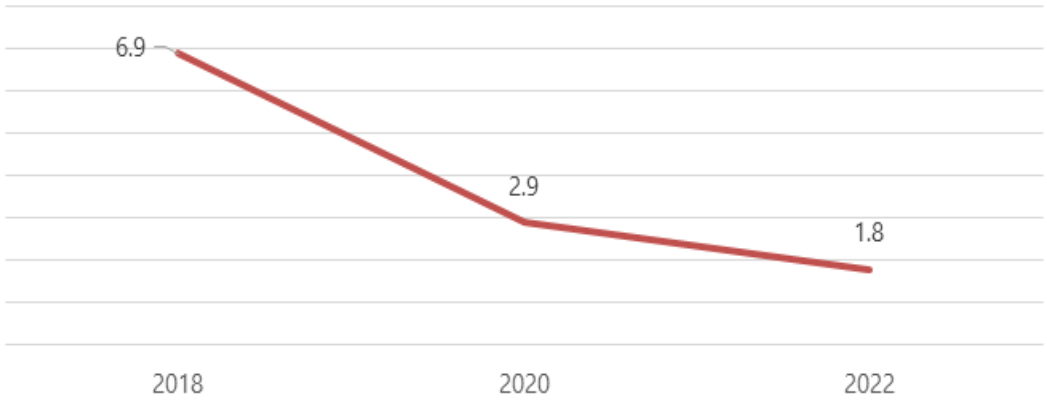
	Table 1. Iceland: Key Recommendations			
#	**Recommendations**	**Paragraph Reference**	**Responsible**	**Timing**
	Payment systems, schemes and instruments			
1.	CBI to work with payment service providers and retail stores to refine contingency plans and test how cash will be distributed and used in a crisis.	15	CBI	I
	Financial sector cyber security oversight			
2.	MoF and CBI to produce a financial sector specific cyber security strategy, clearly setting out the roles and responsibilities of each party.	22	MoF/CBI	I
3.	The Financial Stability Committee to consider developing a cyber and operational risk agenda in support of its broad financial stability objective, with appropriate involvement of the Financial Stability Council.	22	CBI/MoF	I
4.	MoF and relevant authorities to continue to consolidate cyber security efforts and coordination at government level and to emphasize the importance of the services CERT-IS offers to all sectors, and the financial sector in particular.	28	MOF	ST
5.	MoF and CBI to expedite revision of the common coordination plan for the financial sector in the event of a major incident.	36	CBI/MoF	I
6.	CBI, SURF and CERT-IS to arrange further and regular cyber security scenario exercises to strengthen cooperation and coordination, expanding the range of financial institutions and government agencies involved.	36	CBI/CERT-IS	ST
	Supervisory arrangements and practices			
7.	Supervisory guidelines on ICT systems to be subject to regular review and updating.	38	CBI	I
8.	CBI to gradually increase the resources for specialist supervision of operational, ICT and cyber risk at regulated firms and should use the power to appoint external auditors to augment its limited internal resources for cyber risk reviews.	42	CBI	ST
9.	CBI should commence on-site examination of operational, ICT and cyber risk at regulated firms to obtain fuller picture on cyber preparedness, starting with the systemically important institutions and widening coverage as increased resources for specialist supervision allow.	52	CBI	ST
10.	CBI to regularly revise the list of critical operations and critical service providers for internal use and for presentation to the Financial Stability Committee and Financial Stability Council.	52	CBI	I
11.	CBI is encouraged to enhance its incident dashboard by summarizing cyber incidents and examining trends.	54	CBI	I
I Immediate (within 1 year); ST Short term (within 1-2 years); MT Medium Term (within 3−5 years)				

INTRODUCTION

1. The Icelandic financial system is large, concentrated and interconnected - banks and NBFIs - domestically and internationally. There are 10 banks: 4 commercial banks and 6 savings banks, but the system is dominated by just three of the commercial banks (Arion banki, Íslandsbanki and Landsbankinn) that together account for 95 percent of banking assets. It is also dependent on internet access. While the domestic banks have very limited cross-border operations, Icelandic debit and credit card transactions and a securities settlement system are processed/operated offshore by Visa and Mastercard and NASDAQ CSD respectively.

2. Cash use in Iceland is declining leading to an increasing dependence on electronic payment means. A survey conducted by Gallup in spring 2022 for the CBI revealed that 98% of respondents who shop at points of sale on a weekly basis or more often use electronic payment instruments, an increase from previous surveys. Cash tends to be used for gifts and other person to person payments. CBI expects that cash use at points of sale will continue to drop. However, cash is still widely available and accepted as a means of payment and, for as long as there is public demand for cash and as cash is the only fallback in payment system crisis CBI will continue to provide it. Icelandic consumers and Icelandic society in a wider context therefore rely heavily on electronic payment means. This increased digitization widens the potential cyber-attack surface. Almost all (98.6%) electronic payments at point of sale are card payments, of which 37.8% are digital cards stored in a smart device. Only 1.4% of electronic payments are made by other means, including online bank transfers and buy-now-pay-later schemes.

Figure 1. Iceland: Use of Cash Payments at Points-Of-Sale (In Percent)[1]



1. Responses from those who use a payment solution at least weekly.

Sources: Gallup, Central Bank of Iceland.

3. The Icelandic financial sector has not experienced seriously disruptive cyber-attacks or operational issues in recent years. A significant DDoS attack in August 2021 disrupted the

functioning of two of the three main providers of card services and the availability of electronic identification (eID) services used for authentication. Most payment services were recovered within two hours. We understand that since that attack the commercial banks have diversified DDOS protection provision and increased capacity. In common with all jurisdictions, social engineering attacks (phishing etc.) occur frequently. In Summer 2022 the web site of one of the three large Icelandic banks was copied, harvesting log in details, and resulting in some loss for customers. The bank concerned compensated customers for any losses. The banks have in recent years been upgrading many of their core payment systems. That has created some disruptions of service; however, this disruption has not been significant. Winter storms can lead to power outages in more remote parts of the country that may temporarily disrupt connectivity for people living in these areas.

4. This note focuses on the cyber and operational resilience of the financial system and the supervisory and oversight frameworks for systemically important financial institutions in Iceland. The cyber resilience of the financial system is addressed from (i) a sector-wide perspective - how the authorities work together to ensure the cyber and operational resilience of the financial system as a whole, with a key focus on payment systems; and (ii) a firm-specific perspective - how supervisors at the CBI review the cyber and operational resilience of systemically important regulated firms. CBI's Real-Time Gross Settlement system (RTGS), the three systematically important banks (Arion banki, Íslandsbanki and Landsbankinn) and the Icelandic Stock Exchange (*Kauphöll Íslands*) have so far been listed as systemically important. This note sets out an assessment of the work of the CBI, MoF and other authorities in the areas of cyber security strategy, cooperation and coordination; information sharing; contingency planning, incident management and exercising; and supervisory arrangements and practices. The review is based on questionnaire answers provided by the CBI and MoF, interviews with the CBI, MoF and supervised financial institutions and the study of relevant national laws and reports published by the authorities.

5. The basis for this review was derived from international guidance and regulatory good practice. As there are no enforceable international regulatory standards on cyber security risk, the mission team used guidance material developed by standards-setting bodies and regulatory good practice as the basis of this note. The following benchmarks were used: The Basel Committee for Banking Supervision's (BCBS) 'Principles for Operational Resilience' and the revision of the 'Principles for the Sound Management of Operational Risk' (both March 2021) and 'Cyber-resilience: Range of practices' (December 2018); the Financial Stability Board's 'Stock take of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices' (October 2017) and Discussion Paper on 'Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships' (November 2020); the IMF's Departmental Paper on Cybersecurity Risk Supervision (September 2019), the G7's 'Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector' (October 2017) and the Committee on Payments and Market Infrastructure/ International Organisation of Securities Commissions' (CPMI-IOSCO) 'Guidance on Cyber Resilience for Financial Market Infrastructures' (June 2016).

PAYMENT SYSTEMS, SCHEMES AND INSTRUMENTS

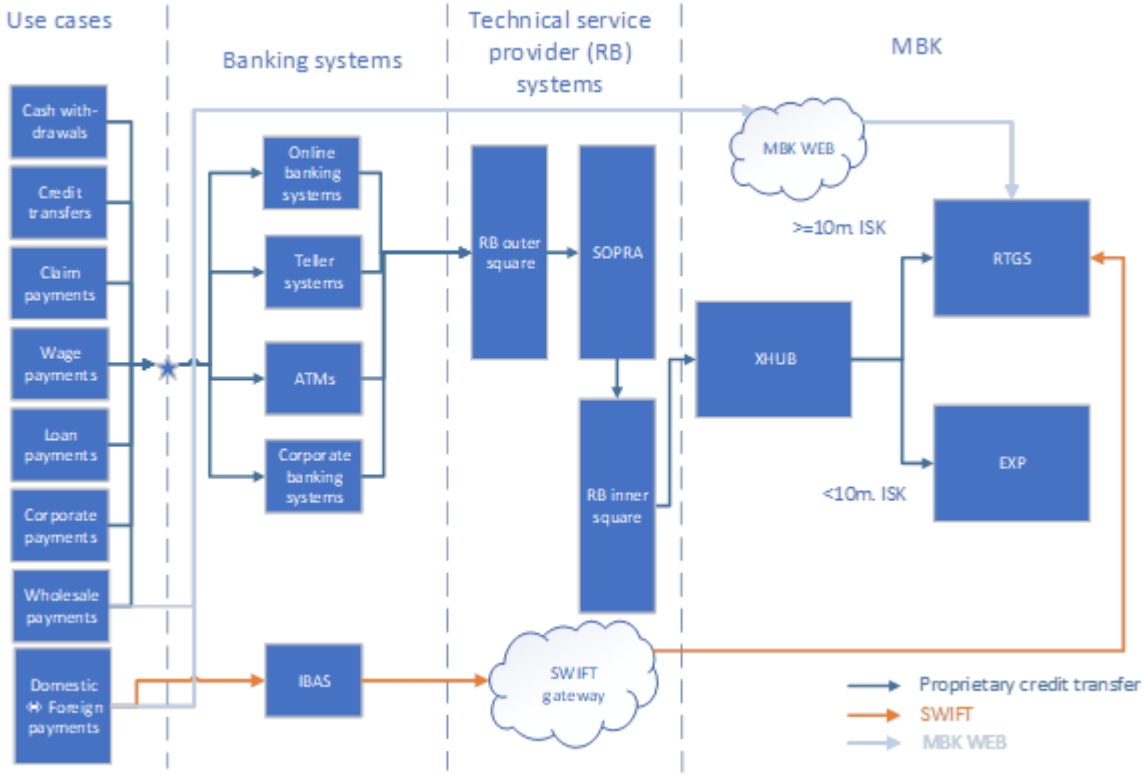
Current Arrangements

6. CBI operates the country's interbank payment system, MBK, key elements of which are outsourced to third parties. The Icelandic payment interbank clearing landscape is set out in Figure 2 below. Participants of the MBK are CBI itself (which also serves as a commercial bank for the Treasury), the domestic commercial and savings banks and two foreign financial institutions (Euroclear and Clearstream). MBK is Iceland's most systemically important FMI. Its technical operation, as well as it's monitoring outside opening hours of the system's gross settlement component, is outsourced to Reiknistofa bankanna (RB), a joint venture entity owned by the CBI and the commercial banks. RB provides the technical interface between the commercial banks and the CBI's two clearing and settlement systems: RTGS, broadly for payments greater than 10 million ISK which operates between 8 AM and 5 PM, and the instant payment system EXP which operates 24 hours. RB's two data centers are both in Iceland, one hosted at the CBI, the other at a remote location and each has an on-site data backup. A third database site is maintained with a 24-hour delay in case of data integrity issues in the primary and secondary databases. Rather than seeing the two data centers as primary and secondary, regular switching takes place between the two. Standard cyber controls are in place over access and network separation.

7. The CBI and RB are coming to the end of a lengthy program to migrate domestic payments away from a mainframe-based core banking system to a zero-trust application to application system. The Icelandic payment infrastructure has undergone significant renovation in recent years. Three significant enhancements have taken place: (i) Implementing a new RTGS and instant payment system (MBK), completed in October 2020; (ii) updating the commercial banks' deposit systems, which the last bank finished in February 2022; and (iii) Decommissioning the old mainframe system in February 2023. This project considerably enhanced the cyber and operational resilience of the payment infrastructure.

8. The RTGS system itself was developed and is updated by a third party. The RTGS system was developed by Perago/SIA (now merged into Nexi Payments SpA, a company based in Milan) and is updated by RB using source code developed by Nexi. Production software is all hosted within Iceland, with the same redundancy arrangements as RB. In addition to processing inter-bank transactions, the RTGS system processes (cash) net settlement transactions five times a day for Nasdaq CSD. Also, the two debit/credit card schemes in Iceland, Visa and Mastercard, settle transactions on a net basis with the CBI acting as a settlement agent. MBK web is an overlay – banks can use it to monitor their positions and to manually initiate transactions, but with very limited capacity. Cross border payments in ISK flow through MBK either via SWIFT to RTGS for wholesale payments or via a proprietary format the domestic banks use for retail payments. Iceland is a participant in the Single Euro Payments Area (SEPA) and the larger banks, which participate, are SEPA-compliant for cross border payments in Euros. The systems underlying SEPA, such as STEP2-T and RT1, fall under the oversight of the European Central Bank (ECB), including for cybersecurity.

Figure 2. Iceland: Payment Interbank Clearing System



Notes: The Use cases shown are not part of the process but are examples of the types of transactions that flow through the system.

One use peculiar to Iceland is Claim payments, which are requests to pay that are initiated by the payee for a service (e.g., plumbing work). The payee makes a claim on the customer's bank account. The customer can see and individually approve the payment when they log into their bank accounts.

The Banking systems shown are hosted by the banks themselves. In practice there are many more individual systems at each bank, but these are examples of the types of system that interface with RB's service square via a web interface.

Source: CBI

9. All Icelandic credit and debit card payments operate through Visa and Mastercard, both of which process transactions outside Iceland. This offshore processing creates a reliance on the international communication infrastructure running through submarine cables to Europe. As at the start of March 2023 there are three such submarine cables, all operated by state-owned electronic communications service provider, Farice ehf. Submarine cables are exposed to cyber and physical attacks, and additionally in Iceland's case, underseas geothermal activity, however Farice is subject to security requirements which the ECOI enforces. The risk represented by dependence on the cooperation of non-domestic payment system providers was highlighted during the Icelandic financial crisis of 2008/9 when Visa and Mastercard refused to settle in Icelandic Krona. Without assurances from CBI, the clearing of credit card payments would have seized up with significant

consequences for the Icelandic payment system (see Bank for International Settlements Report in March 2020[1]). At the time, the Icelandic debit card systems were operated domestically and had continued to operate. The two major acquirers (now known as Teya and Rapyd) have since chosen for commercial reasons to rely on Visa and Mastercard processing for both credit *and* debit cards, thus eliminating the contingency fallback of a domestic system that was present in 2008/9.

10. The central securities depository for Iceland, Nasdaq CSD, processes all transactions remotely in Sweden, adding to the financial sector's dependence on communications technology.

11. Cash distribution is currently the only feasible backup to the debit and credit card systems. Although the use of cash has reduced, cash is legal tender for all payments. CBI can ensure a large enough supply of notes and coins to be used for necessary spending if electronic retail payments are interrupted. RB is the critical service provider on which authorities, banks and community rely for the distribution of cash as a fallback currency. Cash distribution through the ATM network would be compromised in the event that debit and credit card systems failed, but most domestic commercial banks have adopted a new ATM solution that does not require a payment card for cash withdrawals, but instead uses the domestic eID system for customer identification. The eID system relies on effective electronic communications and power but does not rely on the Visa and Mastercard processing systems.

12. A working group established by CBI reported in March 2022 that RB's existing contingency plan for cash distribution was robust, but concerns remained about the ability of stores to accept cash, particularly in the event of power or communication failures. Many points-of-sale are now equipped with electronic payment terminals instead of cash registers, limiting their ability to accept cash for retail transactions. During the DDOS attack referred to above, a minority of customers were able to make direct bank transfers to make purchases, but this is not seen by the authorities as a robust fallback solution – it is time-consuming, and many stores rely on self-checkout which does not support direct bank transfer.

13. Encouraged by the CBI and the National Security Council, work on the adoption of a domestic retail payment system is being expedited. Discussions about the process of implementing an independent domestic retail payment system will be referred to a Forum for the Future, whose role is to shape the vision and priorities for development of core financial market infrastructure in Iceland. The Forum will conduct a basic assessment of ideas and proposals. In addition to the Central Bank, RB, deposit-taking financial institutions and the MoF have representatives on the Forum.

Review

14. Iceland's dependencies on international connectivity and foreign payment systems introduce vulnerabilities into the payment system. The individual decisions by the two major acquirers (now known as Teya and Rapyd) to rely on debit card processing by Visa and Mastercard

[1] The banking crisis in Iceland (bis.org)

have reduced the operational resilience of the Icelandic payment system as a whole with a consequent potential impact on financial stability. Prior to these decisions the acquirers had been using RB's domestic system. In the event of a significant disruption to one or more debit and credit card systems alternative payment methods such as cash and/or direct bank transfers all have drawbacks, and direct bank transfers also rely on internet connectivity. CBI is therefore investigating alternatives for a domestic retail payment solution as a fallback in the event of significant disruption.

15. Large-scale distribution and acceptance of cash as a fallback in a crisis is untested. Given the almost total dominance of card-based payments for point-of-sale transactions a large-scale switch to cash for any length of time may uncover unexpected difficulties. During the DDOS event discussed above, consumers went to ATMs to get cash to pay at restaurants and bars, but long queues formed as not all cards worked at ATMs due to the disruption. One large bank questioned the feasibility of large-scale cash distribution. Furthermore, not all retailers are in a position to accept cash at any scale, if at all.

Recommendations

16. CBI should work with payment service providers and retail stores to refine contingency plans and test how cash will be distributed and used in a crisis. This will require cross sectoral contingency planning, especially regarding electronic communications and power, in addition to finance, and should be tested and revised on a regular basis.

FINANCIAL SECTOR CYBER SECURITY OVERSIGHT

A. Cyber Security Strategy, Cooperation, and Coordination

Current Arrangements

17. MoHESI, responsible for centralised cyber security matters and cross-sector coordination, published a revised Icelandic National Cybersecurity Strategy[2] in February 2022 and a supporting action plan in November 2022. The revised strategy covers the years 2022-2037. The strategy sets out the Government's vision and objectives regarding the state of cyber security in Icelandic society, along with indicators. The vision states that: *"Icelanders enjoy security on the Internet based on strong security culture, reliable cyber security and law enforcement, active cooperation, national and international, and comprehensive legislation that supports innovation and progress in Internet service."* The vision is supported by two objectives related to (i) competence with and use of cyber security technology, and (ii) a secure internet environment. The related action plan lists tasks to be undertaken by specified Government ministries and institutions, all of which were involved in its development. The actions assigned to the MoF are predominantly administrative and do not, for the most part, relate specifically to the finance sector. The strategy is to be reviewed

[2] Icelandic National Cybersecurity Strategy 2022-2037.pdf (stjornarradid.is)

every three years and the action plan is expected to be a living document that will be re-evaluated on a regular basis.

18. The previous (2015) strategy envisaged the establishment of a Cyber Security Council (CSC) and a Cyber Security Forum. The CSC serves the governmental forum on network and information security issues, following up on the implementation of government policy and serving as a forum for information sharing and coordination of actions in the areas of network and information security. The CBI recently became an observer to the CSC. The Cyber Security Forum was envisaged as a collaborative venue for representatives of the public bodies who sit on the Council and private enterprises to work together on cyber security issues, but never became operational in practice. An alternative consultation forum between the Government and the private sector is being rolled out (see "Information Sharing" below).

19. The Financial Stability Council (the "Council"), established by legislation,[3] is the formal co-operation forum of public authorities for financial stability. The Council meets three times a year and serves as venue for consultation, exchange of information and policy formulation with the aim to strengthen and preserve financial stability in the public interest and limit the build-up of systemic risk. The Council co-ordinates the preparedness of public authorities in financial crises. The Council consists of the Minister of Finance, who is chair of the Council, and the Central Bank Governor. In regular attendance for the CBI are the Deputy Governor of Financial Stability and the Director of the Financial Stability Department, and for the MoF, the Director General for Financial Services and the Director General for Economic Affairs. As operational risks (including cyber security) are on the rise, monitoring and coordination of contingency planning is of significant concern to the Council.

20. The Financial Stability Committee within the CBI is tasked with assessing systemic risk and strengthening and preserving financial stability. The Committee was established in 2020 and is chaired by the Governor of the CBI, with the Deputy Governors as members, together with three independents appointed by the MoF. The MoF is represented on the committee by a non-voting member. The Director of CBI's Financial Stability Department also attends. The Committee is tasked with assessing the current situation and prospects for the financial system, systemic risk and financial stability, discussing and defining the actions deemed necessary at any given time in order to affect the financial system with the aim of strengthening and preserving financial stability, and to make comments to the appropriate authorities when warranted. and it adopts administrative directives and decisions to the extent laws stipulate. Also, the Committee decides which supervised entities, infrastructure and markets are considered systemically important, and of a nature that might affect financial stability, at any given time. CBI keeps the Committee informed about cyber risks and progress on the core banking system upgrade. The Committee has not to date directed comments towards any authority in respect of cyber risk.

[3] (Act. No. 66/2014)

Review

21. There is no dedicated cyber security strategy for the finance sector. Further, while the role of each of the authorities and institutions with respect to the cyber security may be gleaned from relevant legislation and/or implied by their wider role, there is no central document setting out how together they safeguard the cyber security of the financial sector. A clearly articulated strategy would provide definitive guidance and context for more detailed actions to preserve the cyber and operational resilience of the sector, ensuring that the actions of the MoF, CBI and other participants were aligned towards common goals. Sector-specific strategies are already in place in several other Nordic countries (Denmark, Norway and Sweden).

22. In this context we note a potential role for SURF, the collaboration forum established by the CBI and including the MoF (see "Information Sharing" below). One aspect of SURF's mandate is to prepare a common vision on actions aimed at promoting resilience of critical infrastructure network and information systems. A list of actions is not a strategy, but SURF's remit could provide a sound basis from which to develop a finance sector-specific strategy. The mission is not aware that SURF has yet started to act on this part of its mandate. A clearly articulated cyber security strategy for the finance sector would, for example:

- Set out the respective roles and responsibilities of the CBI, the different Government Departments and others in strengthening the cyber security of the finance sector;
- Clarify interagency cooperation and coordination arrangements;
- Clarify incident reporting[4] and information sharing arrangements; and
- Set out clear responsibilities in the event of an incident.

23. The Committee has not so far extended its reach to include policies and recommendations with respect to the operational and cyber resilience of the financial sector. The Committee's broad remit in particular presents it with an opportunity to take a leading role in operational resilience with regard to cyber security risk mitigation. The CBI regularly update and inform the Committee about cyber risks, but no actions have yet been directed by the Committee in respect of cyber risk.

Recommendations

24. MoF should work together with the CBI to produce a financial sector specific cyber security strategy, clearly setting out the roles and responsibilities of each party.

[4] Statutory reporting of payment incidents, including cyber-attacks, is outlined in PSD2, which has been transposed in Iceland. Additionally, the three largest banks and stock exchange are obliged to report cyber-related incidents and threat to CERT-IS, as NIS1 provides (transposed in Iceland).

25. The Financial Stability Committee should consider developing a cyber and operational risk agenda in support of its broad financial stability objective, with appropriate involvement of the Financial Stability Council.

B. Information Sharing

Current Arrangements

26. CBI participates in a number of international information sharing fora. The Central Bank participates in workstreams of the European Banking Authority, European Securities and Markets Authority and European Insurance and Occupational Pensions Authority on a best effort basis. The Oversight Department of the Central Bank of Iceland cooperates and meets annually with other Nordic/Baltic central banks, including on cyber related issues. Along with the Bank for International Settlements and other Nordic central banks CBI is a member to the BIS Innovation Hub Nordic Centre in Stockholm and has an employee there.[5] CBI also participates in the BIS Innovation Network[6], and with the other Nordic central banks in the annual Nordic in Finance Cyber Conference, first held in 2017, held most recently in Iceland.

27. Arrangements are in development for formal cooperation and coordination between the financial sector authorities and the private sector in relation to cyber risk matters. The CBI has established a Collaboration Forum on the Operational Security of Financial Infrastructure (Samstarfsvettvangur Um Rekstaroryggi Fjarmalainnvida "SURF") in the Summer of 2021. This forum is led by the CBI with members from MoF, the three systemically important Icelandic commercial banks, Nasdaq CSD, Kauphöll Íslands (the Stock Exchange), CERT-IS, RB and Finance Iceland (which represents financial companies in Iceland). SURF's mandate is to:

- Formulate a common vision on actions aimed at promoting resilience of critical infrastructure network and information systems;
- Coordinate actions at times of operational disruptions that affect the financial system's safety and efficiency; and
- Organize emergency cooperation and joint emergency plans, placing emphasis on strengthening cyber security defenses and the resilience of the financial system against cyber-attacks.

SURF is very important as a venue of cooperation; however formal government preparedness is the responsibility of MoF and CBI (and the Financial Stability Council) along with other relevant Ministries and institutions.

[5] About the hub, please see here: https://www.bis.org/about/bisih/locations/se.htm.

[6] About the network, please see here: https://www.bis.org/about/bisih/network.htm.

28. In addition to SURF, which includes private sector members, CBI cooperates with Finance Iceland. Finance Iceland hosts monthly meetings between the Chief Security Officers (CSOs) of the bigger banks and payment institutions and the Central Bank has participated in those meetings. CSOs of the major telecommunication companies also participate as well as a representative from the police cyber-crime division. A functional communication channel has also been established for Chief Information Officers of larger institutions.

29. CBI is a member of the Nordic Financial Computer Emergency Response Team (NF-CERT). NF-CERT is a collaborative initiative which allows members to work together when handling cybercrime, sharing information and responding to threats in a coordinated manner. CBI uses that forum to assist in evaluating the threat and vulnerability landscape. CBI staff attend weekly online meetings and share Icelandic incident information with other Nordic countries. Many Icelandic banks are also direct members.

30. The authorities have in recent years expanded the resourcing and role of CERT-IS from a focus on telecommunications to cover all significant sectors of the Icelandic economy (operators of essential services and digital service providers). CERT-IS's aim is to conduct regular exercises with members of sectoral groups, increase information sharing and active cooperation at national level and as act as a contact point for the Icelandic government in international cooperation. Certain socially and economically important entities are required to report incidents to CERT-IS which, if relevant, has a duty to share incident information and to set up groups in each sector, including the financial sector, to share information and coordinate responses. At the time of this review, CERT-IS had held one meeting in its expanded format.

Review

31. There is broad agreement that CERT-IS has become much more effective since its scope and resources expanded in 2021, but services lag behind the more established NF-CERT. Feedback from financial institutions and supervisors alike indicates that the functional communications channel is highly regarded, immediate and very helpful. As the longest established financial sector forum, with the widest reach NF-CERT was most highly regarded. NF-CERT provides threat intelligence and information sharing, specialist technical support for incident handling, response coordination and networking opportunities. CERT-IS has recently expanded its remit from a focus on telecommunications and is now active across all NIS-regulated sectors and has duties towards government agencies. CERT-IS provides threat intelligence and information sharing and given its resources, more limited assistance in handling incidents.

Recommendation

32. We encourage the authorities to continue to consolidate cyber security efforts and coordination across the administration and to emphasize the importance of the services that CERT-IS offers to all sectors, and the financial sector in particular.

C. Contingency Planning, Incident Management and Exercising

Current Arrangements

33. ECOI and CERT-IS have a supporting coordination role in the event of a cyber incident, along with the National Commissioner of the Icelandic Police (NCIP) in case of emergency within the meaning of Act on civil protection. CBI therefore coordinates with the ECOI and CERT-IS on cyber incidents. Last October CERT-IS organised and executed an extensive exercise that the Central Bank and members from the financial sector, including RB as an important service provider, participated in. The scenario was a supply chain attack through an infected update to a fictional infrastructure system which resulted in a ransomware attack that made all ATMs and point of sale terminals inoperable. The lessons learned were discussed at SURF's December 2022 meeting. Coordination with the ECOI/CERT-IS and NCIP in the event of a cyber incident in the finance sector requires involvement of the CBI, and if serious, the MoF (and the Financial Stability Council).

34. ECOI/CERT-IS are actively involved with other government agencies when appropriate, for example when the log4j[7] vulnerability was discovered in December 2021, ECOI/CERT-IS and the Department of Civil Protection and Emergency Management, run by NCIP, jointly decided to raise the civil defence risk level. SURF also met to discuss measures that those members of the forum (including the three systemically important commercial banks) had taken to address the vulnerability.

35. Part of SURF's a mandate is to coordinate actions at times of operational disruptions that affect the financial system's safety and efficiency. A working group within the forum, led by RB, is currently drafting a common coordination plan for times of disruptions, including those stemming from cyber-attacks. As part of this initiative, it is envisaged that RB will act as a common incident response center for institutions operating within the financial sector.

36. The FSA has in the past held coordination exercises with all major institutions and service providers as a part of the major upgrades to Icelandic financial market infrastructures. These exercises were operational in nature and did not specifically address cyber-attacks.

[7] Log4j is an open-source logging library commonly used by apps and services across the internet worldwide. If the vulnerability was left unfixed, attackers can break into systems, steal passwords and logins, extract data, and infect networks with malicious software.

37. The supervisory divisions of the CBI (ex FSA) have a contingency plan in place. This, the Financial Service Response Plan, is currently being reviewed to reflect the merger between the FSA and the Central Bank on 1 January 2020.

Review

38. There is some confusion about who would lead the financial sector's response to a major cyber or operational incident. The common coordination plan for times of disruption currently being developed by the working group within SURF should to some extent provide clarifications about this position, once formally issued by the CBI, and presented to MoF. An early draft of the coordination plan shows that the CBI, the largest banks, and a savings bank are included, but government agencies are not. In the event of a major incident, it is highly likely that the MoF and MoHESI will need to be involved to coordinate a response and associated communications. In due course, contingency plans should be developed for different scenarios which would then be exercised.

39. Financial institutions involved in the CERT-IS led cyber security scenario exercise found it to be very valuable and there is an appetite for more. Procedural difficulties were encountered and there were lessons learned which can improve future exercises. Nevertheless, all participants expressed an appetite for more such exercises.

40. The supervisory contingency plan has not been updated since the merger of the FSA and CBI three years ago. An out of date contingency plan may prove ineffective in a crisis.

Recommendations

41. MoF and CBI should expedite the development and dissemination of an overarching strategy and contingency plan for the financial sector especially in the event of a major incident. This should build on the common contingency plan already being developed by the working group within SURF. As part of this work, the supervisory contingency plan should be updated.

42. The authorities should arrange further cyber security scenario exercises to strengthen cooperation and coordination, expanding the range of financial institutions and government agencies involved.

SUPERVISORY ARRANGEMENTS AND PRACTICES

A. Legal and Regulatory Framework

Current Arrangements

43. In common with many jurisdictions, provisions of laws and government orders relating to cyber and operational resilience for the financial sector are numerous and widespread.

Most of the regulations derive from EU legislation, which Iceland, as a member of the European Economic Area is required to replicate in local legislation. Such regulations cover the governance of operational and ICT risk management; operational risk (outsourcing; incident reporting; business continuity management), information systems and security. Of particular relevance are the guidelines on ICT and outsourcing to cloud service providers published by the European Supervisory Authorities (ESAs) and Annex F to the CPMI/IOSCO Principles for Financial Market Infrastructures Core Principles.[8] In March 2019 the FSA issued Guidelines No. 1/2019 on risks due to Information Systems Operated by Supervised Entities which they apply to all supervised entities. They include provisions on management and responsibility, contingency requirements and business continuity plans, outsourcing, security – including cyber security – internal monitoring and incident notifications.[9] The guidelines are derived from the transposed EU regulations. In themselves they are non-enforceable, but any supervisory sanctions would be derived from the underlying legislation.

Review

44. It is encouraging that many of the regulations governing ICT systems were summarised in the guidelines issued by the FSA, but these cover legislation extant in early 2019. Since that date, new regulations have been issued, most significantly the revised Payment Service Directive (PSD2)[10] and the Digital Operational Resilience Act (DORA). In addition, there has been significant regulatory interest in operational resilience. The current guidelines contain many of the principles set out in the Basel Principles for Operational Resilience[11].

Recommendation

45. To remain useful and relevant, the supervisory guidelines on ICT systems should be subject to regular review and updating, in particular in respect of PSD2, the Digital Operational Resilience Act and the Basel Principles for Operational Resilience.

B. Roles and Responsibilities

Current Arrangements

46. The Central bank is the only authority supervising cyber and operational risks in the financial sector. Four departments within the Central Bank focus on the supervision of regulated entities: The Banking Department focuses on supervision of institutions that fall under EBA regulatory framework; The Pension and Insurance Department focuses on supervision of institutions that fall under EIOPA (and pension funds that are not under any ESA framework); and the Markets Department focuses on supervision of institutions that fall under ESMA and also supervision of

[8] Principles for financial market infrastructures (bis.org)

[9] https://en.fme.is/media/leidbeinandi_tilmaeli/Guidelines-1-2019.pdf

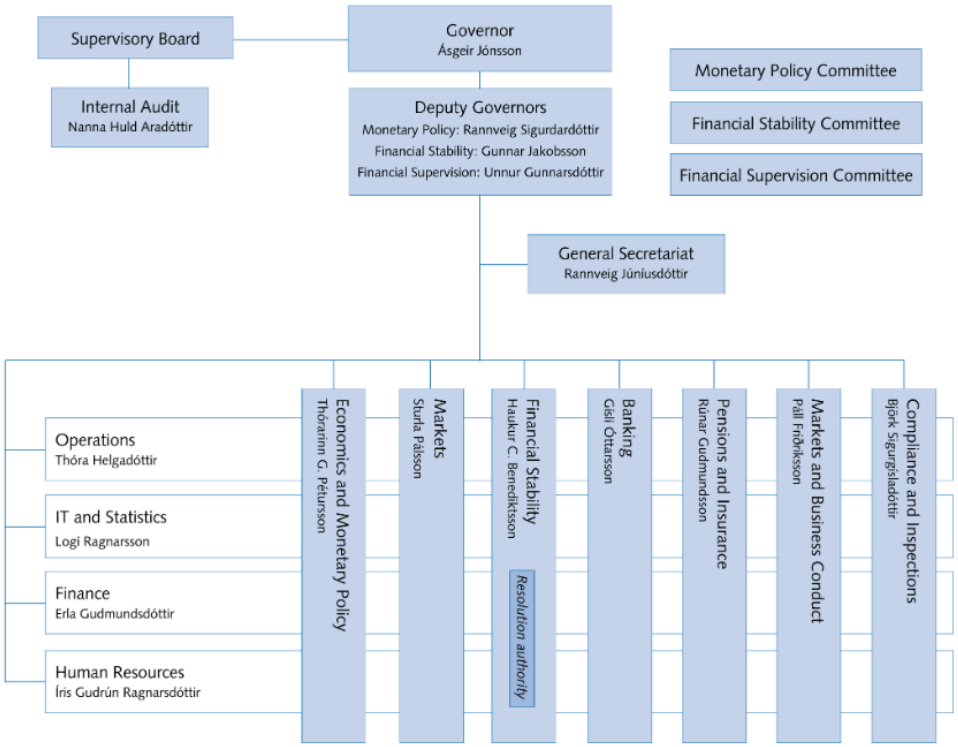
[10] Currently under review, following consultation in 2022.

[11] Principles for operational resilience (bis.org)

consumer issues. There is a separate unit in the Central Bank's Financial Stability Department, the Financial Market Infrastructure Oversight Unit (the "Oversight Unit") which is responsible for monitoring the operational security of the central bank's RTGS infrastructure, including its cyber security.[12] (See Figure 3: Organization Chart of the Central Bank.)

47. Operational and cyber risk expertise in CBI is limited, with very few experienced staff. As noted above, the Icelandic financial system is large, concentrated and interconnected. There are 10 banks, three of which are substantial in Icelandic terms (systemically important), and a large Insurance and Pension Fund sector. Two FTEs in the Bank division and one FTE within Pension and Insurance focus on operational risk. One of these experts focuses on cyber risk. One FTE within the Financial Market Infrastructure focuses on cyber risk within the CBI's core payment system (MBK and RB). The two experts in Banking also provide support to the experts in the other two areas.

Figure 3. Iceland: Organization Chart of the Central Bank of Iceland



Source: CBI

[12] For further information please see: https://www.cb.is/financial-stability/oversight-of-financial-market-infrastructures/.

Review

48. CBI's operational risk experts are experienced and well regarded by financial institutions, but more resources are needed to provide adequate coverage of this increasingly important area. This dependency on very few staff exposes the CBI to the risk of key individuals moving on. With more staff in this area CBI could introduce on-site examinations (see Supervision Approach and Practices below), probe deeper into and provide greater challenge to the self-assessments undertaken by firms and take a more judgement-based approach to the qualitative nature of operational risk and associated controls.

49. The supervisor 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 used this power in the context of cyber risk. 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.

Recommendation

50. CBI should gradually increase the resources for specialist supervision of operational, ICT and cyber risk at regulated firms and to consider using its power to appoint external auditors to augment its limited internal resources for cyber risk reviews.

C. Supervision Approach and Practices

Current Arrangements (Banking, Insurance and Pensions)

51. Cybersecurity is assessed as part of the Supervisory Review and Evaluation Process (SREP), which is undertaken annually for the large banks. During the SREP process the supervisors, supported by the specialists, will consider:

- Incidents reported in the previous year and how they have been handled;
- The results of any vulnerability scans and penetration tests (the three large banks are expected to undertake annual red team exercises);
- Scenarios applied for the SREP stress testing (encouraging banks to explore possible future operational and cyber risk events);
- The outcome of business continuity plan exercises, where cyber aspects are more frequently covered; and
- Code reviews for new applications and internet banking products.

Only systemic institutions are required to do yearly independent penetration testing. It is recommended to other institutions to do this on a risk-based approach. The CBI has decided to

implement the TIBER-EU penetration testing program and has notified the ECB accordingly. The CBI has begun to implement Iceland's version of the framework, which is called TIBER-IS.

No on-site cyber security examinations have been performed at banks. Insurance supervision has recently completed a third on-site inspection on the subject of operational risk with an ICT focus, and a fourth is expected to be performed early in 2023.

52. CBI published its Supervision Focus for 2022-2024, which covered cyber security for the first time: "*It will be ensured that the cyber defenses of important regulated entities are regularly tested with vulnerability scans and cyber-attack drills based on global recognized methodology*". Supervisory work supporting this tends to be in the form of circulars and letters sent to the supervised entities institutions, asking for information, for example, about recovery plan testing. For example, questions were asked about the location of remote data back-up sites in response to the start of the Russia/ Ukraine conflict.

53. Supervised entities are also expected to deliver a regular independent review report setting out an assessment of their ICT and security risk management yearly or every three years based on size. Those institutions that fall under the EBA Guidelines on ICT and security risk management report based on the requirements in those guidelines. Other institutions report based on guidelines from CBI (Guidelines n. 1/2019 on the security of information systems[13]). If deficiencies are revealed in the reports, they are followed up. Supervisors rely on Internal Audit or other independent functions to provide assurance of compliance with supervisory recommendations; in the case of more serious recommendations, supervisors would review the actions taken to address the recommendations.

54. Supervisors conducted an exercise in 2019 to identify critical operations and critical third-party providers. In connection with the implementation of the NIS Directive into Icelandic law, the supervisors conducted an exercise to (i) define critical operations/services provided by the financial sector; (ii) map financial sector interconnections; and (iii) identify key nodes and dependencies on third parties (where failure would endanger financial stability). Key service providers were identified, both technical and financial service providers. However, this may be out of date due to the accelerating rate of outsourcing in the financial sector.

Current Arrangements (Payment System Operators)

55. A three lines of defense model was introduced to CBI shortly after the merger with the FSA. Internal Audit is the third line, the Chief Risk Officer and his team are second line, and the business units make up the first line. In practice and in the context of the CBI's payment systems, the Head of Operations for the Interbank system in the Markets Division and his team constitute the first line.

[13] Guidelines-1-2019.pdf (fme.is)

56. The CBI owns the interbank system (MBK) and as such considers it is required to comply with PFMI Core Principles. RB, as the operator of MBK is required to comply with Annex F to the PFMI Core Principles Self-assessments led by the Head of Operations for the Interbank system in the Markets Division for CBI and by RB in respect of Annex F are expected to commence this year. Once finalized, CBIs Oversight Unit will review the assessment and propose appropriate remediation and improvement as necessary.

57. CBI has entered into an agreement on the cooperation framework for the supervision and oversight of Nasdaq CSD SE. As a branch operation in Iceland, supervision and oversight, including of cyber security, are undertaken by the Latvian supervisors and the CBI Oversight Unit is kept informed.

58. New applicants to be part of the payment system must demonstrate that they have sound systems in place to monitor risks in connection with participation in the system, including cyber security and other operational risks. The Head of Operations for the Interbank system in the Markets Division will carry out this assessment.

Review

59. The supervision process is highly dependent on self-assessments by the regulated entities themselves and independent reviews carried out by third parties. The financial institutions consulted during the mission commented that weaknesses identified in self-assessments and independent reviews were followed up by supervisors but there appeared to be little or no challenge from the supervisors on other assertions set out in the reports. The lack of on-site visits and/or robust challenge to the assertions made in reports on the subject of cyber risk increases the risk that cyber security weaknesses are missed by the supervisor. The introduction of TIBER-style penetration testing by CBI is to be welcomed.

60. Due to recent changes in outsourcing arrangements, particularly the use of cloud technology, the list of critical operations and critical service providers held by supervisors is incomplete. Supervisors have conducted exercises to identify critical operations and critical third-party providers. Without a complete understanding of the use of outsourcing in the financial sector, supervisors may be unaware of the build-up of concentrations and dependencies in the use of key suppliers. This list should be disseminated among supervisors and senior staff to ensure a comprehensive awareness of trends and concentrations. The lists should be subject to regular review and updating. The list should also be reported regularly to the Committee and the Council, which could then consider whether there are such concentrations and dependencies and act accordingly.

Recommendations

61. CBI should commence on-site examination of operational, ICT and cyber risk at regulated firms to obtain fuller picture on cyber preparedness, starting with the systemically important institutions and widening coverage as increased resources for specialist supervision allow.

62. CBI should regularly revise the list of critical operations and critical service providers for internal use and for presentation to the Financial Stability Committee and Financial Stability Council.

D. Incident Reporting

Current Arrangements

63. The Supervisor uses an incident reporting framework based on EBA's PSD2 incident reporting guidelines. Cyber security incidents are included within the general category of security incidents in PSD2. The reporting thresholds set by the EBA have been adjusted to take account of the relatively small size of the Icelandic financial institutions. Expert judgement is used to determine whether an incident needs a follow up, either because of insufficient response by the affected institutions or if an incident is considered to pose a systemic risk. The three systemically important banks and Stock Exchange also are obliged to report incidents to CERT-IS.

Review

64. No formal summary or trend reports are created summarizing cyber and operational incidents and trends. Incident information is shared informally on regular cross divisional meetings within the banks, but there is a danger that patterns in incidents will be missed.

Recommendation

65. CBI is encouraged to enhance its incident dashboard by summarizing cyber incidents and examining trends.