M E M O R A N D U M

Date	2021-03-04	FI Ref. 20-3685
Author	Finansinspektionen	

Finansinspektionen
Box 7821
SE-103 97 Stockholm, Sweden
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Cyber threats and financial stability – FI's role and assignments

Contents

Summary
In recent years, a number of legislative proposals and other initiatives have been presented to strengthen the financial sector's resilience to cyber attacks. Finansinspektionen (FI) has therefore produced this memorandum to describe the role that FI plays in promoting a high level of cyber security and the work that it carries out to prevent cyber threats against the Swedish financial sector.

Although digital development has opened up a world of opportunities in recent decades, there are risks associated with this development that have to be managed. These risks have been amplified by a partial deterioration in Sweden's security policy. FI can confirm that cyber threats present a clear risk and it is in the interests of every financial company to be able to manage this risk. We have also identified risks of 'negative externalities'; by this we mean that not every company has the incentive to take fully into account the impact that a cyber attack on them could have on the economy as a whole. FI therefore has the same fundamental reasons to take action in this area as it does for combating the risk of a traditional financial crisis.

The financial sector is highly digitalised, which has made cyber security a major issue for financial companies in recent years. The central role that the financial sector plays in society makes cyber security in the financial sector an important area of concern for the whole of society. The financial companies and markets are closely intertwined, so any problems can quickly spread, making the need for cooperation even greater. Against this background, it is necessary to develop the ways that government authorities work together to combat cyber risks in the financial sector.

Current legislation already provides FI with a range of tools that it can use to manage cyber risks in the companies that it supervises. However, its powers of intervention vary depending on the different sectors of the financial market. In the second half of 2020, new rules were proposed within the EU that will have an impact on the supervision of the cyber risks of financial companies. Sweden's total defence is also being restructured at the moment, which requires authorities, including FI, to take action to increase the country's resilience to cyber risks.

1. What characterises a cyber threat?

Complex and multifaceted

Problems related to cyber and IT risks vary in nature and can be classified in different ways. One way is to break the problem down into two main areas: firstly, purely technical faults and operating problems; secondly, cyber attacks, where disruptions are caused intentionally to gain access to money or information, manipulate data or sabotage the activities of individual companies or the economy as a whole. These two areas can be referred to as 'non-antagonistic' and 'antagonistic' disruptions respectively. For example, antagonistic attacks can be carried out by a state actor to cause harm to another country. Both kinds of disruptions can take many forms and can affect virtually any operations or societal functions.[1]

The general consensus is that the importance of both of these risks has increased and will continue to increase,[2] despite there being growing awareness, a rapid development of risk management, and security technologies and security procedures. The vulnerability caused by unintentional disruptions is rising, mostly as a reaction to the rapidly increasing dependence on IT and digital networks in all areas of society, and this is particularly true of the financial sector. The significance of antagonistic disruptions is also growing, partly for the same reasons. However, antagonistic disruptions are becoming increasingly more important as the attacks are becoming much more sophisticated; the gains or impact from an attack can be significant, while the risks for the perpetrators are normally considered to be minimal.

Finally, it is safe to assume that this kind of risk is, and will increasingly become, a problem not only for individual financial companies, but also for the financial sector as a whole. FI needs to develop a system-wide approach and procedures to supplement the more company-specific supervision that we have been performing to an increasing extent over many years. Financial regulation and supervision can help reduce vulnerability to cyber risks in an important area, but this requires broad cooperation with different actors, in both the private and public sector.

Focus on cyber attacks

There are several similarities in the impact of IT and cyber problems that have been caused unintentionally and intentionally. Every time a data system or network goes down due to error handling or technical problems, it has the same technical impact as if the disruption had been caused by malicious intent. Good operational security is one way of building resilience and robustness to attacks.

---

[1] In 2018 the Financial Stability Board (FSB) produced its Cyber Lexicon, which contains definitions of a range of terms that relate to cyber security in the financial sector.

[2] See, for example, https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/ (read 27 January 2021) or the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final, p.1.

It should be remembered that unintentional, more everyday disruptions can be considered to be more of a problem quantitatively, as they happen everywhere and on a daily basis; while major attacks are still rare.

However, the reason why special focus has to be placed on attacks and why they should be managed separately to some extent is that they add an additional risk dimension to the traditional, operational risks. They also add another level of complexity – analytically, legally, technologically and organisationally. Currently, it is more likely for an incident that has a broader social and systemic impact, for example a disruption to payment systems, to have been caused by a technical incident than by an attack from a foreign power, terrorist group or criminal organisation.

However, an antagonistic attack can be expected to cause greater damage. One important reason for this is that actors perpetrating an attack have a clear ambition to achieve the most serious and extensive damage possible, while actors on the market have strong incentives to do the opposite, i.e. both to reduce the risk of problems and manage them as efficiently as possible if they do occur. An antagonistic attack can also have greater psychological and political consequences, which has more of an impact on trust. Consequently, it is reasonable to focus on the risks associated with intentional disruptions to the digital functions that are critical for the financial sector. It is the antagonistic disruptions, i.e. cyber attacks, that are the focus of this strategy.

There have been a significant number of known cyber attacks against financial companies and markets with varying degrees of severity; and it is highly likely that there have been many unknown attacks as well. None of these incidents, or a combination of them, has threatened the financial system. However, this is no guarantee that it will not happen in the future.[3]

Here are examples of the kinds of incidents and attacks that can occur:

- Attacks to undermine confidence and trust in the financial market by, for example, creating fake news, spreading rumours and disinformation on social media, sending scam emails from banks or authorities, or carrying out attacks on news agencies such as Reuters and Bloomberg and other suppliers of critical data related to financial services.
- Attacks to manipulate, destroy or publish data, for example personal data.
- Attacks on ATMs, national suppliers of identification services (for example BankID) or payment services (for example Swish).
- Attacks on or through the global payment messaging system (SWIFT).

Some incidents and attacks can impact the financial sector, even if they are not targeted directly at it. Examples include:

[3] The European Commission's Cybersecurity Strategy from 2020 states that the financial sector is one of the main sectors affected by cyber attacks (see the Joint Communication to the European Parliament and the Council on the EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, p. 3).

- Attacks on critical technology components (for example operating systems, applications, and communication protocols for the internet and storage services) that are used by most financial institutions and their service providers.
- Attacks on third-party service providers that deliver critical financial services, for example cloud services, to several systemically important actors on the financial market, which cause these services to be unavailable over a long period of time. They can also take the form of buy-outs and take-overs of important third-party service providers.
- Attacks that disable other critical national infrastructure, such as energy and telecommunications, that cause financial services to be unavailable over a long period of time.

How do cyber risks differ from other stability risks?
The risks to the financial sector are multi-faceted and difficult to monitor, assess, and manage using traditional tools. For example, a cyber incident could suddenly occur without any prior warning and affect most of the financial sector at the same time. If this happened, it would be difficult or impossible to apply traditional tools in time and limit the spread, which is normally possible in the kinds of financial crises we have experienced so far. In addition, there are only disadvantages associated with cyber attacks and non-antagonistic operational risks, which is not the case with traditional financial risks such as credit risks and market risks.

Another aspect is that there are many gaps in our knowledge, particularly about the interaction between different companies and different parts of the financial system when a disruption happens. Furthermore, access to relevant data is limited, as is the possibility to compare relevant data. The reasons for this include, inter alia, the fact that, unlike the situation for traditional financial risks, there are no theoretical frameworks that have been developed, no clear and established definitions, and no extensive historical data to use. As mentioned earlier, experience is also missing as there have not been any major system-critical disruptions yet. As a result, there are, inter alia, limited opportunities to perform a statistically-based analysis, which would normally play a central role in financial risk assessments.

However, the risk profile does contain several special characteristics. These include, for example, in no particular order:

- Disruptions can occur, spread and interact even without human intervention and are not hindered by geographical and institutional borders.
- It is often difficult to specify when, where, how and why a disruption has occurred and how it has spread.

- It is difficult to identify and assess the impact and costs, particularly for more indirect and long-term effects. This also makes it more difficult to price the risks.[4]
- The impact of many smaller disruptions or attacks, which might not have drastic consequences for each of the individual actors, could cause significant damage, when combined, to the trust in, and functionality of, the market as a whole.
- There are also counterproductive incentives; companies are often unwilling to share information about the problems they have experienced because of competition concerns.

Financial markets and companies are closely interconnected financially, for example, through transaction processing, mutual loans, and dependence on the same markets and infrastructures.[5] Added to this is the fact that individual actors do not have an adequate overview of, or sufficient incentives to prepare for, the risks that occur through the interaction between different sections and actors in the system. This means that the problems of one actor could easily become everyone's problems. Cyber threats amplify these interconnectedness risks in a variety of ways. The most important factor is probably the dependency of financial services as a whole on technological systems that are globally linked with a high level of complexity and low transparency, and with large sections exposed to the internet. Technological solutions, software, etc. are also mostly shared.

Technology therefore makes a system that was already strongly interconnected even more interconnected, while there remains insufficient incentives to carry out risk management at a systemic level. It is also becoming increasingly clear that financial companies are exposed to risks that are primarily linked to critical subcontractors, but also customers, the social infrastructure and their own employees. This means that risks in crucial areas are beyond the individual company's control.[6] In other words, the interconnectedness dimension, particularly when combined with the risk of intentional attacks, is a basic systemic vulnerability for cyber risks. These cyber risks can also coincide with, be amplified by and interact with other more traditional kinds of risks and vulnerabilities.

---

[4] The International Monetary Fund (IMF) produced a study that stated that 90% of the costs are indirect, but did not define them in more detail or explain the way that they had been calculated.

[5] Interconnectedness in itself creates externalities. Weak risk management in one company also has a negative impact on other companies. Conversely, good risk management generates positive externalities that benefit other companies. These companies could be said to be getting a free ride from the risk management of other companies and in the worse-case scenario this could give them less incentive to do something themselves.

[6] Oliver Wyman, Combatting the Cyber Threat in Sweden – An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector, pp. 4–5.

2. Cyber risks, financial stability and FI's role

FI has been working increasingly with cyber risks over a long period of time as part of its ongoing supervision of financial companies. Cyber risks are also discussed regularly by the Financial Stability Board, where we work with other authorities that have been tasked with maintaining stability.[7] However, as these kinds of risks are attracting more attention due to their growing importance for all kinds of financial activities, it is important to reflect on and discuss a strategy for FI's role and assignments in this field.

This current chapter discusses FI's role in managing the cyber risks of financial companies and the link between these risks and financial stability. It also describes the tools that are needed to manage cyber risks in the financial sector, and the extent to which FI and other actors currently use these tools.

Risks at different levels

The financial market and financial companies mostly work and act in the same way as other companies in the commercial sector. However, the financial sector and financial activities have some unique characteristics that can cause various kinds of 'market failures'. These are risks that individual companies do not fully have the incentive or ability to monitor or manage, and that can result in protection levels being too low for the economy.

In a worst-case scenario, this could lead to the breakdown of central functions in the financial system; this is normally referred to as 'systemic risk'. This occurs if and when the operational or financial resilience of the companies or markets is not strong enough to absorb a shock or recover reasonably quickly from it. This allows it to spread to other areas in a more or less uncontrolled way, ultimately affecting production and employment throughout the economy. The risks of severe market failures on the financial market are the main reason why this market is regulated and supervised by a government authority in a way that few other industries, if any, are.

Are cyber risks a systemic risk?

It is clearly in the interests of financial companies to address and manage cyber risks. The next question is therefore whether these risks are the kinds of risks that can threaten the functionality and stability of the system or whether they are 'only' a problem for the individual companies. As mentioned previously, there are factors involved in cyber risks that mean that individual companies either cannot or do not have the incentive to manage them. Although this shows that there are corporate risks, it does not necessarily mean that these risks are so significant that they can be classed as systemic risks and require some form of special regulation. There will never be an unequivocal answer to this question as long as there is no historical evidence of an actual attack that

[7] The Financial Stability Board comprises FI, the Riksbank, the Swedish National Debt Office and the Government Offices of Sweden (Ministry of Finance). Chapter 3 of this report contains more information about this organisation and its work.

has threatened the system. However, as suggested previously, the functionality of the system could be damaged if there are more restrictive disruptions and if there is not enough capacity to manage them. These disruptions could cause major economic costs without this leading to an acute system collapse. Consequently, negative externalities that do not threaten the stability of the system could cause significant economic damage.

Based on the various studies that have been conducted, there is still no consensus as to what kind of links there are to the risks that threaten the financial system, and if these links do exist, whether they are direct or indirect. For example, a study from the Bank of England claims that it is unlikely that individual attacks from private actors could create systemic crises. According to the study, only state actors have the capacity to do this, but their primary concern is not considered to be the disruption of the financial systems.[8] However, others have come to different and more pessimistic conclusions.[9] As to the question about the interests of state actors in attacking the financial sector, there are some analysts who think that the financial sector could be an important target.[10]

It is, of course, debatable as to whether a cyber attack can directly shut down a financial system or whether these kinds of problems could result in and be transformed into, for example, credit or liquidity risks, which would in turn create systemic risk. It could be claimed that this is of secondary importance from a more practical perspective; what is important is if and how this kind of disruption could act as a trigger.

Other aspects that need to be taken into consideration in this context include, for example:

- the kinds of functions and companies that are most sensitive to cyber risks
- the role and significance these functions and companies have from a systemic perspective
- the kind of transmission mechanisms to other companies and sectors.

[8] Bank of England, Could a cyber attack cause systemic impact in the financial sector?, Quarterly Bulletin 2018, Q4.
[9] For example, Finanstilsynet, the Financial Supervisory Authority in Denmark, whose assessment is that the threat from cyber risks is very high (*Strategi for den finansielle saktors cyber- og informationssikkerhed 2019-2021*). Finanstilsynet (2019), only available in Danish. IMF takes the position that "… cyber risk is a significant threat to global financial stability". ("*Cyber Risk, Market Failures and Financial Stability"* IMF 2017).
[10] "The US Intelligence Community estimates that there are now more than thirty countries with "military-grade destructive attack capability".9 Moreover, it concluded that the financial sector would be a prime target in the case that nations openly engage in cyber-warfare. By attacking the financial system, destruction and disruption of vital functions could be achieved, potentially resulting in widespread panic." See Oliver Wyman, Combatting the Cyber Threat in Sweden – An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector, p. 5.

Although there is currently not enough knowledge in this area, the section below describes which subsectors are considered to be more at risk and could be particularly problematic from a systemic perspective.

Participants	Importance to financial stability	Attractiveness for malicious actors	Comments
Nordic banks	High	High	• Banks typically present an attractive entry point for malicious actors • Concentration in small number of players drives high importance to financial stability
Payment providers	High	High	• Due to the direct impact on consumers and the fairly high degree of concentration, an attack on payment providers could cause loss of confidence in the financial system • With cash payments increasingly being phased out in Sweden, an attack on payment providers could have systemic impact due to the lack of substitutability
Market infrastructure providers (exchanges, central counterparties, trade repositories, clearing houses)	High	Medium to High	• The potential impact on financial stability of an attack on market infrastructure providers is vast, as these firms perform critical functions for which there are few or no substitutes • The impact on the majority of end consumers from a short-term disruption (counted in hours rather than days or weeks) may be limited, and these firms may therefore not be as attractive targets as banks or payment providers
3rd party service providers	High	Medium to High	• An attack on shared third party services can have wide-reaching consequences for financial stability by simultaneously impacting several parts of the ecosystem • Certain third-party services (for instance BankID and Swish) are also highly attractive targets as any service interruptions would have immediate impact on a large number of end customers
Insurers	Medium	Medium to High	• As a function of their activities, attacks against insurers present less of an immediate threat to financial stability and and insurers are therefore also less attractive targets • Nevertheless, insurers possess a plethora of information about individuals, SMEs and corporations and with IoT, the types of data collected, the number of attack vectors and the value of a successful attack is expected to increase
Branches to international banks	Medium	Medium	• While branches can be a conduit for an attack to spread across borders, they are in themselves less attractive as potential targets and an attack on them present less of a threat to financial stability

Source: Oliver Wyman, Combatting the Cyber Threat in Sweden – An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector.

The lack of historical experience makes it difficult to determine the extent of the systemic risk potential from cyber attacks. However, even *if* it is less likely for an individual cyber incident to cause the financial system to collapse, it is much more likely for a series or combination of incidents (interconnected or independent of each other) to cause major problems throughout the system or to one of its central functions. In other words, this kind of scenario could gradually erode the functionality of and trust in the system, rather than the system suddenly collapsing in a way that is often associated with financial crises. As mentioned earlier, shocks that do not pose a systemic threat can also have major economic costs. Regulation and supervision definitely have a role to play if the companies themselves do not have the ability or incentive to manage these kinds of problems.

Even a cautious assessment would presumably conclude that there are likely to be elements of systemic risk. However, the probable conclusion is that there are risks of less spectacular negative externalities that could still have a significant impact on the economy. FI therefore has the same fundamental reasons to take action in this area as it does for combating the risk of a traditional financial crisis.

3. Tools

Tools for strengthening financial stability
The role of the state in financial stability is to prevent problems, as far as possible, that could threaten the system and to be prepared to manage a crisis if it does occur. The work of a supervisory authority, like FI, focuses on preventive work – supervisory measures based on financial regulations are rarely the right tools to use to manage acute crises. The purpose of these measures is rather to ensure that unsuitable companies are not allowed to conduct financial business and that the companies that are allowed have adequate resilience to combat the risks involved in their business.

There are many different kinds of tools that the state can use to prevent risks that could threaten the stability of the system, central consumer interests or the general functionality of the financial markets. These tools are normally used to correct, in various ways, the deviations that can occur between what is rational from the perspective of an individual company or industry, and what is rational for the economy, i.e. what economic theory refers to as 'internalising externalities'. One way of correcting these deviations is to influence the companies' incentives to limit and manage risks more effectively, for example through direct financial factors such as taxes and capital requirements, but also through more subtle ways called 'moral suasion'. This can involve fairly explicit threats of regulations or interventions, or by shaping opinion.

One alternative (or supplementary) approach is to use regulation to increase resilience in the companies and in the system by setting requirements for capital, liquidity, diversified lending, etc. A third approach is to use regulation and supervision to set requirements for the financial companies' organisational conditions and transparency that are linked to the way that their risk management (both financial and operational) has been designed and organised. Requirements can also be set on the way companies manage any conflicts of interest and the information they give to the authorities, the public and their customers. Another tool that can be used is to make it easier for companies to work together and exchange information on industry-wide issues; i.e. promoting fairly far-reaching self-regulation that can help achieve society's goals with less state intervention.

Can these tools be used for cyber risks?
Although all of these kinds of tools can, of course, be used to manage cyber risks as well, it is important to question how useful they would be. Some form of assessment has to be performed of the nature and size of the negative externalities that are created by each actor or function, which can then be used to address the issue of incentives. However, it is extremely difficult to assess these externalities quantitatively.

Although 'financial airbags' can definitely help in all kinds of crises, it is not clear, for example, whether a large capital buffer would play a crucial role in a

financial company's ability to survive a cyber attack. Both airbags, in the form of capital adequacy, and financial crisis measures, for example, state guarantees, can serve several functions. The mere fact that these measures exist can act as a signal and inspire confidence[11]. They also provide actual resources that can be used to buy time and ideally bridge temporary problems. It should be possible to impose requirements on financial companies for a certain level of redundancy in the companies' IT systems to enhance their cyber security, maybe as a complement to financial buffers.

In an ideal world, regulation and supervision of internal governance, controls and behaviours require the supervisory authority to have a good overview of potential 'attack vectors'; in other words the companies' vulnerabilities to various kinds of attacks and the companies' technical interconnectedness. It is clear that knowledge in this area can and should be improved. However, it is not realistic for FI, or any other authority, to reach and maintain a sufficient level of knowledge for the entire area, particularly as the goalposts are constantly moving. This means that it is essential for companies in the financial sector to have the right capability in place themselves to work systematically on their resilience to cyber threats.

It is most likely that a cyber attack would normally take place within a limited period of time, so there will be a need to share information in real time. The problem is that when a crisis happens, the private actors will probably not have information about how and where a cyber attack started and where it has spread. In a crisis, sharing information and other forms of cooperation might not necessarily be a good enough solution to genuine problems caused by a lack of information. In this respect, it might be worth considering establishing redundancy in strategic parts of the system that could limit any immediate damage and buy time.

All in all, this suggests that new kinds of requirements may need to be imposed on the financial companies. This may, in turn, require a change in the rules and the development of new tools not only for FI, but probably for other authorities as well, so that they can work in a preventive way and manage these kinds of crises effectively. Against this background, it is useful to describe the tools that FI currently has available to manage cyber risks in the Swedish financial sector.

FI's current tools

Crisis management

FI's role is to be an information hub during crisis management. We perform regular market monitoring and oblige companies to report any serious problems immediately to FI, which enable us to gain an understanding of the kind of disruptions involved, how serious they are, and in particular whether

[11] For example the 'recapitalisation scheme' during the crisis in 2008–09. From a purely financial perspective, the scheme was not widely used, but it is quite clear that it helped increase trust and therefore protect stability.

they are problems for specific companies or systemic problems. FI's main role during the crisis management stage is therefore to analyse and forward any relevant information to other actors.

Supervision in accordance with the current sector legislation

Supervision is an essential tool for ensuring a high level of cyber security for companies in the financial sector. Supervision in this context is when an actor (an authority or similar) is given a mandate to ensure that another actor meets specific requirements for their business. In the financial sector, this supervision is often closely linked to the operating licence that the company needs in order to conduct its business. As mentioned earlier, FI has been working over a long period of time on cyber risks as part of its regular supervision of individual financial companies and as part of its framework for the supervision of operational risks.[12]

When assessing whether a company should be granted an operating licence to run a financial business, FI decides whether the company and its management team are suitable for conducting the business in question. This enables us to prevent unsuitable companies from conducting financial business. FI can also take action against companies that violate the rules that apply to the business, ultimately by withdrawing their licence. FI has far-reaching powers of intervention as part of its regular supervision. For example, FI can request that a company or another party provides data, documents, etc., or that a party be called in for interview if they can provide information on a case. FI can also make onsite visits.

FI uses a wide range of rules when supervising cyber security in the Swedish financial sector. What these rules have in common is that they enable FI to intervene with sanctions against companies that do not comply with the rules, and FI can ultimately withdraw their licence to conduct business. Supervision also allows us to regularly check that these companies are complying with the applicable rules. One general requirement for financial companies is that they have to identify and maintain control of the risks associated with their business. As part of this requirement, the financial companies also have to identify and check risks that they or any of their suppliers have been the victim of a cyber attack. Here is an overview of these rules.[13]

FI's supervision of credit institutions (banks and credit market companies) is regulated by the basic provision stipulated in Chapter 6 Section 2 of the Swedish Banking and Financing Business Act.[14] This provision sets out a general obligation for credit institutions to identify, measure, govern, report

[12] FI reports produced by the Banking and Insurance divisions from 2018–19.
[13] It should also be noted that the Financial Stability Board and other international bodies regularly produce various recommendations and reports on cyber security in financial companies.
[14] A more detailed description of FI's tools for the banks' work with cyber security is presented in FI's Supervision Report No 9, Information and Cyber Security Work in Banks, 2018.

internally and control the risks associated with their business. Relevant rules are set out in FI's regulations and general guidelines as well.[15] The European Banking Authority (EBA) has also issued guidelines for managing risks associated with the company's information and communication risks (ICT risks), security risks and outsourcing.[16]

For insurance companies, there are basic provisions in the Insurance Business Act on how to manage cyber risks. Chapter 10 of this act contains provisions on corporate governance, many of which are relevant for the companies' cyber security. They include, inter alia, provisions on risk management, continuity management and outsourcing agreements. These provisions are supplemented by provisions in the Commission's Delegated Regulation supplementing Solvency II and guidelines issued by the European Insurance and Occupational Pensions Authority (EIOPA).[17]

For actors on the securities market, there are a number of different rules in place that relate to cyber security. A lot of the regulation for actors in the financial infrastructure is based on the *Principles for Financial Market Infrastructures* (PFMI), which were jointly developed by the International Organisation of Securities Commissions (IOSCO) and the Bank for International Settlements (BIS).

In terms of central counterparties and central securities depositories, the relevant rules for corporate governance are set out in the EU Regulation on OTC derivatives, central counterparties and trade repositories (EMIR) and the EU Regulation on improving securities settlement and on central securities depositories (CSDR).[18] The requirements for adequate corporate governance include companies being able to identify and manage risks, including cyber risks, in their operations. The Securities Market Act also has similar provisions for securities companies (Chapter 8 Section 4), stock exchanges (Chapter 13 Section 2) and clearing organisations (Chapter 20 Section 1). The various legislation set out above is also supplemented by regulations from FI.[19] It is

---

[15] Finansinspektionen's regulations and general guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions; Finansinspektionen's regulations and general guidelines (FFFS 2014:4) regarding the management of operational risks; and Finansinspektionen's regulations and general guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems.

[16] EBA/GL/2019/04 and EBA/GL/2019/02 guidelines on outsourcing arrangements. Although the guidelines from the EBA or one of the other European supervisory authorities are not formally binding, the relevant companies should comply with them using all the resources at their disposal. ICT is an abbreviation for information and communications technology.

[17] See Articles 258–260 and 274 of Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) and EIOPA's guidelines on the system of governance (EIOPA-BoS-14/253).

[18] Article 26 and Article 45 respectively.

[19] Finansinspektionen's regulations and general guidelines (FFFS 2014:4) regarding the management of operational risks; Finansinspektionen's regulations and general guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems; and

worth noting that there are no rules for cyber security for some trading venues for financial platforms (MTF platforms), fund managers and alternative investment fund managers.

In summary, it is clear that the regulations on cyber risks differ between the various sectors of the Swedish financial sector.

Example: FI's investigations into the Nasdaq companies
In the summer of 2015, FI started its investigation of Nasdaq Stockholm AB and Nasdaq Clearing AB (the Nasdaq companies). These investigations focused on how the companies managed their cyber risks. As functions for, inter alia, information security had been outsourced to the Group's parent company, Nasdaq, Inc., FI investigated the autonomy and independence of these companies.

In December 2016, FI's Board of Directors announced its decision: to issue Nasdaq Stockholm AB with a remark and an administrative fine of SEK 30 million; and to issue Nasdaq Clearing AB with a remark and an administrative fine of SEK 25 million. These sanctions were issued as FI believed that the Nasdaq companies did not have adequate independent competence and had not acquired the information required to be able to assess the quality of the delivered services and therefore place sufficient requirements on the service provider.

The Nasdaq companies appealed FI's decision. The final judgment in this case was presented in August 2020.[20] The Administrative Court overturned FI's decision, as it considered there to be no legal grounds for FI to take action against the companies. The reason for this was that the court considered that the general rule in Chapter 13 Section 1 of the Securities Market Act could not be subject to such a broad interpretation as to cover the grounds on which FI based its sanction decisions.

Supervision of essential services in accordance with the NIS Directive
In 2016, the EU adopted the 'NIS Directive'.[21] This directive aims to raise the level of cyber security in several different sectors. In Sweden, the directive's provisions were enacted primarily through the Information Security for Essential Services and Digital Services Act (2018:1174). This act applies to suppliers that provide an essential service in Sweden; it is the Swedish Civil Contingencies Agency (MSB) that has been tasked with determining which suppliers are subject to the act. MSB regulations (MSBFS 2018:7) on the

Finansinspektionen's general guidelines (FFFS 2005:1) on governance and control of financial undertakings.
[20] Judgment of the Administrative Court in Stockholm on 25 August 2020 in case 25434-19. This judgement was final as FI chose not to lodge an appeal.
[21] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

application and identification of suppliers of essential services list the suppliers that are considered to be essential.

There are two categories that are of particular interest in this context: banking and financial market infrastructure. 'Banking' includes the credit institutions that are in Category 1 or 2 according to FI's annual supervision categorisation, as well as foreign credit institutions that conduct financing business in Sweden through a branch with a balance sheet total of at least SEK 500 billion.[22] 'Financial market infrastructure' includes companies that provide a trading venue with a total turnover of at least SEK 1 billion per day, or services performed by central counterparties. The companies subject to this legislation are required, inter alia, to perform systematic and risk-based information security work and to report any incidents. If a company violates these obligations, the competent supervisory authority is able to issue injunctions and administrative fines.

In December 2020, the European Commission proposed a new NIS Directive that involves more far-reaching obligations for Member States to protect suppliers of essential services.[23] The new NIS Directive, inter alia, enhances rules on incident reporting and also increases the number of companies in the financial sector that may be subject to its rules. In addition to its proposal for a new NIS Directive, the Commission also proposed a new directive on the resilience of critical entities (CER Directive), which will also apply to specific financial companies. [24] The two proposed directives introduce similar requirements for reporting and risk analyses for the companies to which they cover.

Updated Security Protection Act

The Security Protection Act came into force in Sweden on 1 April 2019, setting out obligations for companies conducting security-sensitive activities.[25] The act basically requires both public and private entities to investigate the need for security protection in their business and to plan and take measures as needed. The entity must prevent, inter alia, any adverse effects on data and information systems, as well as the disclosure of any security-sensitive data.

In 2018, a government report presented a proposal for an updated Security Protection Act.[26] According to this updated proposal, FI would be tasked with

[22] See FI's annual supervision categorisation of Swedish credit institutions and the Swedish branches of foreign credit institutions. If banks conduct branch operations in Sweden, FI uses the following categorisations: 'branch' (*filial*), 'significant branch' (*betydande filial*), and 'significant-plus branch' (*särskilt betydande filial*). See *Tillsynskategorisering av svenska kreditinstitut och utländska kreditinstituts svenska filialer för 2021* (FI Ref 20-1930), only available in Swedish.

[23] See the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

[24] See the Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020) 829 final.

[25] Security Protection Act (2018:585) and Security Protection Ordinance (2018:658).

[26] SOU 2018:82 *Kompletteringar till den nya säkerhetsskyddslagen*, only available in Swedish.

supervising the security protection of the financial companies and the equivalent foreign companies that are established in Sweden.[27] The report's proposal has been submitted for consultation and is currently being drafted. A government bill is expected in the spring of 2021.

DORA

On 24 September 2020, the European Commission presented a proposal for a regulation to strengthen the financial market's operational resilience to cyber risks (DORA).[28] The main reason for this is because it has identified a greater need for regulation and supervision to address the growing vulnerability to cyber risks and also a need for greater harmonisation in the regulatory frameworks, both between subsectors and between jurisdictions. The proposed regulation basically targets all of the kinds of companies that are currently subject to FI's supervision. The proposed regulation contains a general requirement for these companies to be in control of all IT-related risks.

This regulation places far-reaching requirements for the financial companies to have adequate systems and policy documents in place to manage these risks. The proposal also contains rules that clarify the responsibilities that the financial companies have for the IT activities that they have delegated to a third party. The European supervisory authorities are tasked with monitoring third-party service providers that are assessed as being 'critical'. This regulation creates more harmonised rules for the actors in the European financial sector. The regulation will now be subject to negotiations between the European Parliament and the Member States.

Categorisation of tools

Based on the overview above, the tools can be divided into the following three categories:

1. **Regular supervisory tools.** This category includes the tools that are included in the regular supervision of financial companies, primarily based on the requirements in the relevant sector legislation for internal governance and control. It also includes rules on ownership and management assessments, as well as capital requirements. The purpose of these tools is to ensure that the financial companies have the knowledge and the ability to manage all the risks associated with their activities. Even though the tools are used to ensure a high level of resilience to cyber attacks, they are largely the same as for the rest of the supervision.

[27] Although the act's current provisions already include these companies, they are under the supervision of the county administrative boards. However, the report stated that the county administrative boards had "basically not conducted any supervision" (p. 371).
[28] Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the finance sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595 final.

2. **Special requirements for financial companies for cyber risks**. This category covers the special requirements that should be placed on financial companies to manage cyber risks. These tools include, inter alia, the supervision of outsourcing agreements, continuity management, system redundancy, incident reporting and testing.

3. **Supervision of third-party service providers**. One special kind of tool that is used in the work to combat cyber risks is the supervision of 'third-party service providers'. These companies have recently taken over an increasing number of tasks that the financial companies used to perform for themselves. It is therefore becoming increasingly important to be able to supervise these companies.

   'Third-party service providers' refer to non-financial companies that perform various IT-related services for a financial company. These companies are frequently large global companies that perform services for a high number of financial and non-financial companies.[29] Although these companies do not conduct licensed financial activities, it is important to ensure that they have adequate resilience to cyber attacks, as a major attack on this kind of provider could have very serious consequences for many financial companies and therefore for the financial system as well.

   As these third-party service providers are often large companies with global activities it can be difficult for an individual national supervisory authority to supervise them. Effective supervision of these providers probably requires close cooperation between the supervisory authorities in several different countries. Another challenge is that these providers can be based outside the EU, which presents a special third-country challenge, for example in terms of equivalence assessments or the application of EU personal data regulations.

4. Cooperation to prevent cyber attacks

It is generally the responsibility of the actor performing a certain activity to combat cyber attacks.[30] This chapter provides an overview of how responsibilities are allocated between the authorities in Sweden in the work to

[29] However, there are also smaller, specialised companies whose services can be of great importance to the industry.

[30] In terms of the authorities, Section 19 of the Crisis Preparedness and the Surveillance Authorities' Measures during Periods of Heightened Alert Ordinance (2015:1052) prescribes that each authority is responsible for ensuring that their own information management systems meet the basic and specific security requirements so that the authorities' activities can be performed in a satisfactory manner. In terms of financial companies, there is legislation as well as regulations from the European supervisory authorities and FI that impose requirements on how they must act to manage risks of cyber attacks in their own activities. The responsibilities that financial companies have for managing risks associated with cyber attacks and FI's ability to supervise their risk management will be discussed in a later chapter.

prevent cyber attacks on the financial sector. It also describes the structures that are in place for public-private cooperation. It concludes with a brief international overview.

Societal work and cyber security

In 2018, the Swedish Parliament adopted a national strategy for information and cyber security,[31] whose purpose is to be a platform for Sweden's continued development work in this area. This strategy will ensure that actors in society have the ability in the long term to work effectively on information and cyber security and raise awareness and knowledge of this throughout society. In this section we will present a brief description of the work being carried out in society on cyber security, focusing on the financial sector.

MSB and the Swedish Security Service

In Sweden, there are several authorities that have a general responsibility for cyber security in society. MSB (the Swedish Civil Contingencies Agency) is tasked by the Swedish government to support and coordinate societal information security, and to analyse and assess global developments in the field. This assignment includes providing advice and support, in relation to preventive work, to other government authorities, municipalities, regions, companies and organisations.[32] MSB is also responsible for Sweden having a national function tasked with supporting society in its work to prevent and manage IT incidents. As part of this assignment, the authority works, inter alia, with the authorities that have special tasks in the field of information security.[33] MSB also issues regulations on IT and information security.

The Swedish Security Service has an important role to play in the field of security protection. This authority is tasked with supervising, inter alia, FI's obligations pursuant to security protection legislation. A proposal is currently being produced to update the security protection legislation, which will give both the Swedish Security Service and the Swedish Armed Forces a coordinating responsibility. It would mean, inter alia, that these authorities would be tasked with developing methodological support and facilitating the sharing of experiences between the various supervisory authorities.[34]

The authorities that have special responsibilities in the field of information security include the Swedish Armed Forces, the Swedish Defence Materiel Administration (FMV), the Swedish National Defence Radio Establishment, (FRA), the Swedish Post and Telecom Authority (PTS), the Swedish Police Authority and the Swedish Security Service. These authorities are members of the Cooperation Group for Information Security (SAMFI), which is led by MSB. The main task of this group is to implement together the proposals for

[31] A National Cyber Security Strategy, Skr. 2016/17:213.
[32] Section 11a of the Instructions for the Swedish Civil Contingencies Agency Ordinance (2008:1002).
[33] Section 11b of the Instructions for the Swedish Civil Contingencies Agency Ordinance (2008:1002).
[34] SOU 2018:82 *Kompletteringar till den nya säkerhetsskyddslagen*, only available in Swedish.

measures that are produced annually as part of the national action plan for societal information security.

Cooperation for supervision in accordance with the NIS Directive

As mentioned earlier, FI is responsible for specific supervision in accordance with the provisions of the NIS Directive. MSB is responsible for coordinating the work between the authorities that are responsible for performing supervision in accordance with the NIS Directive. [35] The NIS Directive also states that each Member State has to establish a *Computer Security Incident Response Team* (CSIRT); this is a specific function to facilitate the exchange of information and cooperation between the Member States. As the national contact point for the NIS Directive and the national CSIRT unit, MSB participates in various international forums, including the NIS Cooperation Group and CSIRT's Network, to monitor and contribute to the development of the NIS Directive in the EU.[36]

A new centre for cyber security

In 2019, the Swedish government decided to set up a National Cyber Security Centre. This centre will comprise the Swedish National Defence Radio Establishment (FRA), MSB, the Swedish Armed Forces and the Swedish Security Service and will support preventive work for the activities that require the most protection in society.[37] Cooperation between private and public actors will play a central role in the tasks and activities of this centre. The centre started to be built up in 2020 and will be fully operational by 2025.[38]

FI's role in total defence

In 2015, the Swedish government decided to resume coherent planning for its total defence. This work includes assigning special responsibilities to various authorities as part of this total defence. The Swedish government has appointed FI as an authority responsible for surveillance. This means that FI is obliged to analyse whether there are vulnerabilities, threats or risks in the authority's area of responsibility.

Authorities that are responsible for surveillance also have to plan so that they can adapt their activities if a situation involving security policy changes. The ordinance specifies in more detail the obligations for these authorities. These obligations include, inter alia, that the authorities must cooperate with the other relevant government authorities, municipalities, regions, associations and businesses. The Swedish government has grouped the authorities responsible

[35] Section 17 of the Information Security for Essential Services and Digital Services Act.
[36] See *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022: redovisning 2020*, only available in Swedish. Sweden's national CSIRT is Cert.se, which is tasked with supporting society in its work to manage and prevent IT incidents.
[37] The authorities listed here have entered into an agreement for in-depth cooperation with the Swedish Police Authority, PTS and FMV.
[38] Response to the assignment (Fö2019/01000/SUND) to set up a National Cyber Security Centre on 19 December 2019. See also 2020/21:1 Expenditure area 6, p. 14.

for surveillance into cooperation areas, which will make it easier for them to coordinate.[39] FI is part of the Economic Security cooperation area.[40]

Government report into civil defence

On 1 March 2021, the final version of the government report into civil defence was presented.[41] The report proposes that the cooperation areas should be wound up and replaced by ten preparedness sectors and four special preparedness areas. They include authorities that are responsible for activities and functions that are particularly important to maintain during a crisis, at times of heightened alert and ultimately during a war. The proposal is to have one authority in each preparedness sector that has a mandate to focus on and coordinate work within the sector: an authority responsible for the sector.

The report proposes that FI is appointed as the authority responsible for the Financial Services preparedness sector. The proposal is for this sector to comprise FI and the Swedish National Debt Office, with the Riksbank as a coopted member. If this proposal is adopted, FI will be required to maintain the sector's planning for heightened alert and for peacetime crises that can affect the sector, such as a major cyber attack. It is also proposed that the authority responsible for a sector is also responsible for ensuring that capacity is built up within the sector so that it can operationally manage crises and periods of heightened alert; this authority would be responsible for contact with the other sectors and preparedness areas as well.

The report also proposes that a special preparedness area is set up for cyber security, as a cooperation between the Swedish Security Service, MSB, the Swedish Armed Forces and FRA.

Cooperation organisations for cyber security

There are currently several different forums that include both private and public actors that have responsibilities in the field of cyber security. Some focus more generally on cyber security, while others specialise in financial stability. Here is a brief description of some of the more central cooperation organisations.

The Cyber Security Council at the MSB, bringing together representatives from a number of authorities, higher education institutions and the business community. It does not have any representatives from FI nor any other authority that has a special responsibility for financial stability. The Cyber Security Council works to, inter alia, ensure that the council's members inform each other about development trends, and to voice their opinions on and ensure the quality of MSB's work in this area.

---

[39] Section 7 of the Crisis Preparedness and the Surveillance Authorities' Measures during Periods of Heightened Alert Ordinance (2015:1052)

[40] Other authorities in this cooperation area are the Swedish Social Insurance Agency, MSB, the Swedish Pensions Agency, the Swedish National Debt Office and the Swedish Tax Agency. The Riksbank (Sweden's Central Bank) is involved in this work as a coopted member.

[41] SOU 2021 *Struktur för ökad motståndskraft*, only available in Swedish.

MSB also administers five different sector-specific forums for sharing information about information security, called 'FIDI'. These forums have been set up to exchange information about threats, vulnerabilities and incidents between relevant authorities and private actors. One of these forums, FIDI-Finans, focuses on the financial sector. It includes representatives of the major Swedish banks, financial infrastructure companies, the Riksbank, the Swedish National Debt Office, the Swedish Police Authority and FRA.[42] FI decided early on that it would not be a member of this particular forum. However, we are a member of the Economic Security Collaboration Area (SOES), which is a cooperation forum that focuses on ensuring that robust systems are in place to make payments. SOES is led by MSB and comprises a total of eight authorities.[43]

Another important cooperation body is FSPOS (the group for private-public cooperation in the financial sector in Sweden). FSPOS was founded in 2005 and is a voluntary cooperation forum, with members from various authorities, including FI, as well as businesses in the financial sector. FSPOS has a permanent organisation in place with three different levels: its council, board and working groups. FI has representatives at every level. FSPOS's operations are funded by the member organisations paying the costs of their own employees who take part in this work. Its activities aim to ensure that private and public organisations in the financial sector can work to improve their ability to prevent, prepare and quickly recover from operational crises. FSPOS's work therefore does not focus solely on cyber security, even though this issue is central to the group's activities.[44]

Four Swedish authorities have a special responsibility to work to secure a stable financial system. These authorities are the Swedish National Debt Office, the Riksbank, the Government Offices of Sweden (Ministry of Finance) and FI. Although these authorities have a shared responsibility, they have different tasks and different tools to perform their tasks. The authorities are members of the Financial Stability Council, a discussion forum for issues relating to financial stability and how to counteract financial imbalances. As the issue of cyber attacks on financial companies can impact financial stability in Sweden, the council has discussed issues surrounding cyber security in the financial sector.

The image below shows the current cooperation groups and other organisations that work with cyber security issues in the Swedish financial

---

[42] More information about the cooperation organisations administered by MSB can be found on its website: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samverkan-inom-informationssakerhet/ (read 21 February 2021), only available in Swedish.

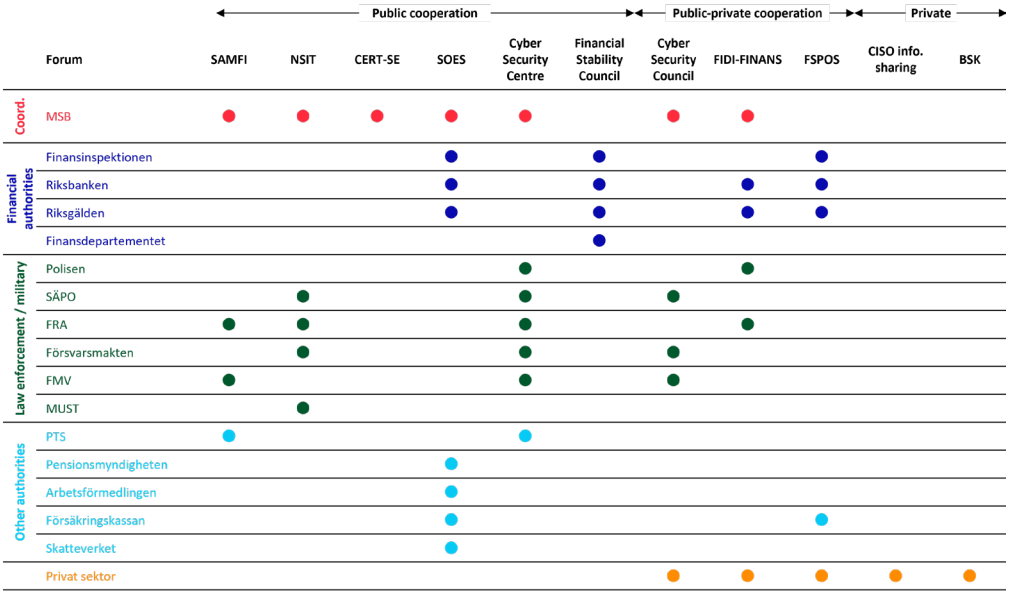
[43] More information about SOES is available on MSB's website: https://www.msb.se/sv/publikationer/samverkansomradet-ekonomisk-sakerhet-soes/ (21 February 2021), only available in Swedish.

[44] See FSPOS's operational plan for 2021 and its strategic plan for 2020–2023, only available in Swedish.

sector.[45]

	Forum	Led by	Description
Public cooperation forums	SAMFI (the Cooperation Group for Information Security)	MSB	Group of the four authorities defined as most critical for the national cyber security strategy – in charge of executing the strategy
	NSIT (National Cooperative Council against Serious IT Threats)	MSB	Cooperation between law enforcement and the military – analyses and evaluates threats and vulnerabilities
	CERT-SE (Swedish Computer Security Incident Response Team)	MSB	Supports authorities, firms and municipalities when cyber incidents occur and publishes warnings and advice on vulnerabilities
	SOES (the Cooperation Council for Financial Security)	MSB	Not directly focused on cyber risk, but works to ensure access and confidence in payments, especially from a societal perspective
	National Cyber Security Centre	MSB	Fully operational in 2025 and will produce analyses, spread information on threats, as well as coordinate during IT incidents and attacks
	Financial Stability Council	Ministry of Finance	Twice yearly meetings between the four authorities responsible for financial stability
Public-private	Cyber Security Council	MSB	Set up to inform, provide opinions on and quality assure MSB's work on cyber security – includes representatives from academia & private sector
	FIDI-FINANS (Forum for Information Sharing on Information Security)	MSB	One of the FIDI forums set up by MSB for information sharing in the sectors most exposed to cyber risk (focused on the financial sector)
	FSPOS (The Financial Sector's Private-Public Cooperation Group)	Riksbanken (rotating)	The main forum for public-private cooperation in the financial sector – has a working group focused on cyber risk
Private	BSK (Bankers' Association's Security Committee)	Bankers' Association	Committee for the shared security work between the banks in the Bankers' Association (including cyber security)
	CISO information sharing	N/A	Loosely organised cooperation on cyber security issues between the CISOs of the main banks

The image below shows the extent to which Swedish authorities participate in the various cooperation forums for cyber security.[46]



In summary, there is a significant number of cooperation bodies and forums to analyse and combat cyber risks from different angles. FI is currently a member of a selection of them. However, there is not one organisation or forum that clearly focuses on the work of the financial sector to combat cyber risks. In the future, it is likely that it will be necessary to increase cooperation between

[45] Source: Oliver Wyman, Combatting the Cyber Threat in Sweden – An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector.
[46] Source: Oliver Wyman, Combatting the Cyber Threat in Sweden – An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector.

authorities and industry representatives to combat cyber threats against the Swedish financial sector.

International overview

It is relevant in this context to take a look at other countries that have already developed cooperation for cyber threats in the financial sector. **Denmark** has adopted a national strategy for its cyber security work. Unlike Sweden, Denmark has developed national sector-specific strategies as well. As part of the framework for its sector-specific strategy for the financial sector, its financial supervisory authority, Finanstilsynet, has been commissioned to be a *decentralized unit for cyber and information security for the financial sector (DCIS).* This means that Finanstilsynet is responsible for the tasks described in this strategy. DCIS therefore works on the financial sector's preparedness for cyber threats, analyses threats and vulnerabilities, and disseminates knowledge.

The **United Kingdom** has a trade association called UK Finance and, on the initiative of the Bank of England, the UK's central bank, it set up the Financial Sector Cyber Collaboration Centre (FSCCC). The purpose of this centre is to enable and facilitate cooperation between public authorities, such as the Bank of England and the Financial Conduct Authority (FCA), and the private sector. This makes it easier to share information between companies operating in the financial sector and the relevant supervisory authorities. The FSCCC enables the exchange of information with the intelligence agencies and law enforcement authorities. Each member of the FSCCC can decide the extent to which they wish to participate in this cooperation work.

Singapore adopted its Cybersecurity Act in 2018, which imposes strict requirements on the financial sector in the country. The country's financial supervisory authority is called the Monetary Authority of Singapore (MAS), which has set up several permanent committees for cooperation in the financial sector for cybersecurity. MAS has established an advisory body as well called the Cyber Security Advisory Panel, which comprises international cyber security experts who advise both MAS and companies in the financial sector on how they should work with cyber security. This panel also serves as a forum for exchanging views on the work to prevent cyber threats.[47]

[47] See https://www.mas.gov.sg/who-we-are/MAS-Advisory-Panels-and-Committees/Cyber-Security-Advisory-Panel (read 2021-02-21).