FI Supervision

Information and Cyber Security work in Banks

No. 9

7 December 2018

7 December 2018
Ref. 18-18413

CONTENTS

FI supervision

Finansinspektionen frequently publishes supervision reports in a numbered series. These supervision reports are part of FI's communication. The reports describe the investigations and other supervision carried out by FI. Through these reports, FI presents its observations and assessments as well as its expectations in various matters. This information can support firms in their operations.

Summary

Several banks are increasing their focus on information and cyber security, but many have not yet fully adapted their work to the changes in the environment introduced by higher level of digitalisation and an increase in cyber threats. FI expects the banks to continue to focus on developing their abilities, and that they will manage and follow up the risks associated with information and cyber security.

Financial stability, both nationally and globally, is dependent on reliable financial infrastructure and banks that support and provide critical functions in the financial sector. Today, the operations of financial institutions are entirely based on IT systems. Over the years, many IT systems have become more complex and interconnected, both internally and externally, in part through integration with other financial actors but also through outsourcing of operations to third-party suppliers.

This change is ongoing at the same time as the number of groups with resources and ability to carry out advanced IT attacks is increasing, both in Sweden and internationally. It is in this context of constantly changing conditions, the banks need to manage information and cyber risks.

It is clear, from FIs supervision activities, that the banks have focus on information and cyber risks. FI has also noted a number of areas where the banks can improve, summarised in the following general recommendations to the management of the banks:

- Ensure that the information security management system – organisation, security enhancing processes, procedures and controls – that has been adopted, is also implemented in the daily operation and throughout all business units of the bank.
- Establish an ability to analyse and assess current cyber threat, and which actors that are behind these threats, enabling to adapt the risk management continuously. Improved and expanded collaboration and information sharing between the banks, and between banks and other stakeholders, will strengthen this ability.
- Prioritise training of staff to raise the level of awareness regarding information and cyber security.

In this report FI describes conclusions from the supervision activities that have been carried out the past few years and FIs view of how this connects to the ongoing changes in the financial market. The banks' work with information and cyber security will continue to be a prioritised area within FI's supervision. FI will follow up on the deficiencies observed and continue to conduct supervisory inspections in this area.

Background to the supervision of information and cyber security

In this report, FI presents the conclusions drawn from the supervision of information and cyber security carried out related to banks in 2017 and 2018, and how this relates to the ongoing changes within the financial market.

KEY TERMS IN THE SUPERVISION REPORT

Terms such as cyber security, cyber threat and cyber risks are being used to an increasing extent. In this report, concepts are based on the Financial Stability Board (FSB) Cyber Lexicon, the final version of which was published in November 2018[1].

This defines cyber security as the preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. A cyber incident is a cyber event that jeopardises the cyber security of an information system or the information the system processes, stores or transmits. A cyber risk is the combination of the probability of cyber incidents occurring and their impact. Finally, a cyber threat is defined as a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.

In this report, FI uses the term “information security” as it is defined in Finansinspektionen’s Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems. Which is: protection of the confidentiality, integrity and availability of information.

Information security management system is another key term in this report and the purpose is to establish, introduce, operate, monitor, review, maintain and develop the information security of the bank. The requirements of the information security management system are described in more detail in Chapter 2 of Finansinspektionen’s Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems.

GLOBAL CHANGE

The risk of cyber-attacks – where external or internal actors attack the banks and their customers online in order to sabotage financial services, steal, manipulate or spread sensitive information – has increased. Several actors have extensive resources and are capable of carrying out advanced cyber-attacks in Sweden and international. A number of serious attacks have taken place globally in recent years, and this has continued in 2018.

A major attack on IT systems in the Swedish banking sector may result in an extensive impact on private and corporate customers. For example, information about customers and their engagement with banks may be deleted or distorted. Important services may also be

1 FSB Cyber Lexicon, see http://www.fsb.org/2018/11/cyber-lexicon/

unavailable to customers and the market. Such a scenario may seriously harm confidence in the financial system and, in the worst-case scenario, cause problems that threaten the financial stability.

In addition to this, there is a transformation within the sector in which innovation and development are challenging the traditional banks' existing services. The banks are focussing on developing their own innovative services and digital channels, at the same time as they are undertaking an extensive development programme in order to adapt to existing and new regulations. All this lead to an increased level of complexity in an already complex IT environment, where new solutions are introduced at the same time as obsolete technology need to be replaced.

Overall, FI concludes that the cyber threats, in combination with the fact that the banks are working under a high pressure of change, increases the risk of IT disruptions in business critical systems.

RULES AND STANDARDS IN INFORMATION AND CYBER SECURITY

The requirements for information and cyber security on banks are based on the rules concerning risk management described in Chapter 6, Section 2 of the Banking and Financing Business Act (2004:297).

In addition, there are regulations and general guidelines issued by FI:

- Regulations and General Guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions
- Regulations and General Guidelines (FFFS 2014:4) regarding the management of operational risks
- Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems

The standard "Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2006, IDT)" was considered when FI formulated the requirements for information security in these regulations.

FI welcomes the fact that the banks largely also base their information and cyber security work on standards such as those included in the ISO 27000 series, the ISF Standard of Good Practice for Information Security and the NIST Cyber security Framework.

An increasingly intensive work is ongoing among international industry organisations and supervisory authorities within the financial sector on information and cyber related risks. Inventories of existing regulations and summaries of guidelines and principles are conducted by several organisations[2] and working groups related to IT and cyber risks. The idea is to, in the long-term, reach a more harmonised

2 E.g. the Committee on Payments and Market Infrastructures, the International Organisation of Securities Commissions (CPMI-IOSCO), the Financial Stability Board (FSB), the Group of 7 (G7), the International Monetary Fund (IMF), the Organisation for Economic Co-operation and Development (OECD) , the World Bank, the European Systemic Cyber Group (ESRB-ESCG), the European Bank Authority (EBA), the Basel Committee on Banking Supervision (BCBS)

regulation and supervisory practice in an increasingly interconnected financial market.

Supervision observations

A number of important areas are described in this chapter, along with the existing expectations on information and cyber security and the observations from FI's supervision. The description of the expectations on the banks, in terms of processes and controls, is based on FI's regulations and international standards[3]. However, the description is only a selection and does not provide a complete view of all the requirements. The banks also need to consider the size, nature, scope and complexity of their operations as part of their efforts to ensure that information and cyber security is sufficiently implemented.

GOVERNANCE, RISK MANAGEMENT AND CONTROL

The objective of governance of information and cyber security is to ensure that information and cyber security risks are analysed and managed within the bank's business and risk management processes, to achieve the business targets within the framework of the bank's risk appetite.

Information security management system

Working with information security in a methodical and structured way requires an evident and clearly defined structure of responsibility and ownership. The person who is responsible for leading and coordinating work with information security needs to have sufficient resources and authority, and clearly allocated responsibilities. The person should also have an adequate seniority at a sufficiently high level in the organisation that provides authorisation to take action and make necessary decisions in an efficient manner.

FI stipulates that the banks shall carry out this work using an information security management system. The information security management system shall guarantee documented goals and direction for information security, procedures for how the bank identifies and manages its information and cyber security risks and how work with information security will be followed up, reviewed and improved. As a part of this, it is important that information and security enhancement plans are approved and committed to, in terms of delivery times and that they describe the security enhancement activities to be performed.

Organisation and division of responsibilities

It is important within the field of information and cyber security for roles and responsibilities to be clear and for the organisation to have the necessary authority, expertise, knowledge and staff required for risk management. In this respect, FI deems it important that the banks' board of directors and the managing director are involved in and

3 E.g. Finansinspektionen's Regulations and General Guidelines regarding governance, risk management and control at credit institutions (FFFS 2014:1), regarding the management of operational risks (FFFS 2014:4) and regarding information security, IT operations and deposit systems (FFFS 2014:5), as well as the NIST Cybersecurity Framework and the ISO 27000 series.

contribute to creating and maintaining a high level of awareness of these issues.

FI has a positive view of the fact that several banks have established a centrally located group of information security specialists that has operational responsibility for threat analyses and the management of security incidents. Since these individuals often handle very sensitive information, an extended security check should be carried out when they are being recruited. Furthermore, it is important that both the information security specialists and all other members of staff have access to regular and relevant training within this field and that activities are carried out in order to raise awareness of these issues.

Risk analysis
Another important factor in governance of information and cyber security is risk analysis. Information and cyber risks shall be analysed once a year and in any changes that can affect the information security. The analysis should include people, processes and technology.

One explicit example where risks related to information and cyber security should always be considered is related to outsourcing agreements when operations are subcontracted to a service provider, as well as in the continual risk management of existing outsourcing agreements. The same applies to related areas such as continuity management and the approval process[4].

Control functions
Information and cyber security risks should be managed as an integrated part of the banks' risk management framework. This means that the banks' risk control and regulatory compliance functions shall have sufficient resources and relevant expertise and also work in an active and independent manner in order to monitor and control the management of information and cyber security risks in the banks' business units. The risk control function should, in consultation with the business units, establish appropriate performance metrics and thresholds for the bank's information and cyber security risks, and also ensure that these risks are included in the bank's risk appetite.

The bank's internal audit function also has an important role to play. It shall conduct independent audits, and should assess and report to the board of directors and the managing director, on how the information security management system is designed and complied to.

Experiences from supervision of governance, risk management and control of the information security management system
FI's conclusion from supervision is that the banks need to make further improvements to their governance, control and organisation. This involves increasing the understanding of the information and cyber area among the board of directors and senior managements of the banks as well as devote more time for them to discuss and make informed decisions concerning the bank's information security management system.

4 The requirements for continuity management and the approval process are described in more detail in FI's Regulations and General Guidelines (FFFS 2014:4) regarding the management of operational risks.

In addition there is an expectation on the risk control function to adopt a clearer role in the reporting of material deficiencies and risks, as well as deviations from thresholds for information and cyber risks. This provides the conditions for the senior management and the board of directors to better understand the scope of these risks. In turn, this is dependent on the risk control function having resources with relevant IT and information security expertise.

Several types of attacks make use of the human factor (phishing[5], vishing[6], social engineering[7]), this also affects banks and their customers. By strengthening the structure of, and follow up on, staff training programs, an increased awareness of information and cyber security could be reached, as well as a clarification of the responsibility that each employee has in the protection of the bank's information and services.

Cyber-attacks causing service disruptions and incidents of the criticality that have gained media attention, have been possible to trace to deficiencies in internal control. Deviations from internal policies, established processes and procedures, as well as known deficiencies that have not been managed lead to vulnerabilities that have been exploited by threat actors. More active governance, control and follow-up activities, would probably have prevented many incidents.

FI's supervision has also found that there is a lack of sufficient staff with information and cyber security expertise in risk control and compliance functions. In addition, the internal audit function generally conducts too few audits of how work with information and cyber security risks is managed by the risk control and compliance functions.

SITUATIONAL AWARENESS AND CYBER THREATS

Banks should maintain a current group wide knowledge base of its users, devices, applications and their relationships. This is required, for among other reasons, to identify the most critical assets that require additional protection, e.g. those that store, transfer or process sensitive customer or business information, but also other assets that may be a potential target for cyber-attacks.

Furthermore, banks should have real-time monitoring and analysis on security events to identify potential cyber-attacks. This may also create better conditions for sharing operational information within the financial service industry; through participation in industry programs, (e.g. industry funded CERTs). FI recommends that banks both participate in collaboration with regard to operational information sharing concerning cyber threats and vulnerabilities and subscribes to industry research on cyber security.

5 Phishing, password fishing, is a form of social manipulation and an illegal method for defrauding holders of bank accounts and other electronic resources of their credit card number, password or other sensitive information online.

6 Vishing, social manipulation with the same purpose as phishing described above, via telephone.

7 Within information security, social engineering is methods used to manipulate people to carry out actions or reveal confidential information.

In supervision, FI has noted that the banks often have a fragmented knowledge base of users, devices, applications and their relationships. However, several banks have ongoing projects that aim to gather the information into an IT system intended for this purpose.

SECURE SYSTEM DEVELOPMENT AND CONTINUOUS SECURITY PATCHING

In order to ensure that the bank is protected against known software security flaws, the bank should follow an established process to obtain, test and deploy security patches and updates in a timely manner based on criticality. Successful deployment of security patches shall be confirmed and any update failures be resolved. Automatic security patches can facilitate to ensure updates in a timely manner. Banks should also considers and mitigate cyber risks arising from use of any unsupported software.

Processes for secure system design, coding and testing standards that incorporate appropriate information- and cyber security controls shall be used when developing software. The purpose of this is to verify information- and cyber security within the framework of the bank's system development process, including agile system development methods.

As part of its supervision, FI has observed that several banks are involved in ongoing projects to update their processes for managing security patches, often in order to increase automation. In the shift between traditional system development methods and agile methods, different approaches to software security verification have been observed. Several banks are currently working to improve their processes for secure systems development.

IDENTITY AND ACCESS MANAGEMENT

The ultimate aim of identity and access management is to enable for the right individuals to access the right resources at the right times for the right reasons.

Clear ownership of identity and access management processes should be assigned. The process owner should be given the mandate and conditions needed to set requirements on, secure implementation of, and control compliance to, the identity and access management processes.

It is important to define structured processes and controls that manage devices and users access permissions through their lifecycle, create, allocate, change and withdrawal, incorporating the principle of least privilege and segregation of duties.

It is also important to regularly follow up and check that existing access permissions are restricted to needs based on work duties allocated and to rectify any identified discrepancies.

It is especially important to tightly control and manage the use of high privileges within the area of identity and access management. High privileges refer in this context to users with full, or close to full authority for critical IT systems or infrastructure components. This means that they can, for example, alter or remove information IT production systems.

When designing processes and controls to manage the use of high privileges, banks need to consider:

- How access permissions can be restricted to the principle of least privilege
- Whether strong authentication[8] should be introduced
- How segregation of duties, e.g. separation of toxic combinations of authorisations should be controlled
- How monitoring and review of the usage of authorisations should be conducted in order to ensure traceability

Many of the incidents and cyber-attacks that have gained global attention over the last few years have occurred due to deficiencies in identity and access management. Attack actors have gained access to high privileged accounts, not protected by strong authentication, and used these accounts in attacks.

One observation FI made in supervision is that the identity and access management is a challenge, primarily for large banks that have an extensive number of systems, complex system integrations and a high number of users moving between organisational units. It is also a challenge to map and get the complete picture of all high privileges that need to be managed.

In addition FI has learned from the supervision that the implementation of the structured processes and controls that have been decided is challenging. Implementation projects are often delayed. Implementation should thus be given a clear mandate, the required resources and full support from senior management.

FI's requirements related to identity and access management are described in Chapter 2, Section 8 of Finansinspektionen's Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems.

SECURITY MEASURES IN IT SYSTEMS AND NETWORKS

Protection of information and data

A huge amount of information is managed in bank operations, e.g. personal and customer specific information, information and data related to transactions and internal business conditions. To protect the information from unauthorised access or theft, a number of measures need to be considered. These measures include monitoring outgoing traffic to prevent data leaving the bank network unauthorised and encrypting data that is transported in the network and stored on servers, computers and various mobile devices.

There shall also be procedures to secure that backups of information are conducted, maintained and tested periodically. Furthermore should procedures for decommissioning of obsolete information storage devices in a sufficient secure manner, be in place.

8 Strong authentication, often multi-factor authentication (MFA) is a method of access control in which users are only granted access after having successfully presented more than one separate piece of evidence to a authentication mechanism – usually within at least two of the following three categories: knowledge (something they know), possession (something they have), and inherence (something they are).

Network segmentation
In order to protect information and IT systems in the internal network – including any wireless networks – from unauthorised access, it is important to design the network based on the requirements on information security. One way to do this is to segment the group network into multiple, separate trust zones. A segmented network zone architecture limits the risk of unauthorised access and enables isolation or shutdown of compromised network segments, thus limiting the consequences of a cyber-attack.

The conclusion from FI supervision is that the banks are working actively on network segmentation, but need to fully implement these measures.

Standard security configuration and management
The hardware and software assets (including operating systems and database platforms) are often delivered in standard configuration, and need to be configured according to the consistent security standard approved by the bank. Consequently, it is important to establish a security standard in line with the banks strategy and the business operation requirements that, e.g. regulates which services and network ports are to be available, how authentication shall be designed etc.

It is important to continuously update such standard configurations as new threats and vulnerabilities are identified. Procedures should be introduced that ensure that all relevant IT systems and network components have the approved standard configuration installed.

Protecting networks from external threats
There is an increasing risk of direct intrusion into the banks' IT systems and infrastructure where the goal is to cause operational disruption, destroy information or prepare for fraud. Denial of service attacks against the banks' internet channels also occur. It is important to provide the internal network with sufficient protection from external threats. Typical security measures include firewalls, intrusion detection systems (IDS), intrusion prevention system (IPS) and protection against malware and harmful code (antivirus).

Also within this area the banks are working actively and need to fully implement these measures.

INCIDENT MANAGEMENT

FI's Regulations and General Guidelines (FFFS 2014:4) regarding the management of operational risks states that banks shall have internal rules to manage incidents arising in its operations. This requirement also applies to information and cyber security related incidents. In order to rapidly respond and manage information and cyber security incidents, it is important that roles and responsibilities for the operational management of security incidents are determined in advance.

Principles for managing and making decisions on measures should be in place, as should internal and external communication plans. Before formal closure of a security incident, it is important to ensure that IT systems and data are fully restored. The investigation of the incident

should involve an analysis of its root cause. Activities to manage the root cause to prevent repeated incidents should be performed. The sequence of events during the incident should be documented.

TESTS

FI's Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems states that banks shall classify its information so that it is ascribed the right level of protection. This classification shall be based on the requirements imposed on the information's confidentiality, integrity and availability in its operations. The internal rules should set out the requirements for regular controls of the firm's IT systems in relation to the established level of protection for the information.

There are a number of approaches to conducting these regular controls, for example:

- Regular automatic vulnerability hardware and software scans and testing for client, server, and network infrastructure to identify security control gaps
- Regular penetration testing of the network boundary (e.g. open network entry and exit points) to identify security control gaps, also performed related to changes implemented in the internet channels, e.g. its online banking platform
- Advanced penetration tests using cyber threat intelligence and cyber threat modelling to design the test where the staff conducting the tests are independent of the function being tested

Banks should adopt a risk based approach when deciding the scope and frequency of the tests. In this context, consideration should be given to the fact that advanced penetration tests of specific threats are a significant and resource intensive way to test the level of protection. This type of test is best suited for banks that have a high level of maturity related to information and cyber security. Banks with critical internet channels should prioritise regular penetration tests of these and regular automatic vulnerability hardware and software scans for known vulnerabilities.

Conclusions

Finansinspektionen concludes that the banks are making substantial efforts and investments in the field of information and cyber security. At the same time, several banks have not yet fully adapted their work with information security to adapt to the changed conditions that mean higher level of digitalisation and an increase in cyber threats.

IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Based on the information from supervision, it is FI's assessment that the banks have generally made substantial progress in the development of their information security management systems. However, the commitment of the banks' senior management needs to increase when it comes to controlling and, when necessary, take appropriate action in related to the implementation of the information security management system into all areas of the bank.

In this work, there is an expectation from FI on the risk control and compliance functions, to take on a clearer role in monitoring and controlling the implementation of the management system in the bank's operations. This will probably result in a need for more staff with IT and information security expertise in these functions, in several banks. The internal audit function can make a contribution by conducting audits of how the bank's information and cyber security work is managed by these functions.

CONTINOUS RISK ASSESSMENT

FI notes that there are challenges in reaching all the way through carrying out continuous risk analyses and assessments of current cyber threats that cover all identified processes of material significance of the banks. This is despite the fact that most banks have established both generic, and information security specific, risk identification processes.

FI would like to draw the attention to the importance of having processes in place that secure that cyber risks are continuously assessed and managed for all processes of material significance of the banks.

INCREASED DETERMINATION

Cyber-attacks causing service disruptions and incidents and that have gained media attention, have been possible to trace to deficiencies in internal control. The human factor is also involved here. Supervision experience indicate that the effects of this type of disruption can be reduced by ensuring that the processes and procedures the banks have developed are fully implemented.

Increased determination and more active governance, control and follow up to ensure that all areas of the bank are adhering to the established processes can probably prevent many incidents and – when incidents do still occur – minimise the consequences and reduce the lead times for resumption of normal operations.

In this context, identity and access management, and the knowledge base of users, devices, applications and their relationships are crucial. FI has observed that the implementation and management of these important processes are fragmented and differ between the banks' business areas.

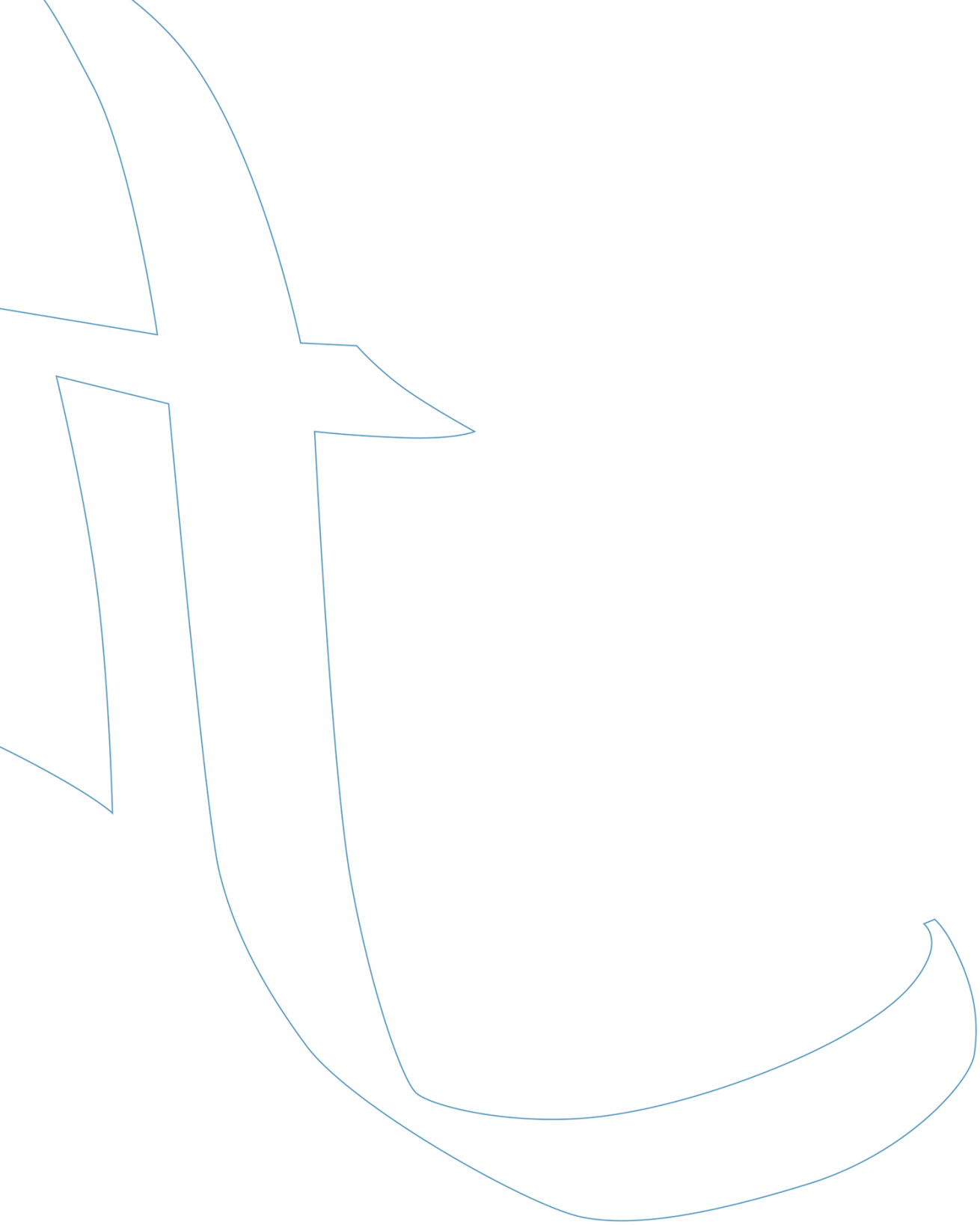
Furthermore, it is FI's assessment that staff training has great potential, and can be used to increase the level of awareness concerning information and cyber security, which can contribute to prevent some cyber-attacks and to reduce their consequences when they do occur.

Another important area is to regularly test the business contingency and security measures and the extent to which the incident management system is adapted to dealing with cyber-attacks.

COLLABORATION WITHIN THE SECTOR NEEDS TO BE REINFORCED

By exchanging information about cyber threats and vulnerabilities within a group, the banks can use their collective knowledge and experience in order to gain a more complete understanding of the threats and attacks that occur. Receiving and using that type of information to constrain or remedy e.g. a cyber-attack, can mitigate or prevent it from spreading to other financial institutions.

Sharing information, in turn, increases the possibilities to identify cyber-attacks specifically targeted at a group of financial institutions, or the financial sector as a whole. Consequently, FI has a positive view on forums for sharing operational information related to incidents, cyber-attacks and cyber threat and improved forms of collaboration between the banks and between banks and other stakeholders of relevance.



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

www.fi.se