



**FINANSTILSYNET**

THE FINANCIAL SUPERVISORY  
AUTHORITY OF NORWAY

Financial Institutions' Use of Information  
and Communications Technology (ICT)

# RISK AND VULNERABILITY ANALYSIS

2023

## Risk and vulnerability analysis

Finanstilsynet performs an annual risk and vulnerability analysis (RVA) of the financial sector's use of ICT. The purpose of the report is to describe risks and highlight the principal threats to and vulnerabilities in financial institutions' ICT systems and the financial infrastructure that could have an impact on the institutions, financial stability and well-functioning markets. Vulnerabilities and threats targeting institutions' customers are also described. Monitoring of reported incidents, findings from inspections and other contact with the financial sector give Finanstilsynet a good insight into financial institutions' use of ICT, payment services and relevant risk areas.

# Risk and Vulnerability Analysis 2023

- 1. SUMMARY .....4
- 2. FINANCIAL INFRASTRUCTURE .....7
  - 2.1 Importance .....7
  - 2.2 Financial Infrastructure Crisis Preparedness Committee .....8
  - 2.3 Changes in the financial infrastructure and joint measures in the financial industry .....9
- 3. CYBERCRIME AND THE THREAT LANDSCAPE .....12
  - 3.1 The cyberthreat landscape is evolving .....12
  - 3.2 Organised crime as a threat .....12
  - 3.3 Foreign states as a threat .....13
  - 3.4 Cyberattacks as a political tool .....13
  - 3.5 Attacks on value chains .....14
  - 3.6 Attacks on key service providers and data centres .....15
  - 3.7 Criminals' use of artificial intelligence .....15
  - 3.8 National measures – TIBER-NO .....15
  - 3.9 Institutions' countermeasures .....16
  - 3.10 Collaboration in the area of security .....17
- 4. FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS .....19
  - 4.1 Inspections of ICT and payment services .....19
  - 4.2 Vendor management of access management .....21
  - 4.3 The institutions' assessment of important factors related to ICT operations .....22
  - 4.4 Summary of the institutions' risk and vulnerability reporting .....24
  - 4.5 Strengthened consumer protections in the new Financial Contracts Act .....28
  - 4.6 Misuse of login credentials .....29
  - 4.7 Risks associated with using chatbots .....30
- 5. FRAUD AND FRAUD STATISTICS .....32
  - 5.1 Reporting of fraud statistics .....32
  - 5.2 Losses associated with the fraudulent use of payment cards .....32
  - 5.3 Losses associated with the fraudulent use of payment cards at norwegian merchants .....35
  - 5.4 Losses linked to account transfers .....35
  - 5.5 Losses related to account transfers initiated by payment initiation service providers .....36
  - 5.6 Losses from social engineering fraud .....36
  - 5.7 Losses where the fraudster issues the payment order .....37
- 6. INCIDENT REPORTING .....38
  - 6.1 Number of ICT-related incidents .....38
  - 6.2 Security incidents .....38

6.3 Errors and vulnerabilities at cloud service providers .....	40
6.4 Incidents in systems for detecting money laundering and terrorist financing.....	40
6.5 Causes of operational incidents.....	41
6.6 Incidents by type of institution.....	41
6.7 Analysis of incidents as a measure of availability.....	43
6.8 Incidents related to problems with dedicated PSD2 interfaces.....	44
<b>7. OUTSOURCING.....</b>	<b>45</b>
7.1 Notification of outsourcing.....	45
7.2 Governance .....	46
7.3 Contractual provisions for the termination of outsourcing agreements .....	46
7.4 Risk associated with outsourcing.....	46
<b>8. ASSESSMENT OF THE FINANCIAL INFRASTRUCTURE AND INSTITUTIONS' ICT OPERATIONS.....</b>	<b>49</b>
8.1 The financial infrastructure is robust.....	49
8.2 Risk associated with vulnerabilities in institutions' ICT operations.....	49
<b>9. NEW REGULATIONS ON DIGITAL RESILIENCE – THE DORA REGULATION.....</b>	<b>52</b>

Cut-off date 3 May 2023

Figure data updated as of 3 May 2023

# 1. SUMMARY

Norway's financial infrastructure is robust. Changes to the cyberthreat landscape, including those due to Russia's attack on Ukraine and an increase in cybercrime, have contributed to a greater focus on the risk of systemic cyber incidents and the importance of digital resilience and recoverability in the financial sector.

Finanstilsynet and the Financial Infrastructure Crisis Preparedness Committee (BFI) pay particular attention to entities that support important functions, including critical functions in society identified by the Norwegian Directorate for Civil Protection (DSB).<sup>1</sup> Key institutions in Norway's financial infrastructure generally have satisfactory contingency plans. The actors maintain constant oversight of operations and have quickly implemented required measures when necessary.

No ICT incidents had consequences for financial stability in 2022. Both the number of security incidents and the number of operational incidents were on a par with 2021. There has been a reduction in adverse consequences due to incidents in recent years, and Finanstilsynet's assessment is that the overall availability of payment and other customer services was generally the same from 2021 to 2022 and slightly better than in the preceding years.

There were fewer attacks on the financial infrastructure in 2022 than in 2021, although the scale of cybercrime with consequences for the financial sector appears to still be increasing. Even though cybercrime targeted at institutions in the Norwegian financial sector has not led to systemic crises or severe incidents, serious vulnerabilities have been identified that could have had major consequences had they been exploited. Service providers also experienced security incidents with consequences for the institutions involved.

Institutions in the financial sector are constantly working to strengthen their defences and automate the management of adverse incidents. Cyberattacks are usually averted before institutions and their customers suffer any consequences. The financial industry's collaboration via NFCERT<sup>2</sup> helps improve knowledge about the risk landscape and relevant threats, and better equip institutions to handle attacks.

Finanstilsynet believes that to maintain the financial infrastructure's resilience, institutions should strengthen their ICT work by reducing the likelihood of operational incidents, increasing resilience in relation to cybercrime and enhancing ICT security. This work must be tailored to developments in the cyberthreat landscape.

Supervisory activities in 2022 identified weaknesses and vulnerabilities in the institutions' ICT work. Finanstilsynet pointed out weaknesses in, for example, the emergency preparedness and crisis management plans of various institutions, such as inadequate or missing business impact analyses. In addition, lack of compliance with current regulations for outsourcing ICT operations was identified, including some cases where agreements had not been considered by the institution's board of directors. The monitoring of some service providers' compliance with institutions' security requirements was also inadequate. Other findings include inadequate involvement in service providers' testing of their emergency preparedness solutions, inadequate ICT expertise in institutions' second line of defence, and insufficient transaction monitoring with respect to money laundering and terrorist financing.

---

<sup>1</sup> [BFI](#) is chaired by Finanstilsynet and follows up emergency preparedness and incidents in the financial infrastructure. The link points to a topic page on Finanstilsynet's website.

<sup>2</sup> [Nordic Financial CERT](#). Link to NFCERT's website.

Following a security breach at an ICT service provider in autumn 2021, Finanstilsynet conducted follow-up supervision in 2022 on institutions' improvement of ICT service provider governance, focusing on management, monitoring, and control of access rights.

The electronic payment system's emergency preparedness was further strengthened in 2023 with the introduction of so-called 'offline PIN' in BankAxept's card system. This allows the PIN code to be verified against information on the payment card if payment terminals lose network connectivity.

Finanstilsynet considers vulnerabilities in institutions' defences against cybercrime to be the main ICT risk. This is due to both the high probability of attacks and the serious consequences should an attack succeed. The risk associated with failures in institutions' defences against cybercrime is also regarded as somewhat higher than in 2021. Vulnerabilities in relation to vendor management, access management and information leaks are also key risks, and the overall risk is considered moderate to high. While the risk associated with inadequate vendor management was considered higher in 2022 than in the year before, the risk associated with institutions' defences against information leaks was regarded as slightly lower.

Through reporting and dialogue with Finanstilsynet, institutions and providers of ICT services pointed out several key risks and vulnerabilities associated with ICT operations. They highlighted that an inadequate overview of the controls included in an institution's internal control can result in operational risk not being identified. Inadequate expertise can result in problems and errors that can be challenging to resolve, and more complex service provider relationships can result in poorer follow-up and control over critical and outsourced ICT services. The institutions also pointed out that insufficient security management can result in criminals causing damage to institutions through cyberattacks.

Other risk factors highlighted by institutions include complex value chains and shortages of ICT resources. They also pointed out that the scale of ID theft is growing. The risk of ID theft is mentioned as one of the highest risks. More complex system portfolios can result in poorer operational stability, and the rapid pace of development presents risks linked to change management. Moreover, they highlight that inadequate emergency preparedness can present challenges with respect to maintaining critical ICT services in the event of serious incidents that impact normal operating locations. The institutions also point out that inadequate access management can result in damage due to intentional or unintentional acts, and that inadequacies or errors in data can result in analyses, checks and decisions being made on an incorrect or inadequate basis.

Phishing activities increased in 2022, where criminals targeting both customers and employees attempted to gain access to user login credentials (one-time codes, passwords, etc.). In one case, an employee's login credentials were stolen. The attacker acquired all the employee's rights and used them for criminal acts.

The widespread use of BankID for both private and public services within and outside the financial sector entails a risk of users being insufficiently vigilant with respect to fake logins and, for instance, being tricked into disclosing security credentials. The wide range of uses presents criminals with opportunities to exploit a number of methods in their fraud activities.

Some 156 000 fraudulent transactions were carried out with payment cards in 2022, compared with 147 000 in 2021. Despite a small increase in the number of fraudulent transactions, losses from card fraud increased by 35 per cent to NOK 219 million in 2022. The proportion of fraudulent transactions was highest for cross-border transactions, especially for transactions executed in countries outside the EEA.

Losses due to account transfers, mainly using online banks, amounted to NOK 395 million in 2022, up from NOK 346 million in 2021. However, as a percentage of total account transfers, losses were slightly lower in 2022 than in 2021. The losses were related to both transactions in which the fraudster issued or modified the payment, and transactions where the fraudster manipulated the payer into making the payment themselves.

Losses due to social engineering, where the payer is tricked into carrying out the fraudulent transaction, amounted to NOK 290 million in 2022, compared with NOK 240 million in 2021. NOK 269 million of the NOK 290 million stemmed from account transfers, while the remainder was linked to payment card use. A proportion of the fraudulent transactions where the fraudster initiates the transaction based on stolen information is also regarded as being a consequence of social engineering. There is probably some obscurity in the figures, which makes it difficult to estimate the extent of losses due to social engineering.

Banks prevent an increasing proportion of fraud attempts, which helps limit losses. Social engineering fraud still appears to be the most profitable method for criminals.

In 2022, Finanstilsynet received more than 240 outsourcing notifications, which is about 20 per cent more than the year before. As in previous years, the notifications bear witness to the growing use of cloud services for both application and infrastructure services. Outsourcing often results in institutions having to deal with an increased number of platforms, which can lead to greater complexity and more complicated risks.

Institutions must assess a number of risk factors when considering outsourcing ICT operations, including governance, security, monitoring of service provision, emergency preparedness and crisis management. They also need sufficient expertise to, for example, stipulate the necessary requirements for the service provider's solutions and ICT security and fully understand the service provider's deliveries. Monitoring outsourced ICT operations must be integrated into the institution's risk management and internal control system.

The main themes for Finanstilsynet's inspections of ICT and payment services in 2023 will be the institutions' governance of ICT operations, management of ICT security, including cyber security, and emergency preparedness, and testing of their emergency preparedness and crisis management. Furthermore, through its supervisory activities, Finanstilsynet will assess the governance and monitoring of outsourced ICT operations, institutions' payment services, and major changes in the financial infrastructure.

Finanstilsynet believes it is important for institutions to properly address the security of their services so that customers do not suffer losses. Through its supervisory activities, Finanstilsynet also ensures that institutions do not share their customers' data without consent and that these data do not fall into the hands of unauthorised parties.

Finanstilsynet monitors ICT incidents and vulnerabilities in institutions' ICT solutions. The focus is on institutions identifying causes and implementing preventive measures. The threat landscape for cybercrime is monitored and institutions' emergency preparedness work targeting vulnerabilities and cyber security is reviewed.

BFI follows up emergency preparedness and incidents in the financial infrastructure. In special circumstances, such as the Covid-19 pandemic and the war in Ukraine, BFI closely monitors the ICT operations and emergency preparedness of the main actors.

For further information about Finanstilsynet's monitoring of supervised institutions, see appendix 3.

## 2. FINANCIAL INFRASTRUCTURE

### 2.1 IMPORTANCE

Efficient, robust and stable payment and settlement systems and marketplaces, as well as trust between market participants, are fundamental prerequisites for financial stability and well-functioning markets. The Norwegian Directorate for Civil Protection (DSB) has identified financial services as a critical function.<sup>3</sup> If payments or trades in financial instruments cannot be executed or settled, important social functions will quickly stop functioning satisfactorily. The social consequences could be particularly severe if institutions operating on behalf of several or all institutions are affected.

The financial infrastructure is designed to ensure that payments and transactions in financial instruments are registered, cleared and settled. The infrastructure is complex and includes many parties and service providers, see box 2.1. An entity's or service provider's poor resilience or security can constitute a weak link in a value chain, meaning that incidents can spill over to other parties. The financial sector is also dependent on infrastructure such as power supply and electronic communication. Failures involving key entities in the financial industry or infrastructure can have significant social consequences<sup>4</sup> and, in a worst-case scenario threaten financial stability, irrespective of whether the failure is caused by criminal activity or by operational non-conformances.

Sensitive information going astray or breaches of the rules on handling inside information may undermine confidence in marketplaces and the financial system. If unauthorised persons gain access to customer and account data and compromise them or render them unavailable, customers and institutions can face significant challenges.

Finanstilsynet and Norges Bank cooperate on monitoring the Norwegian financial infrastructure, including through joint inspections, reports, and risk assessments.

---

<sup>3</sup> Norwegian Directorate for Civil Protection (DSB): [Vital functions in society](#)

<sup>4</sup> The Security Act defines both economic stability and freedom of action as national security interests, cf. [Security Act](#), section 1-5 Definitions (Lovdata). This includes financial infrastructure and objects that are vital to the functioning of civil society.

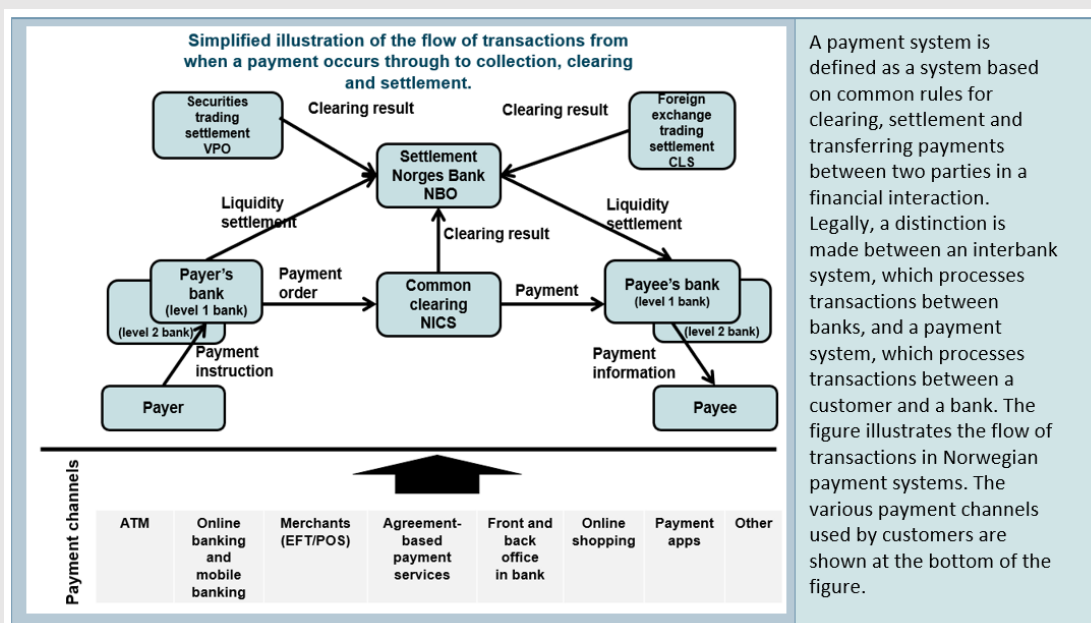


## Box 2.1 Flows of transactions in the Norwegian payment system

The financial infrastructure consists of the payment system and the securities settlement system, as well as the Norwegian Central Securities Depository, marketplaces and key counterparties.

The payment system includes interbank systems and systems for payment services for transferring funds, with formal and standardised arrangements and common rules for processing, clearing, or settling payment transactions.

The payment system, including payment services, is regulated by legislation such as the Act relating to Payment Systems, Regulations on Payment Services Systems, and Regulations on Payment Services, as well as through the financial services sector's self-regulation administered by Finance Norway and Bits.



Source: Finanstilsynet

The securities sector is regulated by legislation such as the Securities Trading Act, the Securities Trading Regulations and the Central Securities Depository Act. The securities sector includes actors involved in securities transactions related to equity instruments such as shares and equity certificates, including the execution of trades and related settlements.

## 2.2 FINANCIAL INFRASTRUCTURE CRISIS PREPAREDNESS COMMITTEE

The Financial Infrastructure Crisis Preparedness Committee (BFI) was established in order to:

- prepare and coordinate measures for preventing and resolving crisis situations and other situations that may result in major disruptions to the financial infrastructure. In a crisis situation, the committee must notify and inform affected actors and authorities of the problems that have occurred, the potential consequences of the problems and the measures that must be implemented to resolve the problems.
- perform the necessary coordination of preparedness within the financial services sector. This includes, based on the civil preparedness system, coordinating the preparation and implementation of notification plans and preparedness measures in the event of national security crises and war.

Finanstilsynet chairs and is the secretariat for the committee. Central authorities and actors responsible for critical functions in the financial infrastructure sit on the committee. BFI holds regular meetings and conducts annual emergency response exercises. The work in BFI, which reviews severe and critical incidents, helps provide Finanstilsynet with a good, broad picture of the status of the financial infrastructure. Further information on BFI's work is available in the committee's annual reports, see Finanstilsynet's website, topic page [Financial Infrastructure Crisis Preparedness Committee \(BFI\)](#).

## 2.3 CHANGES IN THE FINANCIAL INFRASTRUCTURE AND JOINT MEASURES IN THE FINANCIAL INDUSTRY

A number of significant changes were announced and implemented in the Norwegian financial infrastructure in 2022.

In 2020, the banks in the Eika Alliance entered into an agreement with Tietoevry regarding delivery of core banking solutions to the local banks in the alliance. The transition from SDC to Tietoevry is taking place in batches and completion is planned for 2023. Several banks have already completed the transition without significant non-conformances. The agreement will result in a significant increase in the proportion of Norwegian banks using Tietoevry as their operations service provider.

Verdipapirsentralen AS (Euronext Securities Oslo) is planning to transfer its ICT operations to Tietoevry in May 2023.

Seen in isolation, the transfer to Tietoevry of Verdipapirsentralen AS and the banks in the Eika Alliance increases concentration risk since several institutions in the financial sector already use Tietoevry as their operations service provider.

To develop cross-border payment services in the Nordic countries, Vipps entered into an agreement in 2021 for a common solution for Vipps' wallet and payment solutions, Danske Bank's wallet MobilePay and OP Financial Group's wallet Pivo. Objections from the European competition authority led Pivo to withdraw from the partnership. In 2022, Vipps merged with MobilePay and its business was integrated into the new company Vipps MobilePay AS in May 2023. The agreement resulted in BankAxept and BankID being separated from Vipps' wallet business and established as a separate company, BankID BankAxept AS.

In 2020, BankID BankAxept AS launched the BankID app. The gradual phasing out of 'BankID på mobil' (BankID Mobile) started in 2022. New users are no longer able to activate 'BankID på mobil' although the solution will continue to function during a transitional period.

### **Modernisation of the payment infrastructure**

#### Instant payments

In 2021, Bits, the banking and financial industry's infrastructure company, initiated the 'Straks 2.1' project for transition to ISO 20022 in the transaction exchange for instant payments and direct submission to the NICS Real clearing system. The project is scheduled for completion in the first half of 2023. By the end of 2022, more than 60 banks had adopted the Straks 2.1 solution. Increasing the use of instant payments is dependent on meeting the corporate market's need to pass on structured customer information.

#### Modernisation of the Norwegian Interbank Clearing System (NICS)

Modernising NICS is an important long-term measure initiated by Bits in order to maintain an efficient and secure interbank clearing infrastructure. NICS is intended to only be a clearing solution, standardised by aligning NICS with ISO 20022 and eliminating ties between NICS and other services to reduce service provider dependence. The project will affect a number of banking solutions in addition to the NICS solution.

### Changing banks (AvtaleGiro)

Bits has developed functionality that enables customers to move fixed direct debit payment orders easily between banks when changing banks using self-service solutions. This will simplify changing banks. The solution went live at the start of 2023.

### **BankAxept backup solution**

The Norwegian financial industry has established a backup solution for BankAxept in order to strengthen emergency preparedness in the electronic payment system. Participation in the backup solution is voluntary for merchants that accept BankAxept payment cards. The backup solution was strengthened in 2021 by significantly increasing the capacity for the use of BankAxept payment cards. This enhancement is offered to critical actors in the retail market with a broad market presence, such as supermarkets, pharmacies and petrol stations.

For the backup solution to function as a satisfactory emergency preparedness solution, merchants must sign up and regularly test that it works as intended. An incident on 16 May 2022 revealed that several merchants had not activated the backup solution and that testing of the payment terminals was inadequate, see section 6.5. To improve the electronic payment system's emergency preparedness, the banks and BankAxept must increase the number of merchants enrolled in the backup solution, particularly critical actors in the retail market.

### **Offline PIN**

The financial industry is constantly striving to improve the emergency preparedness of the electronic payment system. So-called 'offline PIN' has been introduced as a measure to strengthen BankAxept's card system. It allows the PIN code to be verified against information on the payment card if payment terminals lose network connectivity. The solution can be activated when, for instance, BankAxept's backup solution is in operation, provided that the card is compatible. The project started in 2022 and the issuance of cards that support offline PIN is expected to start in 2023. All ordinary BankAxept cards will have to be replaced, which will take approximately three years.

### **Joint digital solutions for the insurance industry**

Insurers in Norway are working together on a major project to establish and operate joint solutions via Finance Norway Insurance Services. This is a key actor in the Norwegian insurance industry's infrastructure and its purpose is to perform tasks and activities that the members believe should be carried out jointly. Some of the key solutions are:

- TFFAuto Register of motor vehicles subject to compulsory insurance in Norway
- DBS Appraisal system for damage to motor vehicles.
- Finans-FREG The financial industry's interface with the modernised population register, FREG.
- Norsk pensjon A pension portal that provides a summary of your expected total retirement pension from different pensions schemes.
- Pension Account Register A register of pension accounts.

### **Collaboration between the financial industry and the public sector in Norway (DSOP)**

The public sector and the financial industry collaborate on digitalising and improving the efficiency of important services via DSOP.<sup>5</sup> The solutions provide significant benefits for the financial industry, customers and the public sector. Several projects are under development. Regulatory clarifications were needed for some of the services before their full functionality could be put into use. Both the original purpose behind

---

<sup>5</sup> Bits' website: [Digital Samhandling Offentlig Privat](#) and [Aktivitetsrapport DSOP 2022](#)

collecting data and sector-specific regulations can provide guidance on further sharing of information. A key principle in DSOP involves reusing functionality established in earlier projects and existing public or private national solutions.

## 3. CYBERCRIME AND THE THREAT LANDSCAPE

### 3.1 THE CYBERTHREAT LANDSCAPE IS EVOLVING

The cyberthreat landscape is constantly evolving, partly as a result of the war in Ukraine and the overall security situation, including tensions between China and the US. Criminals are constantly developing their methods and how they collaborate. It is also difficult to distinguish between threats from organised criminals and from foreign intelligence services since criminal groups often provide services to state actors. Both the Norwegian Intelligence Service (E-tjenesten) and the Norwegian Police Security Service (PST) point out that nation-state actors are a significant threat, including through their use of intelligence and network operations (digital mapping and sabotage of critical infrastructure), while the Norwegian National Security Authority (NSM) points out threats such as the recruitment of insiders within institutions.

In 2022, the cyberthreat landscape helped increase awareness of systemic cyber risk and the importance of digital resilience. Threat actors are also likely to exploit any vulnerabilities that arise due to the increasing digitalisation of the financial sector.

The threat posed by actors searching for security vulnerabilities in widely used software appears to be increasing. Such security vulnerabilities can, for example, result in information leaks and/or unauthorised changes to an institution's systems and infrastructure.

Institutions are constantly striving to improve their systems for monitoring suspicious activity, automatically detecting incidents and preventing attacks. Even though the institutions' systems are steadily improving and incidents are increasingly managed automatically, detected incidents still require comprehensive manual review. Cyberattacks are usually prevented before institutions and their customers suffer any consequences.

Institutions are constantly striving to improve their expertise in cyber security. As described in section 3.10, the cooperation via NFCERT helps increase awareness of the threat landscape and risks targeting the financial industry, with the intention to better equip institutions to handle cyberthreats and prevent adverse incidents.

Institutions must continue their work on analysing risks and vulnerabilities, implementing preventive measures, and preparing to deal with attacks and the consequences of such attacks. Protecting confidential information and raising the awareness of employees are important elements of this work.

Finanstilsynet continues to observe varied levels of maturity in institutions with respect to assessing the risk of inadequate data protection. For the sake of preventing and managing incidents effectively, it is important that institutions analyse which assets may be exposed through business impact analyses.

### 3.2 ORGANISED CRIME AS A THREAT

Organised cybercrime usually has a financial objective. In other words, criminals choose targets that could provide the greatest possible gain at the lowest possible cost. Criminals may also aim to damage IT systems and data, which may include making services unavailable for use and information retrieval.

The attacks have evolved, with greater cooperation and specialisation between different groups and the establishment of new constellations in connection with such incidents. Services provided by criminal actors include information gathering, selling information about cyber vulnerabilities, phishing campaigns, and expertise in penetrating institutions' cyber protection mechanisms. The use of ransomware is widespread

among criminal organisations but has so far not had major consequences for institutions in the financial sector. Criminal activity related to online fraud has also increased. Criminals can be expected to attempt increasingly sophisticated attacks, which makes ever greater demands on the cyber defences of institutions in the Norwegian financial sector.

Finanstilsynet believes that organised cybercrime will continue to represent a significant threat to Norwegian financial institutions.

### 3.3 FOREIGN STATES AS A THREAT

Foreign states have many resources that can be used for cyberattacks. The NSM believes that threats to the financial sector could originate from Russia, China and others. The NSM regularly publishes updated risk and threat assessments, including of attacks by state actors.<sup>6</sup>

So far, the war in Ukraine has not resulted in any registered increase in adverse cyber activity against Norwegian institutions in the financial sector. Nevertheless, the risk is considered elevated given the duration of the war and a registered increase in security incidents that might be related to the war.

It has been revealed that Ukrainian IT systems were corrupted with malicious code long before the war in Ukraine was started.<sup>7</sup> This underlines the importance of institutions preventing unauthorised access to their systems and the introduction of malicious code even before a conflict or situation arises. The lessons learned from Ukraine should be included in institutions' risk assessments.

### 3.4 CYBERATTACKS AS A POLITICAL TOOL

The threat from extremist religious groups and politically motivated actors, like pro-Russian hackers, is increasing. Attacks by such threat actors can happen quickly. An example is the consequences of the Koran burning in Stockholm, which led to Islamic groups carrying out denial of service (DoS) attacks against Swedish institutions and government agencies in February 2023. If attackers do not announce such attacks in advance or claim responsibility afterwards, identifying those responsible can be challenging.

Political attacks are usually not intended to achieve financial gain but are rather designed to get attention, spread insecurity, social unrest and disinformation, or to demonstrate dissatisfaction with a country or institution. They can also affect institutions in the financial sector, as demonstrated by the DoS attack on BankID and other financial institutions' websites during the summer of 2022. The attack could, for example, have challenged the public's trust in whether the banks' ID solution worked.

The scale of DoS attacks by hackers has increased, but the attacks constitute a limited threat to institutions' operations. Normally, DoS attacks only temporarily affect the availability of web-based services. Such attacks often do not have other consequences for the affected institutions than putting customer self-service solutions and information pages out of operation until the institution has implemented countermeasures. Nevertheless, the attacks can have significant adverse consequences for users if institutions do not remedy the situation quickly. Affected institutions are generally able to continue to perform tasks that do not rely on web-based solutions.

DoS attacks are well-suited as tools for making political statements because criminals easily achieve broad publicity at a low cost. If users experience that they are unable to reach affected services via the usual websites, it can create an impression that the security of an institution's services is vulnerable.

---

<sup>6</sup> Norwegian National Security Authority (NSM) – topic page: [National Cyber Security Centre \(NCSC\)](#)

<sup>7</sup> Digi.no – article 24 February 2022: [Skadevare viser at angrepet på Ukraina har vært forberedt i flere måneder, mener cybersikkerhetsselskap](#) (in Norwegian only)

It is important to note that in addition to effective systems and procedures for detecting and counteracting attacks, institutions should carefully manage information about an attack to prevent the attacker achieving its goal of gaining publicity, and to avoid causing increased uncertainty and unrest.

### 3.5 ATTACKS ON VALUE CHAINS

The exploitation of vulnerabilities in digital value chains by cybercriminals has increased recently. Long and complex supply chains represent a vulnerability that threat actors know to exploit. The threat level for this kind of attack is expected to continue to rise. Value chain attacks can occur when compromised subcontractors that provide components, code or services to service providers that supply institutions in the financial sector, have corrupted code or backdoors introduced into their solutions that attackers subsequently exploit to compromise an institution's solution. Such attacks can have significant consequences for affected institutions.

One example of a value chain attack is the ransomware incident in 2022 which had consequences for at least seven Norwegian financial institutions (including banks, insurers and fund managers) due to the system provider's use of a subcontractor. This resulted in significant disruptions to the institutions' operations, expensive recovery processes for the solutions, and possible damage to the affected institutions' reputation, see section 6.2 for further details. Examples of similar attacks include the exploitation of critical vulnerabilities in Microsoft Exchange Server and Apache Log4j in 2021, which affected major organisations on multiple continents.

Value chain attacks can be difficult to detect for a number of reasons. Digital value chains are often complex, can cross national borders and involve several national authorities. Increasing use of service providers and of components in complex structures makes it challenging to maintain oversight of systems. Recognised best practice involves keeping systems updated to reduce the risk of cyberattacks. It can be challenging for institutions to find a balance between updating their systems as soon as possible with software patches and updates from service providers, and performing adequate testing of software updates and changes before they are deployed in a production environment.

There are a number of countermeasures that can be used against value chain attacks that institutions should consider implementing or ensure that their service providers implement:

- use of micro segmentation<sup>8</sup> and encryption of internal networks to prevent unauthorised access and code spreading
- monitoring network traffic, including internal network traffic, aimed at detecting suspicious data traffic patterns or behaviour
- strengthening control of system deliveries, service providers and service providers' use of subcontractors, including outsourcing that includes general IT dependencies
- use of systems and solutions for automated checks and verification of program code

For the institutions, the value of monitoring network traffic is reduced due to increased outsourcing of system portfolios to cloud service providers. However, outsourcing requires close monitoring of the service provider's ICT security management and subcontractors. Considering the increased threat of value chain attacks, Finanstilsynet expects institutions to use the resources necessary to ensure proper monitoring of their service providers.

---

<sup>8</sup> Micro segmentation is a method, and emerging best practice, for creating zones in data centres and cloud environments with the aim of restricting user access rights. It offers several advantages in relation to more established approaches such as network segmentation and application segmentation.

### 3.6 ATTACKS ON KEY SERVICE PROVIDERS AND DATA CENTRES

A significant proportion of ICT operations in the financial sector are outsourced to a relatively small number of key service providers and data centres, which often also provide important services to other sectors. If a key service provider experiences problems, it can cause ripple effects that impact large parts of the financial infrastructure and other important social functions in Norway. These actors can therefore be attractive targets for an attacker. At the same time, key service providers may have more resources and expertise to develop resilient solutions and the necessary emergency preparedness than institutions would individually. Using service providers can thus also help reduce the risk of cyberattacks resulting in serious incidents in the financial sector.

Institutions should monitor dependencies on key suppliers, such as operations centres, service providers, including outsourcing, and other institutions and organisations with which they cooperate, and assess the vulnerability that would result from successful attacks against them and measures to safeguard critical business functions.

Institutions are also expected to carry out realistic emergency preparedness exercises where the scenario involves the loss of one or more service providers.

### 3.7 CRIMINALS' USE OF ARTIFICIAL INTELLIGENCE

Criminals are expected to start using artificial intelligence (AI) tools like ChatGPT for fraud and other crimes.<sup>9</sup> Europol believes that there is a great potential for criminal exploitation of AI tools such as chatbots<sup>10</sup>.

Criminals can use AI to quickly gather information about new and unfamiliar topics. For example, it can be used to gather information about how to break into systems, create encryption tools, or manipulate people into disclosing information for fraudulent activities by creating convincing, well-written text. The tool can also be used to generate sophisticated emails and text messages, to speed up the production, and to circumvent antivirus solutions and spam filters.

The ability of chatbots to produce text makes them particularly effective in the context of so-called 'phishing'. In some forms of phishing, text messages with illegitimate links entice users to access a fake website where the user is led to disclosing login credentials or other sensitive information, see section 4.6.

The more advanced these types of solutions become, the harder it will be for institutions to protect themselves. Avoiding being tricked into disclosing information will also require greater caution on the part of users of financial services.

### 3.8 NATIONAL MEASURES – TIBER-NO

In autumn 2021, Norges Bank and Finanstilsynet decided to establish a framework for testing the security of critical functions in the Norwegian financial sector.<sup>11</sup> The Norwegian framework, TIBER-NO<sup>12</sup>, is based on the European Central Bank's Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU). The goal is to contribute to financial stability by increasing the resilience to cyberattacks of institutions that perform critical functions for the Norwegian banking and payment system.

---

<sup>9</sup> Europol 27 March 2023: [The criminal use of ChatGPT – a cautionary tale about large language models](#).

<sup>10</sup> A chatbot is a computer program that has been developed to interact with people via written or spoken language.

<sup>11</sup> Finanstilsynet's news item 21 October 2021: [Norges Bank og Finanstilsynet etablerer rammeverk for testing av cybersikkerhet i finansiellsektor \(TIBER-NO\)](#) (in Norwegian only).

<sup>12</sup> Norges Bank's website: [TIBER](#).



The framework provides guidelines on testing financial institutions' capabilities in detecting, protecting against, and responding to sophisticated cyberattacks. The use of threat intelligence and external testing specialists ('Red Team') is designed to help make the testing realistic.

In 2022, Norges Bank staffed a TIBER Cyber Team (TCT-NO), which has formal responsibility for managing TIBER-NO and following up institutions to ensure TIBER-NO testing is carried out.

Norges Bank and Finanstilsynet identified critical functions in the financial infrastructure in 2022 and the entities that are responsible for such functions. In the second quarter of 2022, these entities and other entities that showed particular interest in security testing were invited to take part in tests with the aid of TIBER-NO and the TIBER-NO forum. The first institutions started testing in the fourth quarter of 2022. TIBER-NO will prioritise testing and protection of functions in the financial sector where the consequences of being compromised or failure would be greatest.

### **3.9 Institutions' countermeasures**

Each individual institution is responsible for the cybersecurity of its own systems, including those parts of its operations that are outsourced. This responsibility includes the capacity to counter and detect attacks and having effective plans and solutions for system recovery after attacks.

#### **Safeguards against attacks**

An important safeguard to counter cyberattacks is ensuring that the production systems have been updated with the latest, verified and approved versions and security updates. It is also important to remove components that are not in use and passive and/or outdated systems. There is also a clear correlation between older systems in use and heightened risk of incidents, as well as costs for safeguarding against such incidents. Value chain attacks can be countered by conducting risk assessments and establishing appropriate change management controls. The necessary training and skills enhancement in the area of IT security for the organisation in general and the IT security organisation in particular are also important.

#### **Measures for detecting attacks**

To detect attacks, institutions must have the necessary expertise in-house and consider using external specialist services. Surveillance tools that can detect unwanted activities are also required.

Finanstilsynet recommends institutions not covered by TIBER-NO to consider using TLPT (Threat Led Penetration Testing) and to comply with recognised principles and standards when conducting such tests.

#### **Emergency preparedness**

Financial institutions must ensure that their operations can be restored after cyberattacks and have updated and tested plans for this. In addition to having plans for re-establishing systems and any lost data, they must have plans for managing an incident up to the point where systems and lost data have been restored. Institutions must also have communication plans for various incident scenarios.

Assessments should be made and safeguards implemented to ensure that the institutions' emergency preparedness systems and backup copies of systems and information are protected against cyber attacks.

Institutions should regularly carry out scenario-based emergency preparedness exercises. The lessons learned from these exercises should be reviewed in order to eliminate weaknesses and deficiencies in emergency preparedness plans and procedures.

It is also important that institutions test how quickly their systems can be re-established in different scenarios and assess the consequences any downtime could have for the institution and the institution's customers.

Finanstilsynet encourages the institutions to consider the use of information and experience-sharing services and CERTs<sup>13</sup>. Such services have proven to be useful for strengthening the institutions' capacity to implement proactive safeguards and serve as support in actual attack situations.

### 3.10 COLLABORATION IN THE AREA OF SECURITY

#### **Critical actors in the financial sector**

The Security Act<sup>6</sup> states that economic stability and freedom of action are national security interests.<sup>4</sup> The ministry responsible for a sector must identify and maintain an overview of fundamental national functions (FNFs) and entities that are of vital or material importance for these. For the financial sector, it is the Ministry of Finance that decides whether an institution that is of vital importance for FNFs will be fully or partially subject to the Security Act. The ministry has made decisions in relation to some private actors, but not within Finanstilsynet's area of responsibility. This work has not been completed.

Institutions of vital or material importance for an FNF may be more attractive targets for cybercrime and cyberattacks by foreign intelligence services. Threats from nation-state actors are described in section 3.2.

#### **Collaboration and information sharing result in a better understanding of risk**

The financial industry in the Nordic region collaborates through Nordic Financial CERT<sup>13</sup> (NFCERT)<sup>2</sup>, where the purpose is to strengthen the Nordic financial industry's resilience to cyberattacks. Collaboration and information sharing between financial institutions help improve knowledge about relevant threats and risks, strengthen resilience to cyberattacks, and better equip institutions to react rapidly to cyberthreats and online crime. NFCERT produces and distributes regular threat reports to its members. In Finanstilsynet's experience, institutions that do not take part in this partnership may be poorly equipped to manage cyberthreats and adverse incidents.

Finanstilsynet has been designated as sectoral response environment (SRE) by the Ministry of Finance and tasked with handling ICT security incidents in the part of the financial sector for which Finanstilsynet is responsible. Finanstilsynet performs this role in collaboration with NFCERT.

Finanstilsynet is a partner in the Norwegian Cyber Security Centre (NCSC), which is an arena for national and international collaboration on detection, management, analysis, and advice related to cyber security. NCSC was established to strengthen Norway's digital resilience and emergency preparedness and is part of the Norwegian National Security Authority (NSM). Participation provides Finanstilsynet with access to an up-to-date understanding of the threat landscape in the area of cyber security, as well as an opportunity to interact and share information with other actors when dealing with cyberthreats and cyberattacks.

Finanstilsynet also participates in the NSM's collaboration forum for authorities that supervise ICT security in their sector. The collaboration forum is useful for exchanging information and sharing experiences between supervisory authorities. In 2022, Finanstilsynet presented its inspection module for emergency preparedness and crisis management to the forum.

---

<sup>13</sup> Computer Emergency Response Team

### **Security testing in the financial sector**

Finanstilsynet and Norges Bank established a framework for testing cyber security in the financial sector in 2021 (TIBER-NO). See section 3.8 for further information.

### **European collaboration and information sharing**

In January 2022, the European Systemic Risk Board (ESRB) published a strategy<sup>14</sup> for reducing the risk of financial instability as a result of cyber incidents. For instance, a need to develop macro regulation mechanisms that capture systemic cyber risk has been identified. The ESRB has established a working group (ESCG)<sup>15</sup> tasked with investigating systemic cyber risk and whether and how a cyber incident could cause a systemic crisis. The ESRB also recommends that a European coordination framework be established for systemic cyber incidents (EU-SCICF),<sup>16</sup> cf. the provision on cross-sectoral cooperation in the regulation on digital operational resilience for the financial sector (DORA), see chapter 9. The aim will be to ensure rapid communication and coordination between supervisory authorities and other relevant authorities in order to avoid failures in the event of a serious incident occurring. Pending the establishment of EU-SCICF, ESCG has established a forum for sharing information on cyber incidents.

### **Cyber security roadmap for the financial industry**

To meet growing and more complex cyberthreats, and to better equip institutions to comply with more complex and detailed regulations in the area of ICT, the financial industry, via Finance Norway, has commenced the process of establishing a cyber security roadmap for the industry. The objective is to develop a comprehensive approach in which the industry can agree on a common direction and to facilitate the establishment of arenas for strategic discussions about cyber security within the industry and/or with other sectors (for example based on the DSOP<sup>5</sup> model).

---

<sup>14</sup> European Systemic Risk Board (ESRB) 27 January 2022: [ESRB recommends establishing a systemic cyber incident coordination framework](#)

<sup>15</sup> European Systemic Cyber Group (ESCG)

<sup>16</sup> Pan-European systemic cyber incident coordination framework (EU-SCICF)

# 4. FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS

## 4.1 INSPECTIONS OF ICT AND PAYMENT SERVICES

### Information from completed inspections

Finanstilsynet conducted 22 on-site inspections focusing on ICT and payment services in 2022. Of the 22 inspections, nine were conducted at banks, two at payment institutions, two at insurers, one at an infrastructure provider, three at investment firms, one at a debt collection agency, one at a real estate agency, and two at audit firms. Three of the inspections at banks were thematic AML inspections where the bank's systems for electronic monitoring of suspicious transactions was the main theme. Some of the findings from the inspections in 2022 correspond with findings from inspections in 2021.

More details of the conducted inspections of ICT and payment services can be found on Finanstilsynet's website.<sup>17</sup>

### Outsourcing

Several insufficiencies related to the outsourcing of ICT operations were pointed out during inspections in 2022. For example, at a number of inspections, Finanstilsynet discovered that institutions had not complied with the requirement in the Notification Obligation Regulations to maintain an overview of all of their outsourcing agreements.

Finanstilsynet also found instances of non-compliance with the ICT Regulations, section 2(4), which states that outsourcing agreements for ICT operations and amendments to such agreements must be considered by the institution's board. The inspections in 2022 also revealed that there are still outsourcing agreements that do not meet the requirements of the ICT Regulations, section 12. This requires that such an agreement must ensure that institutions under supervision are given the right to control and audit all services carried out by the service provider under the agreement. They must also ensure that Finanstilsynet has access to information from ICT service providers and has a right to inspect the service provider where Finanstilsynet deems this to be necessary as part of its supervision of the institution.

### Inadequate monitoring of service providers

During its inspections in 2022, Finanstilsynet found insufficiencies in the institutions' monitoring of outsourced ICT services, especially in the monitoring of service providers' compliance with the institutions' security requirements. One incident identified in 2021, where a service provider's employees misused their access rights to search customer data for non-work purposes, was followed up (see section 4.2).

Finanstilsynet found inadequate procedures for access management and logging at the service provider, which makes it difficult to detect any misuse of access rights for non-work-related searches. In its inspection reports, Finanstilsynet underlined the institutions' responsibility for the governance of access rights, including when services are outsourced.

Finanstilsynet also highlighted the individual bank's responsibility for monitoring purchases and the use of joint services from a service provider. Additionally, Finanstilsynet pointed out that the ICT Regulations' provisions apply irrespective of whether the outsourcing is intragroup or external.

### Inadequate involvement in the service provider's testing of crisis management solutions

At several of the inspections, Finanstilsynet pointed out that the institutions' involvement in planning the testing of crisis management solutions at service providers was inadequate. Without the institution's

---

<sup>17</sup> Finanstilsynet: [Tilsynsrapporter for IT og betalingstjenester](#)

involvement, one cannot ensure that processes and systems that the institution has categorised as business critical are included in the tests at the service providers.

### **Inadequate ICT expertise and expert ICT resources in the second line of defence**

At several inspections in 2022, Finanstilsynet found reason to point out the importance of the institution having sufficient ICT expertise and expert ICT resources in independent control functions in the second line. The second line must conduct autonomous and independent assessments, in addition to conducting checks of ICT operations.

### **Three lines of defence**

**First line of defence** (operational management): The first line of defence is conducted by the operational management as owner, and manages identified risks and is responsible for implementing corrective measures. The operational management must also establish effective, appropriate processes and controls to ensure that risk is identified, analysed, monitored and managed. The first line of defence must also report risk, ensure that risk is contained within the limits accepted by the institution and ensure that ICT activities are in compliance with external and internal requirements.

**Second line of defence** (risk management and compliance): The second line of defence consists of risk management and compliance functions that oversee and follow up the operational management's governance. The responsibility of the risk management function is to facilitate the implementation of the institution's risk management framework. The risk management function is also responsible for assisting the first line in implementing risk management and ensuring that processes and controls established in the first line are effective and correctly designed. The function is also responsible for identifying, overseeing, analysing and reporting risks indicated by first-line risk reporting and using these to provide a comprehensive picture of the institution's risk situation. The responsibility of the compliance function is to oversee compliance with legal and regulatory requirements and the institution's internal requirements. It is also responsible for advising the executive management and other stakeholders on compliance with these requirements, for establishing guidelines and processes for managing compliance risk and for ensuring compliance. The second line of defence may also consist of other non-operational functions, for example within data security.

**Third line of defence** (internal audit) An institution's third line of defence consists of an independent internal audit unit which conducts risk-based and general audits and reviews of the institution's governance. The internal audit is also responsible for independent review of the first two lines of defence. An independent internal audit unit is an important instrument for the institution's board in the work of assessing and obtaining confirmation of compliance with governance frameworks and laws and regulations and identifying situations that imply high risk.

### **Missing or inadequate business impact assessments**

The inspections in 2022 identified that business impact analyses (BIAs) are still missing or are inadequate in many institutions. BIAs are an important basis for the institution's work on emergency preparedness and crisis management plans, including for outsourced services.

### **Data quality**

At a number of inspections, Finanstilsynet pointed out that a data governance framework may be required to ensure the quality of the data. This also applies to large institutions/groups with cross-disciplinary business processes and complex value chains. Data governance must ensure the consistency and reliability of data and prevent misuse and is a prerequisite for automating and streamlining business processes.

Finanstilsynet also found inadequate classification of information and inadequate assessments of the risk of data loss. The classification of information and assessments of the consequences of data loss provide the basis for setting access and protection requirements for data and should be included in BIAs.

### **Inspections of monitoring systems**

At the inspections of the banks' systems for monitoring suspicious transactions relating to money laundering and terrorist financing (AML/CTF), Finanstilsynet found cases where the transaction monitoring system did not perform checks against the information collected about the customer (KYC data<sup>18</sup>) or against the relevant sector or products. In many cases, there were few rules<sup>19</sup> aimed at high-risk customers, few customer-specific rules, and few rules aimed at terrorist financing. At several inspections, Finanstilsynet pointed out that the lack of references to the rules in AML risk analyses makes it impossible to assess the extent to which the transaction monitoring covers the institution's money laundering and terrorist financing risks. The inspections also showed that institutions that had made major changes to their rules based on thorough risk analyses saw significant improvements in the form of greater accuracy and more true positive alarms.

### **Inspections of payment institutions**

Finanstilsynet pointed out inadequate procedures for managing security-related customer complaints in relation to the obligations that follow from the Financial Institutions Regulations, section 3-2(a). Finanstilsynet also pointed out that user (customer) contact information was missing, meaning that it was hard for the institution to fulfil the requirement in the Regulations on Payment Services Systems that users must be informed of incidents that could have an impact on their financial interests. It was also pointed out that users' options for contacting the institution efficiently were limited if they needed to instruct the institution to stop access to specific accounts or to change the accounts to which the institution should have access.

To ensure secure communication throughout the payment service process and prevent the forwarding of account requests that breach the rules of the PSD2 Regulatory Technical Standard,<sup>20</sup> Finanstilsynet pointed out that communication between the institution and its customers should be secured using eIDAS certificates<sup>21</sup> or their equivalent.

## **4.2 VENDOR MANAGEMENT OF ACCESS MANAGEMENT**

In 2022, Finanstilsynet followed up a security incident from 2021 in which a service provider's employees had misused access rights for non-work-related searches. The follow-up covered all institutions that use this service provider. In addition, inspections at selected institutions were conducted, as discussed in section 4.1. Finanstilsynet focused on the institutions' procedures for following up ICT service providers in relation to the administration, monitoring, and oversight of access rights, including which internal control activities and audits have been conducted at the instruction of the institution, cf. the ICT Regulations, sections 12 and 5.

The security incident in 2021 and follow-up of the institutions' access management show that better procedures for detecting the misuse of access rights for non-work-related searches are needed.

Furthermore, Finanstilsynet observed insufficiencies in the institutions' governance of access rights for outsourced solutions. Institutions, together with ICT service providers, are expected to implement measures

---

<sup>18</sup> Know Your Customer (KYC)

<sup>19</sup> Electronic transaction and/or customer controls may be referred to as rules, filters, controls, risk parameters, or scenarios. The term 'rules' is used here.

<sup>20</sup> Regulatory Technical Standard (RTS)

<sup>21</sup> eIDAS (electronic IDentification, Authentication and trust Services) certificates are certificates for businesses that can be used throughout Europe in line with the eIDAS Regulations. PSD2 requires the use of qualified electronic seal certificates (eIDAS certificates) in communication between payment service providers and account servicing payment service providers, cf. Commission Delegated Regulation (EU) 2018/389 (RTS), Article 34.

that ensure that these are adequate, and that the institution establishes access management solutions and controls that ensure that access rights are, wherever possible, assigned for the individual assignment based on work-related needs.

### 4.3 THE INSTITUTIONS' ASSESSMENT OF IMPORTANT FACTORS RELATED TO ICT OPERATIONS

In their dialogue with Finanstilsynet, the institutions and ICT service providers highlighted a number of important factors concerning ICT operations.

#### **The board's responsibility for ICT operations**

Boards are responsible for ensuring that ICT operations comply with laws and regulations, and with enterprises' ethical guidelines. This also applies to outsourced ICT operations, where the board must ensure that agreements and contracts are in line with the enterprise's information security policy and ensure compliance with acts and regulations. It is also important that the board has an overview of which ICT services have been outsourced and that procedures are in place to ensure that outsourced ICT operations are managed in a proper and secure manner.

#### **Management model and internal control**

In the dialogue with the institutions, Finanstilsynet learned that an inadequate overview of which controls are included in the institution's internal control and how the controls should be performed, monitored, and audited may result in operational risks not being identified. This can in turn result in the necessary risk-mitigating measures in line with the institution's risk tolerance not being implemented.

Like the year before, the institutions pointed out that an institution's size is of relevance with respect to their capacity to establish an organisation with a clear division of the first and second line's internal control tasks.

#### **Skills and skills management**

Shortages of resources in Norway within operations, architecture, security, and new technology, as well as inadequate skills management, could lead to institutions being unable to meet current and future competency needs. This applies to both established and new technology, especially within cloud technology. This could result in issues that are challenging to resolve and increased dependency on access to foreign expertise.

#### **Vendor management**

Managing complex supply chains is steadily becoming more challenging. With more service providers and subcontractors in the value chain, the interaction models have become more complex and extensive at a strategic, tactical and operational level. Insufficiencies in this area can result in poorer monitoring and oversight of critical outsourced ICT services.

Good vendor management within a clearly defined framework, with clear descriptions of the information the institution wants from the service provider, is crucial.

#### **Cybercrime**

In the dialogue with the institutions, it was pointed out that inadequate security testing, security updates, training and awareness among employees, and insufficient monitoring of operations in their own technical infrastructure, including networks and systems, may result in criminals inflicting damage on an institution through cyberattacks. Defrauding bank customers is the new form of robbing banks and the institutions regard this as a social problem.

### **Information leaks**

Inadequate information classification and controls for monitoring information sent by email, copied to external storage devices, or copied to private cloud services can result in unauthorised persons gaining access to information and can cause harm to the institution or its customers.

### **Classification**

It is important that institutions have classified their documents with respect to confidentiality and criticality, so that they can establish solutions that help prevent unauthorised data access or sharing.

### **ICT operations**

Secure and stable ICT operations are a high priority for all institutions. However, secure and stable ICT operations are being challenged by steadily increasing complexity due to integration between systems from different service providers, integration between old and new systems, increased functionality in self-service channels, greater use of cloud services, inadequate management of technical debt, and insufficient monitoring of the IT environment.

### **Emergency preparedness and crisis management**

Inadequate analyses of the consequences of a crisis, inadequate training and exercises in crisis management, shortcomings in testing of crisis management plans, and inadequate crisis management plans can present challenges for institutions when it comes to maintaining critical ICT services in the event of severe disruptions at operating locations. Monitoring emergency preparedness solutions is challenging, especially where institutions create and communicate the framework for testing service providers' emergency preparedness solutions.

### **Emergency preparedness – emergency preparedness tests based on scenarios and BIAs**

A BIA\* is designed to analyse the effect an incident would have on an institution's business processes and services. These analyses are based on processes and services that are critical for an institution's activities. The analysis also includes mapping and classifying the activities and resources needed to deliver critical processes and services. BIAs also provide a basis for an institution's emergency preparedness and crisis management plans. Institutions must ensure that testing and exercises are based on the institutions' BIA in order to ensure that critical business processes and services can be safeguarded in the event of an incident. This also includes outsourced operations. Finanstilsynet underscores the importance of institutions including scenarios that also incorporate deliberate cyberattacks when planning their exercises and testing activities. The institutions' emergency preparedness work should be based on business-critical services, vulnerabilities, and the current threat landscape, including arrangements where ICT operations are outsourced.

\*Business Impact Analysis

### **Geopolitical factors**

Contact with the institutions revealed that country risk and other geopolitical factors are regarded as being at the same level as in previous years, and that there have been no changes in these factors that would entail a greater security threat to the Norwegian financial industry.



### **Change management**

The rapid pace of development can result in pressure to put a solution into production, possibly at the expense of quality. This can result in functional errors and security vulnerabilities not being identified. Inadequate control of changes in operating configurations may result in interruptions to critical business processes and to institutions being exposed to cybercrime. The institutions are aware that continuous deployment is a change management strategy that presents challenges, but that using the DevSecOps<sup>22</sup> process can help ensure that this strategy does not create new risks for the institution.

### **Access management**

Inadequate control and monitoring of extended access rights for employees and service providers' personnel can result in an institution being harmed by intentional or unintentional operational incidents. This can also lead to information leaks. Institutions consider it important that service providers' access management systems are integrated with their own access management systems so that they have a better overview of the service providers' access rights.

### **Data quality**

Inadequacies or errors in data may result in analyses, controls, and decisions being based on incorrect or insufficient information. This includes errors in credit ratings, errors in controls aimed at detecting money laundering or fraud, and errors in risk assessments. Within data governance, institutions are increasingly carrying out activities to improve their monitoring of data quality. In its dialogue with the institutions, Finanstilsynet pointed out that it is important that institutions' service providers understand the importance of good data quality.

## **4.4 SUMMARY OF THE INSTITUTIONS' RISK AND VULNERABILITY REPORTING**

Finanstilsynet has collected risk and vulnerability assessments of ICT operations from payment service providers and other institutions, cf. the Regulations on Payment Services Systems, section 2(3) and the ICT Regulations, section 3. For further details, please see appendix 1.

### **Governance**

Based on the reported material in 2022, it is evident that most institutions rate the risk associated with governance as low. More than three of four institutions report that they believe the ICT systems provide a good basis for governance of operations, that they have well integrated processes for risk analysis, and that they have documented goals and procedures for ICT security approved by the executive management team. The vast majority report that they comply with the principle of three lines of defence. However, several institutions report that the risk is moderate or high when it comes to an overview of which controls the institution utilises within the three lines of defence, broken down on controls that help ensure integrity, confidentiality and availability, respectively. It appears from the institutions' comments that the degree to which they have complete and uniform documentation of controls varies within the individual areas of responsibility and lines of defence.

About three of four institutions report a low risk related to ongoing monitoring of service providers and deliveries with respect to delivery quality. While the majority of institutions also report that the risk associated with procurement competence is low, the reports show that several institutions regard this as one of their greatest risks. Some institutions also highlight their reliance on external ICT expertise.

---

<sup>22</sup> DevSecOps stands for development, security, and operations. This is an approach to culture, automation and platform design that ensures that security is a joint responsibility throughout the ICT lifecycle.

One of three institutions believe that the risk associated with a lack of, or inadequate, guidelines for ICT security, including risk assessments of payment services, security controls, and measures for protecting users against identified risks, is moderate or high. The risk is considered to be increasing. A solid majority of the institutions believe that the risk associated with adequately training and raising the awareness of employees is low.

- *Finanstilsynet notes that institutions generally report the risk associated with governance of ICT activities as being low. Finanstilsynet's experience from its supervisory activities gives a somewhat more varied picture of the institutions' risk in this area. Inspections have revealed deficiencies in the governance of ICT operations, particularly at small and medium-sized institutions, which results in vulnerabilities and increases the risk of incidents.*

### **Data protection**

A substantial majority of the institutions report that the risk of unauthorised changes being made and of the services no longer functioning properly is low. When new solutions are developed, institutions report that they consider the needs of all business areas. The institutions report that the risk associated with protecting data during both transfer and storage is low.

The institutions collect information on operations, transactions and fraud, and use this information to make the services more secure. The scale and consequences of errors in applications and data that impact data integrity were lower in 2022 than in 2021.

### **Change management**

The institutions' overall assessment of the risk associated with change management was stable. The risk associated with test systems not being equivalent to production systems is falling. However, more than half of the institutions consider the risk to be moderate or high. A high degree of complexity in ICT systems is associated with high or moderate risk in about four of five institutions. As far as the complexity of ICT systems is concerned, institutions point to value chains as one of the causes of the high risk. If a system linked to one service is changed, this can also affect systems for other services. This is also one of the issues with change management. Most of the institutions assessed the risk as high, but stable.

Several institutions regarded new regulatory requirements as one of the highest risks. The risk associated with institutions constantly having to modify systems as a result of new regulatory requirements is increasing. In this context, reference is made in particular to the new Financial Contracts Act, PSD2, and DORA (see chapter 9). The institutions' comments show that the pace of change is rapid and accelerating. Furthermore, changes can be challenging for small institutions. While some institutions pointed out that changes are announced early, which means that the changes can be planned and checked, others said that the implementation period is short. The institutions emphasise that substantial resources are allocated to deal with new requirements.

The institutions also focus on good procedures, expertise and resources, and on mitigating key person risk.

### **Operations**

The risk associated with operations is generally stable. Around half of the institutions report that this risk is moderate or high. The institutions' assessment of risk due to technical debt has decreased, even though a majority of the institutions still consider the risk to be moderate or high. The risk of interfaces used by third

parties not being compliant with the security requirements of Commission Delegated Regulation (EU) 2018/389<sup>23</sup> is reported to be low, although it is trending upwards.

Well over half of the institutions consider the risk linked to maintaining an up-to-date overview of ICT outsourcing, and associated risks, to be moderate or high. The institutions point out that they track and follow up agreements, and that checks are conducted. In some cases, it appears that the monitoring and review requires improvement.

Replacing banks' core solutions is highlighted as one measure that allows a better overview of the business processes that are affected by outages or irregularities in operations. It was also pointed out that in some cases PSD2 interfaces are tested by service providers.

## Security

A majority of the institutions regard ICT security as the highest risk. The level is reported to be generally stable. Heightened geopolitical tensions are highlighted as a reason for the increased risk of cyberattacks. The institutions point to value chains as one risk factor when ensuring ICT security. The shortage of ICT resources was also emphasised by many as one of the highest risks. As far as access to ICT security expertise is concerned, including the setting of requirements related to outsourcing, around two of three institutions regard the risk as high or moderate and on an upward trend.

- *In the opinion of Finanstilsynet, inadequate access to ICT resources, combined with an elevated threat of attacks, represents a material risk.*

Just under half of the institutions assessed the risk of measures designed to protect against attacks not being sufficient as moderate or high. The institutions largely point to measures such as the procurement of security products, the introduction of antivirus utilities, firewalls for home PCs, and the use of sandboxes to analyse files.

The institutions regularly utilise security testing, including penetration testing. Just under half of the institutions consider the risk associated with testing to be moderate or high. Some institutions also point out that weekly vulnerability scans have been introduced. Several of the institutions also report that they use external service providers in connection with security testing.

## Data protection

A substantial majority of the institutions believe that the risk associated with protecting both structured and unstructured data is low, as is the risk associated with having good guidelines for classifying data. The risk related to granting and maintaining the access rights of employees, suppliers, consultants, and applications in the systems is also regarded as low. However, a large proportion of the institutions regard the risk associated with logging access rights to data and systems as moderate or high. While several institutions report that they have access to logging systems and analyses, many institutions report that the logging of access rights and alarms is performed by external service providers or other institutions in alliances. Some institutions report that logging and reporting suspicious behaviour will be a priority area for 2023.

## ID theft

Compared with 2021, the institutions regard the risk associated with ID theft to be somewhat higher. Several institutions believe that the risk associated with having inadequate measures for preventing an attacker from taking over and misusing a customer's ID is rising. Unlike in 2021, institutions now regard the

---

<sup>23</sup> [Commission Delegated Regulation \(EU\) 2018/389](#)

risk of not having adequate measures to prevent an attacker taking over and misusing a customer's ID as high. Meanwhile, the overall risk remains stable and unchanged. Several institutions pointed to the risk of ID theft as one of the highest risks. The institutions pointed out that attempted ID theft is increasing, as are the consequences of the thefts for those who are affected, including both institutions and customers. See the separate discussion on stricter requirements for institutions below.

Otherwise, the institutions are focused on controls, following up cases of fraud, providing customers with information, and using strong customer authentication.

### **Stricter requirements for institutions**

In a ruling dated 13 September 2022, the Norwegian Supreme Court established that the bank was liable for a loss after a customer was tricked into disclosing their BankID code and password over the telephone, whereafter money was withdrawn from the customer's bank account. According to the agreement with the bank, the customer had an obligation not to disclose their code and password. This also applied with respect to the bank. However, the Supreme Court found that if the customer was to be liable for the loss, cf. the Financial Contracts Act (1999), section 35\*\*, the customer had to be aware of the breach of the obligation, which in this case the customer was not.

The Supreme Court ruling tightens the rules surrounding banks' liability, which appears to have triggered the institutions to focus more on this. This may explain why the institutions regard the risk as higher than before. The new Financial Contracts Act entered into force on 1 January 2022, and corresponding provisions have been retained in the new Act.

### **Internal irregularities**

Approximately half of the institutions rate the risk associated with control over internal irregularities and irregularity scenarios as moderate. The feedback indicates that the institutions focused on these threats in 2022 as well. The risk associated with inadequate logging and reporting is also considered to be moderate by half of the institutions, although the proportion that considers the risk to be high has increased somewhat.

### **Money laundering and terrorist financing**

Money laundering and terrorist financing is an area that institutions generally rate as representing a moderate or high risk. A clear minority of the institutions regard the risk as low, while several institutions consider the risk of money laundering and terrorist financing to be one of the greatest risks.

A substantial majority of the institutions consider the risk associated with ICT systems not providing an overall picture of the customer, customer relationships, and customer behaviour to be moderate. The feedback indicates that the institutions were focused on 'Know Your Customer' (KYC) tasks in 2022, and several report that they had put in place, or were putting in place, better ICT solutions for relevant customer information.

Several institutions still regard the risk associated with disclosing suspicious transactions without sufficient precision as moderate or high. It was pointed out that in many cases a large number of the disclosures are false positives. A majority of the institutions believe that the risk associated with the systems for monitoring transactions not capturing all payment transactions is moderate to high, which should be investigated further. The institutions point out that they pay a lot of attention to this area, that the systems are being

developed further and improved, and that external systems are procured. It was reported that ongoing work and development in this area will be continued in the future.

A substantial majority of the institutions believe that the risk associated with the AML systems' recognition of suspicious patterns over time is moderate or high. Several institutions report that they have adopted and developed machine learning and scenarios that use customers' earlier behaviour compared with statistical data to recognise suspicious patterns.

The risk associated with the sanctions screening system accurately identifying listed people and enterprises is assessed to be moderate or high by a substantial majority of the institutions. Several institutions highlight the uncertain geopolitical situation and say that keeping the AML systems updated in relation to sanctions rules and changes to lists of names has been a challenge. The institutions report that sanctions screening ICT systems have been improved and their accuracy enhanced, partly as a result of Finanstilsynet's inspection in 2022.

### **Other observations**

Finanstilsynet has noted that the responses of many institutions in alliances are very similar. The risks and vulnerabilities that are highlighted can be highly relevant for many institutions of similar size with similar business models and limited complexity. However, every institution has an obligation to conduct an independent assessment of the institution's risk and vulnerability. Documentation of the institution's own assessment was missing in several reports.

Some subsidiaries of financial institutions have not documented that they have conducted an assessment of their risk and vulnerability and simply refer to the parent company's report.

Finanstilsynet would like to remind the institutions subject to the ICT Regulations or equivalent Regulations that they are required to conduct risk analyses to ensure that their risk is managed within acceptable limits relative to the institution's business, cf. the requirements of the ICT Regulations, section 3.

## **4.5 STRENGTHENED CONSUMER PROTECTIONS IN THE NEW FINANCIAL CONTRACTS ACT**

The new Financial Contracts Act<sup>24</sup> entered into force on 1 January 2022. The Act strengthens consumer protection and makes banks more liable for any misuse of BankID.

Pursuant to section 2-7(1) of the Act, consumers are entitled to claim reimbursement of the amount if they are defrauded when they pay with a credit card. The Act also applies to defective goods, incorrect amounts, or orders that never arrive. The use of debit cards is not regulated by law in the same way, although the contract terms and conditions for Visa and Mastercard debit cards can contain provisions on claims and compensation.

Pursuant to the Financial Contracts Act, banks must ensure that consumers have access to clear, rapid, secure and easy to use procedures for changing payment accounts, cf. section 4-34 and discussion on changing banks in section 2.3. The process for moving standing orders and the banks' obligations in relation

---

<sup>24</sup> [Financial Contracts Act](#)

to this are regulated by sections 4-37 and 4-38. This includes moving standing orders and direct debit authorisations like AvtaleGiro.

## 4.6 MISUSE OF LOGIN CREDENTIALS

Finanstilsynet has noted an increase in activities where criminals attempt to gain access to users' login credentials (one-time codes, passwords, etc.), so-called 'phishing'. The login credentials are used to log in, thus providing the criminal with the same rights as the victim when logged into a site and allowing them to exploit the rights for their own gain. It is likely that nearly all users experienced a phishing attempt in 2022 and very many experienced being targeted by attempts several times. Several of the victims were robbed, see chapter 5 on fraud and fraud statistics.

### **Misuse of employee login credentials**

Finanstilsynet is aware of cases where employees in the financial industry have had login credentials stolen, where the attacker has acquired all the rights of the employee and used these to send emails with false payment requests in the employee's name. Finanstilsynet is not aware of any cases where attackers have succeeded in acquiring funds.

In such attacks, after successfully logging in, the attacker receives an electronic access certificate, a so-called 'session object'. The access certificate is valid for a period of time set by the website that issues the certificate. The validity period is often so long that the attacker has good time to carry out attempted fraud, for example using fake emails.

The connection between the user and the website is usually encrypted and thus protected against this form of ID theft. The user can check the website's name and that the connection is encrypted before entering their login credentials. Many people are probably not aware that they can carry out these checks. Because users have not really been taught to check what a certificate says, they will not discover that the attacker has established an encrypted connection to their own website.

An institution is able to specify the workstations that will have access. This makes it harder for an attacker to carry out phishing attempts. However, a workstation's IP address can be falsified and, therefore, this is not a reliable means of identifying a workstation. Using a workstation's physical address, its so-called MAC address, can provide better security.<sup>25</sup>

Finanstilsynet is aware that cloud service providers offer additional services that ensure protection against attacks. These are offered as separate additional services. Finanstilsynet has reason to believe that not all cloud service users are aware of the consequences of choosing not to use such additional services.

### **Theft and misuse of login credentials for financial services**

In addition to being the key ID in the financial sector, BankID is used in a number of other places in both the private sector and the public sector. The BankID login page that users see differs in appearance from one website to the next. Users often have no basis for determining whether a website is entitled to ask the user to log in using BankID or to ask the user to disclose login credentials for this purpose. This puts users in a difficult position given that, based on the contract with the bank, the user has promised to keep their login credentials secret. There is a risk that an attacker is behind the website and phishes for users' login credentials.

---

<sup>25</sup>MAC addresses are normally not part of the digital information sent. The institution responsible for the website must in this case programme its application to include the MAC address or any other information suitable for identifying the workstation.

When logging in to frequently used financial services, such as online banking, institutions use other checks in addition to BankID to authenticate users. Such checks can involve the user's input biometrics, checking that the user's workstation (mobile phone, PC or tablet) has been updated with the latest version of the operating system and security updates, that the user's geolocation matches expectations, and that the transaction is consistent with the user's normal behaviour (for example, 'Jane Smith does not usually send larger sums abroad at two o'clock in the morning'). Where BankID is seldom used for logging in, for example to Altinn, Helse-Norge, and the land register, it can be harder to perform additional checks based on behaviour. Therefore, when a stolen ID is used these websites may be more vulnerable than services provided by an issuer of BankID.

The large-scale use of BankID for both private and public services outside the financial sector, with variations in the login context, entails a risk of users not being sufficiently vigilant and being tricked into logging into a fake website and disclosing security credentials. The wide range of uses affords criminals opportunities to exploit a broad range of methods in their fraud activities and may contribute to more fraud.

### **Measures against theft and misuse of login credentials**

Finanstilsynet believes that efforts should be intensified in a number of areas in order to reduce the scale of ID theft, including:

- assessing measures in relation to the service's potential to cause harm
- teaching users about the checks a user can/should carry out
- raising the awareness of users and merchants' technical personnel
- considering possible measures and additional checks such as limiting the validity period of session objects, limiting sender addresses to a particular geographical area, defining the computers that can be used, checking the security of the sender's hardware (operating system level, level of security updates, etc.), conducting checks against the user's normal behavioural pattern (amounts, user frequency, etc.) and requiring that more people must approve transactions.

## **4.7 RISKS ASSOCIATED WITH USING CHATBOTS**

AI chatbots<sup>10</sup>, like OpenAI's ChatGPT, represent a technology that is in the process of being integrated into ordinary work tools. Major actors such as Google and Microsoft are investing heavily in developing and integrating AI-based functionality into browsers and Office products. Chatbots like ChatGPT are advanced text generation models that, as well as writing text, can be used to answer questions and perform tasks, and to translate text from one language to another. ChatGPT can also be used for systems programming since it is designed to understand, debug, and suggest code.

The use of digital tools such as ChatGPT can provide major gains for institutions since they are user-friendly, available around the clock, can answer a wide range of questions, and are cost-effective. However, the use of chatbots is not without challenges or risks. The system can collect and store information that is sensitive or personal, and this may make complying with the General Data Protection Regulation (GDPR) challenging. Chatbots are language models, not knowledge models, and there is a risk of chatbots providing incorrect information or misunderstanding user questions. They can provide incorrect representations of the information they find, or present answers that look plausible but that are in fact incomplete, inaccurate, or inappropriate.

Chatbots are trained using large data sets. The answers they provide are influenced by the sources of the data set and whether the information used is continuously updated or the information is not updated after a certain date. If the data sets used to train the models are not diversified and representative, the risk of bias and unwanted results increases. Machine-based models such as chatbots also have no awareness of moral aspects or ethics.

Like any other ICT tool, the use of chatbots should be based on risk assessments and take place in a responsible and conscious manner. Users should be aware of the chatbots' limitations and the risk associated with using them.



## 5. FRAUD AND FRAUD STATISTICS

### 5.1 REPORTING OF FRAUD STATISTICS

According to section 2 of the Regulations on Payment Service Systems, banks, financial institutions, e-money institutions, payment institutions and branches of such institutions headquartered in another EEA state must report fraud statistics to Finanstilsynet at least once a year. Finanstilsynet has decided that the institutions' reporting on fraud should take place semi-annually, which is in line with the guidelines for fraud reporting in the revised Payment Services Directive (PSD2).<sup>26</sup>

Both the amount defrauded and the number of fraudulent transactions are reported, as well as the total transaction amount and the total number of transactions in the period. The reporting distinguishes between domestic transactions, cross-border transactions in the EEA, and cross-border transactions outside the EEA. Furthermore, fraudulent transactions are classified into three categories based on whether the fraudster issues the payment order, changes/modifies the payment order or manipulates the payer into initiating the payment order.

Table 5.1 shows losses linked to account transfers and card payments with cards issued by Norwegian card issuers, as well as total losses per year. The figures show an increase in total losses of NOK 106 million from 2021 to 2022.

Table 5.1 Total losses from fraud

Amounts in NOK million	Fraudulent transactions - account transfers (online banking etc.)	Fraudulent transactions with payment cards reported by card issuers	Total losses
H1 2022	162	98	
H2 2022	233	121	
<b>Total 2022</b>	<b>395</b>	<b>219</b>	<b>614</b>
H1 2021	188	79	
H2 2021	159	83	
<b>Total 2021</b>	<b>346</b>	<b>162</b>	<b>508</b>
H1 2020	225	73	
H2 2020	130	75	
<b>Total 2020</b>	<b>355</b>	<b>148</b>	<b>503</b>

Source: Finanstilsynet

### 5.2 LOSSES ASSOCIATED WITH THE FRAUDULENT USE OF PAYMENT CARDS

Payment card fraud is primarily fraud in which the fraudster issues the payment order. The largest subcategory is theft of card details.

Issuing banks reported that losses due to fraudulent card payments amounted to NOK 215.8 million in 2022. Losses increased by 18 per cent from the first to the second half of the year, representing NOK 96.8 million and NOK 119 million, respectively. In addition to this come losses of NOK 3.4 million through the misuse of payment cards to withdraw cash, which split between the first and second half of the year at NOK

<sup>26</sup> Article 96 no. 6 in [PSD2](#) (EUR-Lex) and [Guidelines on fraud reporting under PSD2 \(EBA\)](#). See also [Regulations on Payment Services Systems](#), section 2, fourth subsection.

1.5 million and NOK 1.9 million, respectively. Overall, total losses through the misuse of payment cards amounted to NOK 219.2 million. This represents a 35 per cent increase from 2021.

Table 5.2 shows total losses from fraudulent payments using payment cards owned by Norwegian customers over the past three years, irrespective of whether the loss was covered by the customer, the bank or the payment card company. Total losses came to 0.021 per cent of total transaction value, up from 0.016 per cent in 2021.

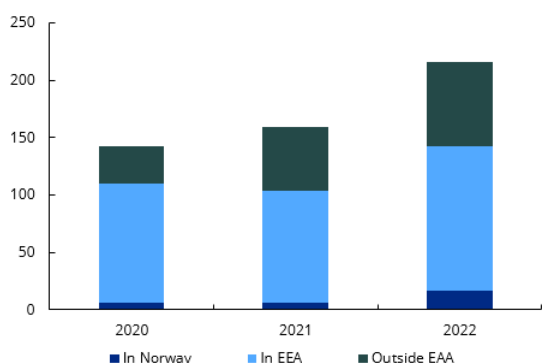
**Table 5.2 Losses from fraudulent use of payment cards (both payments and cash withdrawals)**

Type of payment card fraud (amounts in NOK million)		2020	2021	2022
Total	Total transaction amount	953 960	985 699	1 061 408
	- Of which fraud	147.6	162.0	219.2
	Fraud in per cent	0.015	0.016	0.021
Cash withdrawal fraud	Total transaction amount	47 204	36 664	41 828
	- Of which fraud	4.6	2.8	3.4
	Fraud in per cent	0.010	0.008	0.008
Fraudulent card transactions initiated electronically and non-electronically	Total transaction amount	906 756	949 036	1 019 580
	- Of which fraud	143.0	159.2	215.8
	Fraud in per cent	0.016	0.017	0.021

Source: Finanstilsynet

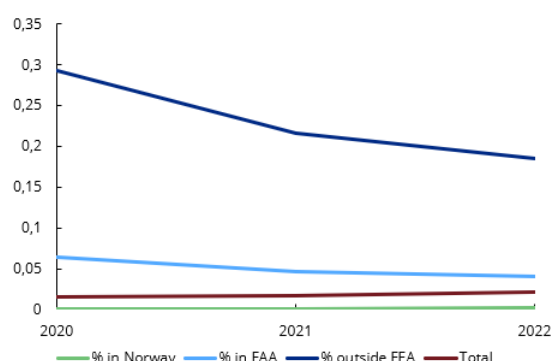
Although there was a rise in losses due to fraudulent card payments of approximately 35 per cent from 2021 to 2022, the increase in per cent of the total transaction amount was slightly lower at 31 per cent.

**Figure 5.1 Losses related to card payments by geography in NOK million**



Source: Finanstilsynet

**Figure 5.2 Losses in per cent of total card payments by geography**



Source: Finanstilsynet

Table 5.3 shows losses broken down on transactions in Norway, cross-border transactions in the EEA and cross-border transactions outside the EEA, as well as the proportions initiated non-electronically and electronically respectively. The figures are exclusive of cash withdrawal fraud. The proportion of fraud was

highest for cross-border transactions outside the EEA. In this category, fraud accounted for 0.17 per cent of transaction value, down from 0.22 per cent in 2021.

Losses from card payments that were initiated non-electronically accounted for NOK 13.6 million of the total losses of NOK 215.8 million in 2022. These are card transactions where the payment card details have been communicated by the purchaser to the seller over the telephone or via email.

**Table 5.3 Transaction value and fraudulent transactions with payment cards reported by card issuers\*.**

**Figures for 2022**

Transaction value (amounts in NOK million)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total transactions
Card payments (issuer)				
Total	677 462	302 253	39 866	1 019 580
- Of which fraud	16.9	124.6	74.3	215.8
Fraud in per cent	0.002	0.041	0.186	0.021
Of which initiated non-electronically:				
Total	5 053	6 803	3 439	15 295
- Of which fraud	0.3	5.8	7.6	13.6
Fraud in per cent	0.005	0.085	0.220	0.089
Of which initiated electronically:				
Total	672 408	295 450	36 426	1 004 285
- Of which fraud	16.6	118.8	66.7	202.1
Fraud in per cent	0.002	0.040	0.183	0.020

\*The figures are exclusive of cash withdrawal fraud. Source: Finanstilsynet

The proportion of fraud is higher when using payment cards for remote purchases (typically online shopping) than for in-person shopping (using a payment card in a terminal in person at the merchant's). For remote payments without strong customer authentication, fraud accounted for 0.07 per cent of transaction value in Norway in 2022, up from 0.005 per cent in 2021. Fraud accounts for 0.32 per cent of cross-border transactions outside the EEA, an increase from 0.24 per cent in 2021. For further details, please see the tables in appendix 4.

**Table 5.4 Transactions and fraudulent transactions with payment cards reported by card issuers in 2022**

Payment card transactions (volume) 2022	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total
Total	1 809 504 351	739 213 179	77 436 653	2 626 154 183
- Of which fraud	6 656	94 483	55 263	156 402
Fraud in per cent	0.0004	0.0128	0.0714	0.0060

Source: Finanstilsynet

A total of approximately 2.6 billion payments were made by card in 2022. Around 156,000 of these transactions were fraudulent, representing 0.006 per cent. This is roughly on a level with 2021. The proportion of fraud was highest for cross-border transactions outside the EEA.

**Table 5.5 Transactions and fraudulent transactions with payment cards reported by card issuers**

Fraudulent transaction with payment cards (volume)	2020	2021	2022
Total	2 440 487 232	2 553 179 043	2 626 154 183
- Of which fraud	204 603	149 169	156 402
Fraud in per cent	0.008	0.006	0.006

Source: Finanstilsynet

### 5.3 LOSSES ASSOCIATED WITH THE FRAUDULENT USE OF PAYMENT CARDS AT NORWEGIAN MERCHANTS

Table 5.6 shows total losses related to fraudulent transactions with payment cards reported by card acquirer. The table shows losses from fraudulent transactions at Norwegian merchants broken down on fraud with payment cards issued in Norway, payment cards issued in the EEA and payment cards issued outside the EEA. The table shows that losses related to fraud have been reduced both in total and in per cent of total transaction value.

**Table 5.6 Transactions and fraudulent transactions with payment cards reported by card acquirers**

Transaction value (amounts in NOK million)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total transactions
Figures for 2022				
Total	565 222	269 307	36 302	870 832
- Of which fraud	5	28	50	82
Per cent	0.001	0.010	0.137	0.009
Figures for 2021				
Total	541 292	182 249	22 199	745 739
- Of which fraud	3	42	43	88
Per cent	0.001	0.023	0.194	0.012

Source: Finanstilsynet

### 5.4 LOSSES LINKED TO ACCOUNT TRANSFERS

Fraud involving account transfers is where the fraudster issues or modifies the payment or manipulates the payer to initiate the payment order.

**Table 5.7 Transactions and fraudulent transactions – account transfers**

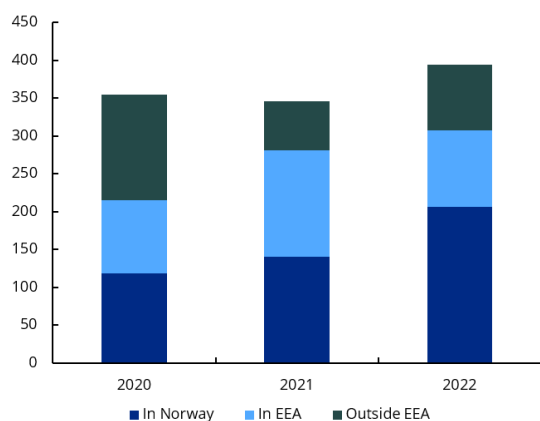
Account transfers initiated electronically (amounts in NOK million)	2020	2021	2022
Total	38 454 037	35 724 912	46 091 136
- Of which fraud	355.5	346.5	394.8
Fraud in per cent	0.0009	0.0010	0.0009

Source: Finanstilsynet

Losses linked to account transfers (generally online banking, see table 5.8) amounted to NOK 395 million in 2022, compared with NOK 346 million in 2021, an increase of 14.2 per cent. The figures show total losses for online banking fraud for Norwegian customers in recent years, irrespective of whether the loss was covered by the customer or the bank. The reported figures show that fraud now increasingly affects transactions in Norway rather than cross-border transactions. One of the reasons for this is that domestic transactions are executed faster.

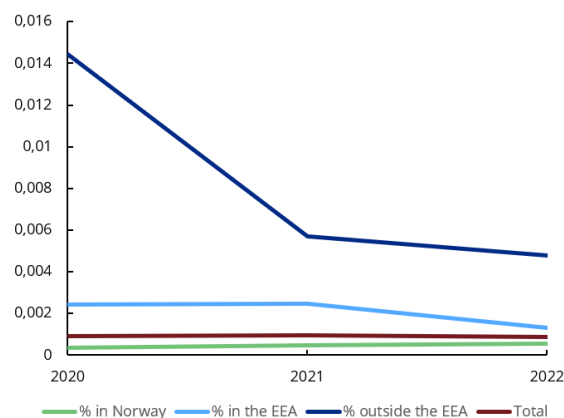
Although there is an increase in losses due to fraud related to account transfers in NOK, losses in per cent of the total transaction amount remain relatively constant, see figure 5.4.

**Figure 5.3 Losses linked to account transfers by geography in NOK million**



Source: Finanstilsynet

**Figure 5.4 Losses in per cent of total card payments by geography**



Source: Finanstilsynet

**Table 5.8 Transactions and fraudulent transactions – account transfers (online banking, etc.) 2022**

Account transfers initiated electronically (amounts in NOK million)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total
Total	35 273 723	7 727 106	1 805 789	44 806 618
– Of which fraud	206.1	101.6	87.0	394.8
Fraud in per cent	0.0006	0.0013	0.0048	0.0009
Of which different types of fraud:				
– Fraudster issues the payment order	78.4	19.7	19.6	117.7
– Fraudster modifies the payment order	0.4	4.6	3.2	8.2
Fraudster manipulates the payer into issuing the payment order	127.3	77.4	64.2	268.8

Source: Finanstilsynet

## 5.5 LOSSES RELATED TO ACCOUNT TRANSFERS INITIATED BY PAYMENT INITIATION SERVICE PROVIDERS

Reported figures for losses related to account transfers initiated by payment initiation service providers show an increase in fraudulent transactions from 2021 to 2022 of approximately 100 per cent and a rise in losses of about 400 per cent.

## 5.6 LOSSES FROM SOCIAL ENGINEERING FRAUD

The reported figures for social engineering fraud, i.e. where the fraudster manipulates the payer into carrying out a transaction, amounted to NOK 290.3 million in 2022, NOK 268.8 million of which involved online account transfers. The total is 21 per cent higher than in 2021 (NOK 240.6 million). This is due to an increase in losses, both where the fraudster manipulates the payer into making a card payment (33 per cent) and where the fraudster manipulates the payer into making an account transfer (20 per cent).

The scale of social engineering fraud is uncertain because payers must bear the losses themselves and some instances of fraud of this type are probably not reported to banks. It is assumed that the actual losses are substantially higher than the reported losses. The defrauded customers often contact their bank to ask them to stop transactions and reverse the transfer of funds. Banks also alert customers, for example when they identify repeated transactions that are extraordinary for the customer.

**Table 5.9 Social engineering – the fraudster manipulates the payer into carrying out a transaction**

Social engineering (amounts in NOK million)	2020	2021	2022
Fraudster manipulates the payer into making a card payment	9.2	16.6	21.5
Fraudster manipulates the payer into making an account transfer	285.3	224.0	268.8
<b>Total</b>	<b>294.5</b>	<b>240.6</b>	<b>290.3</b>

Source: Finanstilsynet

Some of the losses caused by fraudsters initiating payments also result from social engineering (see section 5.7), which in turn contributes to uncertainty about the extent of social engineering. Based on reports<sup>27</sup> from the largest banks to Finanstilsynet, the number of attempted cases of social engineering fraud is steadily increasing. The sum involved in attempted fraud (attack amount) is many times greater than the customers' actual losses. Banks prevent an increasing number of fraud attempts, which means that the amount defrauded as a share of the total transaction amount was somewhat reduced from 2021 to 2022. This is largely due to banks' ongoing fraud prevention and detection.

Social engineering fraud still appears to be the most profitable method for criminals. The type of social engineering where criminals are most likely to succeed is changing. Reporting in line with PSD2 does not distinguish between various types of social engineering, although Finanstilsynet had received figures for subcategories from some of the large banks. These figures suggest that the largest category of fraud in 2022 was phishing, where the potential fraud amount was somewhat higher than before.

## 5.7 LOSSES WHERE THE FRAUDSTER ISSUES THE PAYMENT ORDER

In the PSD2 reporting, social engineering is defined as payment transactions where the fraudster manipulates the payer into carrying out a transaction. However, phishing scams also include some elements of social engineering. When phishing is used, the payer is tricked into disclosing contact and payment information that the fraudster uses to issue a payment order on behalf of the payer. In PSD2 reporting, this is categorised as fraud where the fraudster issues the payment order, see table 5.10. Losses from this type of account transfer fraud came to NOK 117.7 million in 2022, an increase of NOK 9.4 million from 2021. Payment card fraud represented NOK 202.1 million in 2022, up from NOK 145.2 million in 2021.

**Table 5.10 Losses from fraud where the fraudster issues the payment order**

Fraudster issues the payment order (amounts in NOK million)	2021	2022
<b>Payment card fraud</b>	<b>145.2</b>	<b>202.1</b>
– Of which fraud initiated through remote payment channels (e-commerce)	136.0	180.6
– Of which fraud initiated through in-person payments	9.2	21.5
<b>Account transfer fraud</b>	<b>108.3</b>	<b>117.7</b>

<sup>27</sup> Including DNB's [Annual Fraud Report 2022](#)

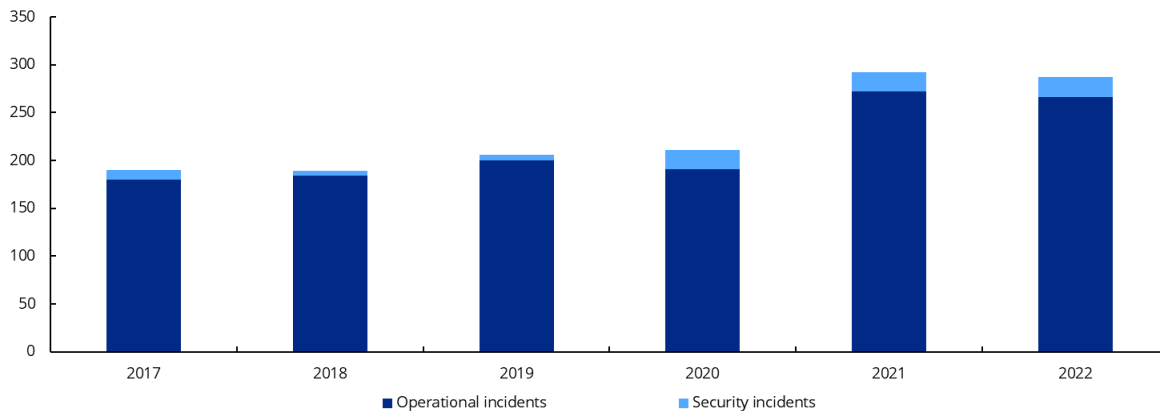
## 6. INCIDENT REPORTING

### 6.1 NUMBER OF ICT-RELATED INCIDENTS

Pursuant to the ICT Regulations, operational incidents or security incidents must be reported to Finanstilsynet without undue delay. Reporting incidents helps ensure a true and timely risk landscape in the financial sector and to reveal patterns and relationships that may be difficult for individual institutions to detect. Nevertheless, the key aspect is the individual institution’s management of ICT incidents to ensure rapid restoration of services followed by the implementation of relevant preventive measures.

The institutions reported 287 ICT-related incidents to Finanstilsynet in 2022, which is on a par with the number the year before.<sup>28</sup> When incidents occur, Finanstilsynet believes it is important that the institution identifies the causes, takes steps to prevent recurrence, and produces a final report. Incidents involving serious irregularities must be monitored throughout the duration of the incident.

**Figure 6.1 Number of reported ICT incidents**



See attachment 5 for further information about the figures. Source: Finanstilsynet

### 6.2 SECURITY INCIDENTS

21 security incidents were reported in 2022, which is on a par with the two preceding years. Some of the incidents were serious for the institutions affected, although no security incidents impacted the financial infrastructure or had serious consequences for the large financial institutions.

In 2022, one institution reported that the vulnerability in the Log4j logging utility, which was found in December 2021, had been exploited to access one of the institution’s servers. The institution found no signs of the access being exploited before the server was shut down.

<sup>28</sup>The increase in the number of incidents from 2020 to 2021 was mainly due to more types of institutions reporting, such as debt collection agencies, and the fact that the institutions reported more types of incidents, including incidents related to systems for detecting money laundering and terrorist financing, as well as interfaces for trusted third-party access to customer payment accounts.

## Vulnerabilities due to the use of open source code

The logging utility Log4j is based on open source code. Such software can be vulnerable because it is released without a description of the built-in security mechanisms or guidance on how it can be implemented securely. Many such utilities are also included in routine libraries with very widespread distribution in development environments. Therefore, mapping all of the consequences of an incident in which a vulnerability in open source code has been exploited can be very demanding. The use of open source code must be based on risk assessments and must be documented.

On 2 March 2022, Nordea was targeted by a DoS attack which prevented access to the bank's services for large parts of the day. Several Norwegian entities, including some financial institutions, were subjected to a DoS attack between 29 June and 5 July. The attacks had only limited consequences. It is often difficult to identify who is behind such attacks unless the attackers identify themselves.

In December 2022, an ICT service provider in Sweden was hit by a security incident that resulted in the service provider shutting down its services for several days. This had consequences for at least seven Norwegian financial institutions, including banks, insurers, and fund managers. One of these institutions found traces of an attack on its servers. For many of the affected Norwegian institutions, the incident meant that the electronic systems for monitoring transactions became unavailable.

Attacks that result in systems being unavailable and/or a risk of data being published are occurring more and more frequently. Attacks can be directed against an institution itself or against service providers on which the institution's relies for various tasks. Finanstilsynet believes it is important that the risk of this type of attack is included in the institution's BIA and in the monitoring of service providers.

- *Security is no better than the weakest link in a supply chain. Finanstilsynet expects institutions to set requirements for subcontractors' ability to maintain security. This can involve subcontractors having to document their own resilience based on conducted security analyses and measures.*

In August 2022, an attacker managed through phishing to compromise the two-factor authentication for an employee's login credentials for a Norwegian financial institution's cloud-based workspace. The employee clicked on a link in an email which led to a login page for the cloud-based solution and logged in with two-factor authentication. However, the login was carried out on the attacker's device and not on the employee's device, which resulted in the attacker's computer being registered as an approved device. In the period before a new two-factor authentication was required, the attacker had the same access rights as the employee to SharePoint, Teams, email, etc. In this case, the attacker used the access rights to send an email to the finance manager, in the employee's name, with a message that the finance manager should pay a large invoice. The attempted fraud was detected.

Microsoft described the new attack method in an article in July 2022.<sup>29</sup> Since the start of 2023, an increased number of such attacks have been observed, although Finanstilsynet is not aware that more financial institutions have been impacted. The vulnerability is not related to a specific cloud solution. One measure for protecting against such attacks is to pre-register all of the devices that can be used to log in.

---

<sup>29</sup> Microsoft's article dated 12 July 2022 describing the method used in the incident: [From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud](#)



Other security incidents in 2022 included the hacking of employee email addresses, falsification of payment instructions and phishing attacks sent to the institution's email address.

Finanstilsynet is in contact with Nordic Financial CERT (NFCERT) about most of the security incidents. In the case of security incidents at institutions that are not members of NFCERT, Finanstilsynet recommends that the institution share information about the security incident with NFCERT.

### **Security testing**

In 2022, an incident was reported to Finanstilsynet where a security test identified a vulnerability in a web-based customer service that could have resulted in improper access to personal and account information. Account numbers was part of the URL\* for some of the searches in the web service and could easily be manipulated. Including data such as an account number in a URL is a breach of good practice in the development of secure web-based applications. To avoid that such vulnerabilities, as well as equivalent ones, are identified many years after the service was introduced, as was the case here, security testing must be carried out as part of the delivery prior to deployment. Thereafter, regular security testing should be carried out.

\* A URL (Uniform Resource Locator) is the string of characters that identifies the address of a page on the internet

## **6.3 ERRORS AND VULNERABILITIES AT CLOUD SERVICE PROVIDERS**

Finanstilsynet has received a number of reports about non-conformances and vulnerabilities at cloud service providers. In 2022, the reports primarily concerned business disruptions due to changes in IT systems at cloud service providers. Such incidents often impact a number of institutions.

In 2022, one institution reported that it had been exposed to a vulnerability ('BlueBleed') in a cloud-based storage service. Following an investigation and analyses, the institution confirmed that none of its data had been exposed. A security incident involving the compromising of a cloud service provider's two-factor authentication, cf. section 6.2, was also reported.

### **Cloud solutions**

Using cloud solutions does not mean that the risk of incorrect configurations, security breaches, or human error will disappear. The risk may be mitigated, but on the other hand, using cloud solutions can introduce new risks and the consequences of an error can have a very broad impact. The institutions must continuously monitor and assess the risk of using cloud solutions.

## **6.4 INCIDENTS IN SYSTEMS FOR DETECTING MONEY LAUNDERING AND TERRORIST FINANCING**

In 2022, 16 incidents were reported that involved non-conformances in an institution's electronic transaction monitoring systems for detecting money laundering and terrorist financing. The incidents were largely related to errors in screening customers and/or transactions against sanctions lists or lists of politically exposed persons (PEPs). The reported errors concerned different service providers, although one common denominator was that the errors arose after changes were made to the service providers' IT systems. When changes are made to transaction monitoring solutions, it is important to ensure that test

plans include both domestic and international transactions and that controls are carried out against updated sanctions and PEP lists<sup>30</sup>.

### 6.5 CAUSES OF OPERATIONAL INCIDENTS

Operational ICT incidents are often caused by errors resulting from changes to ICT systems. Such errors most often have consequences for the availability of services, although they can also involve non-conformances that impact data integrity and confidentiality.

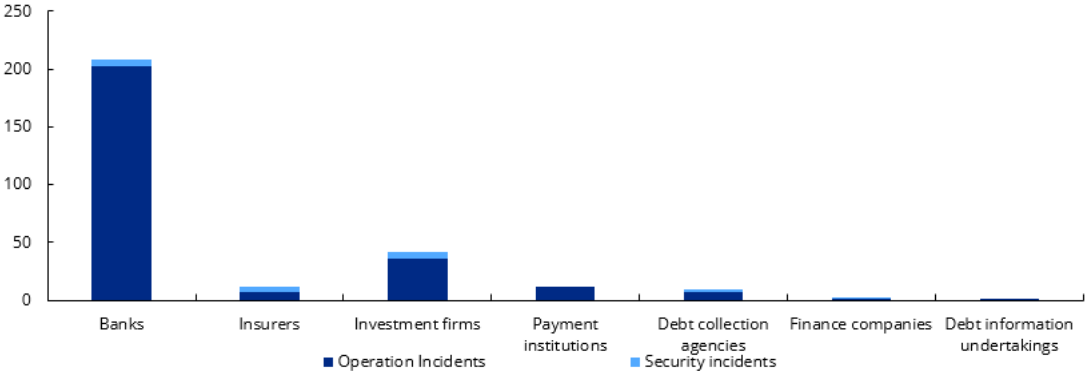
In 2022, 266 operational incidents were reported, which is slightly fewer than in 2021. Several of the incidents concerned errors related to processing of transactions after they were registered by the customer, including unauthorised access to information. The incidents affected a number of institutions at the same time due to errors or changes implemented at common service providers. Several of the reported non-conformances were not identified until many years after the changes had been implemented. This underscores the importance of thorough testing at service providers and acceptance testing and internal controls at the institutions. The individual institution is responsible for its systems and services irrespective of whether they were developed by the service provider or the institution itself.

Other causes of operational incidents in 2022 included various forms of inadequate capacity monitoring, including out of date certificates or insufficient memory allocation, hard coding of parameters in solutions, errors in version management, and differences between backup solutions and production solutions.

### 6.6 INCIDENTS BY TYPE OF INSTITUTION

Figure 6.2 provides an overview of the number of incidents by type of institution and by operational incidents and security incidents. The incidents are discussed in more detail below.

Figure 6.2 Incidents reported in 2021 by type of institution



Source: Finanstilsynet

#### Banks and payment institutions

None of the operational ICT incidents that affected banks or payment institutions in 2022 lasted a particularly long time, although some of the incidents simultaneously affected access to payment services in many banks, as well as Vipps, and lasted two to five hours. There is a heightened risk of operational ICT incidents after changes have been made, particularly changes to software, systems, operational processes, networks or infrastructure. Errors resulting from changes usually have consequences for availability, which is particularly critical for banks and payment institutions. Incidents were also reported concerning errors in

<sup>30</sup> Overview of politically exposed persons

customer account balances. These were caused by business disruptions that resulted in various forms of duplicated transactions. These are critical non-conformances, although the errors were corrected within a short space of time.

On the morning of 16 May 2022, there were problems using payment cards in a number of shops and retail outlets. Neither BankAxept nor international cards were working. The offline backup solutions requiring signatures worked for merchants that had activated this. Some merchants, including Vinmonopolet (the state-owned alcoholic beverage retailer), had not introduced this backup solution. The incident was caused by network changes implemented in Nets. There also proved to be a technical error at one of the terminal providers, which amplified the problems.

The security incidents reported by banks included DoS attacks, vulnerabilities in the logging utility Log4j, an attack on a data service provider in Sweden, and the falsification of payment instructions, see section 6.2 for further details.

### **Investment firms**

Approximately half of the incidents reported by investment firms in 2022 were related to regulated marketplaces.

The security incidents reported by investment firms involved vulnerabilities in the logging utility Log4j and an attack on a data service provider in Sweden, see section 6.2 for further details.

Over the course of the year, there were three operational incidents at Euronext Securities Oslo (Verdipapirsentralen AS) that had the potential to become very serious. In April, an error was identified which in some cases resulted in shareholders being unable to take part and cast votes at the annual general meetings of some Norwegian public limited companies. The error was detected in connection with an annual general meeting in April 2022 and resulted from an update to the IT system in 2020. In May, there was an incident in which a party to a securities settlement lacked sufficient liquidity to meet its obligations. An unauthorised restart of the IT system resulted in calculation errors and the wrong amount being deducted from a liquidity bank. The error had limited consequences but could potentially have been very serious. In November, an error occurred in the payment of dividends from a company listed on Oslo Børs, which resulted in a shareholder being paid too much. While calculating the basis for the payment of share dividends, the normal payment process stopped due to amount limits. A rapid change was implemented and during the subsequent manual registration, the wrong amount was entered for this shareholder. The error was not identified during verification control.

Other reports of operational incidents by investment firms predominantly involved problems with access to online trading in financial instruments and short business disruptions linked to services at marketplaces.

### **Insurance**

The security incidents reported by insurers involved DoS attacks, the hacking of employee email addresses, including one case where the hackers managed to circumvent two-factor authentication, and institutions that were affected by the attack on a data service provider in Sweden, see section 6.2 for further details.

The reported operational incidents involved the exposure of vulnerabilities, the display of incorrect policyholder names, and unavailable customer services.

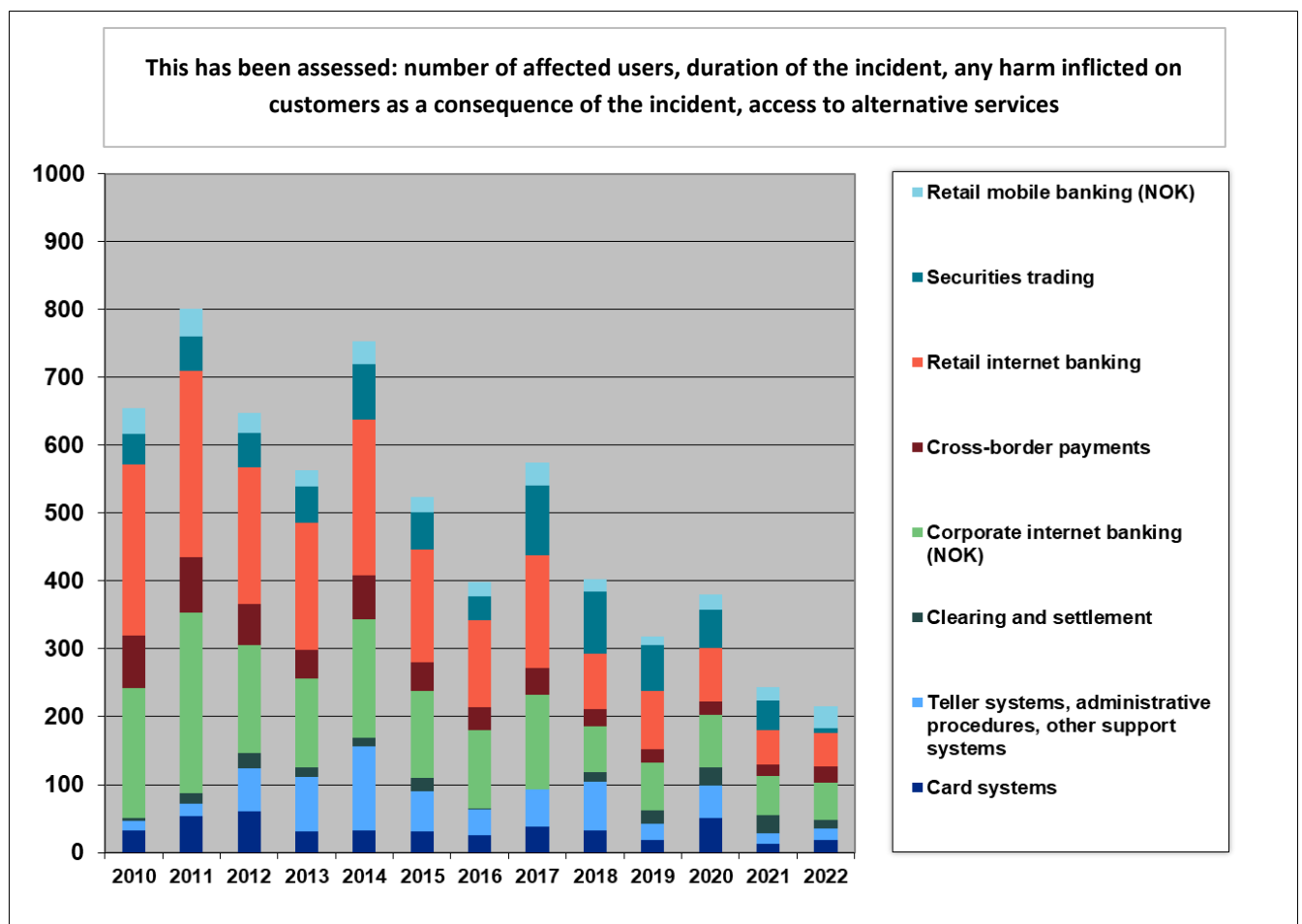
## Debt collection agencies

The security incidents reported by debt collection agencies primarily involved non-conformances in demands for payment. One security reported incident involved a phishing attack against the institution's email address.

## 6.7 ANALYSIS OF INCIDENTS AS A MEASURE OF AVAILABILITY

The severity of the reported incidents varied. With respect to the incidents that caused reduced availability, Finanstilsynet assessed and weighted the incidents based on when they occurred, the duration of the disruption, the number of institutions affected, the number of customers affected, and whether there were alternative services that could meet customer needs. Weighting the incidents resulted in an index that is shown on the vertical axis in figure 6.3. The findings have been collated in a time series so that the trend can be monitored over time.

Figure 6.3 Incidents causing reduced availability for users. Weighted by estimated impact\*



\*The scale on the y-axis is an index based on the weighting of each incident. A lower index value indicates fewer business disruptions with consequences for users. Source: Finanstilsynet

Figure 6.3 shows that the availability of payment systems and other customer services was assessed as being largely unchanged from 2021 to 2022, and somewhat better than in previous years. Overall, service availability was considered satisfactory in 2022.

There were few prolonged operational incidents in 2022, although there were some incidents that affected a large number of users. Transactions that were debited twice, amounts that were reserved twice, and charges that were wrongly debited were included in the category 'Clearing and settlement'.

When incidents are assessed, existing alternative services that meet the needs of customers are considered, for example, whether the customer can use web-based services if mobile phone app services are not working. Furthermore, if the alternatives do not provide the same scope of services, the actors seek to take account of this. For example, mobile phone payment solutions usually do not provide all the services offered by web-based solutions.

### **There is a high degree of redundancy in the Norwegian payment system**

- The customer can often choose between several platforms (mobile bank, online bank, etc.) to perform key services. If one channel is down, the customer can use another channel.
- If one payment service provider (bank) is down, the customer can, if it has multiple banking connections, use another payment service provider that is not affected by the error. For example, electronic invoices are visible in all of the customer's banks and a new customer relationship can be established electronically in the space of a few minutes.
- Payment service providers offer various solutions when it comes to authentication and signing, biometrics, and biometrics in combination with codes and BankID, to mention just a few. If one of these is down, the customer can use a different one.
- Many payment solutions are based on cloud services, which generally have a high degree of redundancy.

This redundancy means that, seen in isolation, the availability of payment services and customer services is increasing. This entails that even though the number of incidents per year is increasing, the services can nonetheless be experienced as being more available than in previous years.

## **6.8 INCIDENTS RELATED TO PROBLEMS WITH DEDICATED PSD2 INTERFACES**

According to the regulations, both account servicing payment service providers and payment service providers must report to Finanstilsynet any problems with dedicated interfaces for third-party providers' access to customers' payment accounts, see discussion in separate box. In 2022, DNB reported the status of its dedicated interface on a weekly basis, including any problems regarding availability or functionality. Other banks reported if they experienced problems with the interfaces in terms of either availability or functionality. Third-party providers also reported frequently in 2022 if they observed downtime and inadequate functionality in the banks' dedicated interfaces for access to customers' payment accounts. Finanstilsynet has published clarifications regarding the regulations, based on the follow-up of received reports.<sup>31</sup>

---

<sup>31</sup> PSD2 – [Presisering og avklaring om regelverket](#)

### **Duty to report non-conformance in dedicated interfaces**

Payment service providers, both account servicing payment service providers and providers of the new payment services, must immediately report issues concerning dedicated interfaces (APIs) to Finanstilsynet.

Furthermore, in the event of non-conformance, account servicing payment service providers must inform third-party providers about the non-conformance and reestablishment measures and describe possible alternative solutions.

The threshold for reporting issues concerning dedicated interfaces must be lower than for incidents pursuant to the ICT Regulations.

## **7. OUTSOURCING**

### **7.1 NOTIFICATION OF OUTSOURCING**

Institutions in the financial sector, with some exceptions, are obliged to notify Finanstilsynet when the institution signs an agreement concerning critical or important outsourcing of, for example, ICT operations, in the event of amendments to such agreements, or when changing service provider. If the outsourcing is not regarded as prudent, makes inspections difficult, or breaches regulations, Finanstilsynet can stipulate terms and conditions for the outsourcing or issue an order to stop implementation of the agreement or terminate it.

In 2022, Finanstilsynet considered around 240 notifications regarding the outsourcing of ICT deliveries, almost 20 per cent more than the year before. Some of the notifications came from cooperating groups of banks on behalf of several banks.

Most of the notifications regarding outsourcing received in 2022 concerned outsourcing to cloud service providers. Finanstilsynet would like to emphasise the importance of ensuring that agreements comply with applicable regulations when purchasing ICT services and that the associated risk is within the institution's risk limits.

### **Some agreements do not meet the requirements of the ICT Regulations**

Finanstilsynet's inspections have identified outsourcing agreements with third parties that do not satisfy the requirements of the ICT Regulations. The most commonly found non-conformances relate to requirements concerning the institutions' right to information and conduct audits of the service provider's delivery, as well as restrictions on Finanstilsynet's access to information from, and inspections at, the ICT service provider where this is a necessary part of an inspection at an institution.

Finanstilsynet requires institutions to revise and update their agreements in line with the applicable regulations. In the future, Finanstilsynet's inspections will have a greater focus on outsourcing agreements that have been signed in the past and agreements with service providers where inspections have previously revealed non-compliance with the regulations.

So far, few institutions have moved their core solutions to public cloud services, although several institutions are currently considering doing this. Moving core systems to cloud-based solutions will often

be an extensive and demanding process, and the institutions' decisions concerning this must be based on thorough risk assessments.

Outsourcing means that institutions may have to deal with more platforms, for example systems at an operations service provider in combination with various cloud-based systems from multiple cloud service providers. This results in greater complexity and a more complicated ICT risk landscape. Finanstilsynet notes that it is becoming increasingly difficult for institutions to monitor ICT outsourcing since the distribution of responsibilities between the service providers can be unclear, which can make it harder to identify errors in the event of incidents.

The increased outsourcing of services to just a few service providers may entail concentration risk, which is difficult for individual institutions to manage. To gain a better overview of the use of subcontractors, Finanstilsynet has recently introduced a new Altinn (the Norwegian public reporting portal) form for submitting outsourcing notifications. The solution covers the outsourcing of both operations and ICT services and is also designed to facilitate automation and standardisation of Finanstilsynet's evaluation of incoming outsourcing notifications.

## 7.2 GOVERNANCE

Institutions are responsible for ensuring that ICT operations are outsourced properly and in compliance with regulatory requirements. See Finanstilsynet's guidance on outsourcing in circular 7/2021.<sup>32</sup>

While institutions must have good expertise in purchasing and monitoring, they also need good functional and technical expertise, including ICT security expertise, in order to both stipulate adequate requirements for service providers' solutions and ICT security and to fully understand the delivery.

The conclusion and monitoring of each outsourcing agreement must be operationalised in line with established internal policies and procedures, and the monitoring of the agreements must be incorporated into the institution's system for risk management and internal control in line with the institution's other activities. This must be established before the institution implements an outsourcing agreement.

## 7.3 CONTRACTUAL PROVISIONS FOR THE TERMINATION OF OUTSOURCING AGREEMENTS

In recent years, there has been a greater focus on the challenges surrounding changes of service providers (contractors) in relation to outsourced operations. To ensure service deliveries, it is important that outsourcing agreements contain provisions that regulate the parties' obligations upon termination of the agreement, including the contractor's obligation to assist the institution (client) in the winding-up phase regardless of the reason for the agreement's termination. The provisions should also cover the contractor's obligation to help the client initiate service deliveries at a new service provider.

In Finanstilsynet's experience, detailed contractual provisions linked to the termination of agreements are particularly important to ensure that the institution's service deliveries are ensured by the contractor.

## 7.4 RISK ASSOCIATED WITH OUTSOURCING

### Cloud services

To date, it has not been customary for the financial sector to transfer critical and important IT systems to the cloud. There are a number of reasons for this, although one of the main reasons appears to relate to the

---

<sup>32</sup> Finanstilsynet: [Rundskriv 7/2021 Veiledning om utkontraktering](#)

institutions' assessment of the maturity of the cloud platforms and ICT risk associated with developing and operating critical and important systems in the cloud.

In the last couple of years, an increasing number of institutions have deemed cloud platforms sufficiently mature and concluded that the associated development and operating risk is lower than when using traditional platforms. The institutions' main arguments include the opportunities for dynamically scaling processing and storage capacity in line with needs and the fact that the cloud platform's capacities provide genuine opportunities for testing emergency preparedness and crisis management plans. Cloud platforms also offer new tools for advanced error management, where backup solutions can automatically be implemented at alternative geographical locations based on defined rules.

Traditionally, institutions have focused on keeping the number of applications, development tools, and technical platforms to a minimum because this results in lower costs and ICT risk. Governance of a larger number of applications, tools, and operating platforms will be more demanding, including having enough capacity to manage ICT risk. It may also entail more extensive interaction between actors in the case of both operations and incident management and increase the range of potential targets that could be attacked in the institution's ICT infrastructure. The institutions must conduct an equivalent assessment with respect to the development and operation of solutions based on cloud services that they conduct for traditional platforms.

### **Risk of lock-in**

Traditionally, many institutions have signed long-term agreements for the development and operation of core systems, typically with 10 to 15-year horizons. When establishing new core systems, institutions have been more likely to sign more or less 'permanent' partnerships with the system service provider, since it possesses both technical and professional business expertise on the core system, rather than with the chosen operations service provider, apart from when the service provider offers both system solutions and operations.

In connection with the development and operation of core solutions based on cloud technology, the use of cloud platform-specific functionality may result in institutions being locked into the chosen service provider. On the other hand, the utilisation of platform-specific functionality can provide institutions with the best value in terms of efficient development, reduced security risk, streamlined emergency preparedness and crisis management plans, and more stable and reliable operations.

Finanstilsynet is of the opinion that the lock-in risk relating to a cloud-based outsourcing model, where the core system makes use of the cloud platform's specific functionality, will not necessarily differ from the risk associated with a traditional outsourcing model. Experience shows that withdrawing from agreements related to core systems based on traditional outsourcing models requires a long implementation horizon since there will often be technological and functional ties, often in combination with outdated technology.

The risk of lock-in must in any case be included in an institution's risk assessment when deciding whether to outsource or not.

### **Exit plans**

To ensure that institutions are as well-equipped as possible to handle situations where service deliveries cease, irrespective of whether the institution or the service provider chooses to end the agreement, it is important that the institution has assessed the consequences of the cessation of the individual deliveries covered by the agreement. Furthermore, the institution must have ensured that the agreement's termination provisions are sufficient to ensure the transition to a new service provider. Institutions' exit plans should also include an assessment of alternative service providers.



## **Supply chains**

Technological advances have increased the complexity of institutions' ICT systems and their operation, and the dependencies between them. Such dependencies can mean that an outsourcing agreement, which seen in isolation is not viewed as critical or important, can have consequences for services that are critical or important.

In order for the business to be operated properly and in compliance with the requirements set out in sectoral legislation and any licence terms and conditions, the institution must have the capacity and expertise necessary to enter into, monitor, and terminate outsourcing agreements. A concrete decision must be made concerning the capacity and expertise the institution must have at any given time. Factors that should be considered include what risk any shortcomings in its capacity or expertise could entail for the institution's operations. The institution must also assess how it will gain access to the required capacity and expertise in order to ensure the stability of the service provision if the institution has to bring back the outsourced services.

In many ICT outsourcing relationships, the contractor will be able to outsource parts of the assignment to its subcontractors. The institution must maintain oversight of the risk associated with services delivered by the contractor's subcontractors, and it is, therefore, appropriate to include contractual provisions that ensure that the institution has a say in relation to this. Unplanned or unwanted changes of subcontractor could, for example, affect an institution's reputation, costs, delivery times, and delivery quality.

When an institution uses ICT systems that were jointly negotiated by several institutions, each institution must conduct an independent impact analysis to assess the effects on its operations of signing up to the joint system. Examples of such ICT systems include the banks' joint operation infrastructure and ICT systems included in the pension account register to which insurers can connect.

# 8. ASSESSMENT OF THE FINANCIAL INFRASTRUCTURE AND INSTITUTIONS' ICT OPERATIONS

## 8.1 THE FINANCIAL INFRASTRUCTURE IS ROBUST

Finanstilsynet believes Norway's financial infrastructure is robust. The institutions' services appear to be well protected against attacks. There were no major ICT incidents that impacted financial stability in 2022, although one incident on 16 May gained a lot of attention, see section 6.6. The institutions' operational stability was satisfactory and better than in previous years.

Slightly fewer incidents were reported in 2022 than in 2021. The proportion of security incidents was about the same as in 2021, while slightly fewer operational incidents were reported. Given the duration of the incidents, the number of users affected, and when they occurred, Finanstilsynet's assessment is that the availability of payment and other customer services was better in 2022 than in previous years, see section 6.7.

The regularity of the clearing and settlement systems was generally good in 2022, although there were some individual incidents. The regularity of the communication with the international message network for payments and securities transfers, SWIFT,<sup>33</sup> and the international settlement system CLS<sup>34</sup> was also good.

While there were fewer attacks on the financial infrastructure in 2022<sup>35</sup> than in 2021, the scale of cybercrime with consequences for the financial sector still appears to be increasing. There was a significant increase in phishing. So far, cybercrime has not resulted in systemic crises or had serious consequences for institutions in the Norwegian financial sector.

Serious vulnerabilities were also identified in some institutions in 2022 that could have had major consequences had they been exploited. Security incidents also occurred at service providers that had consequences for the institutions involved. Vulnerabilities and security holes entail a risk of, for example, information leaks or unauthorised changes to the systems and infrastructure of an institution or their service providers. At the same time, institutions must take account of the fact that the cyberthreat landscape is constantly evolving, partly due to Russia's attack on Ukraine.

A cyber incident can occur without warning, collapse financial infrastructure, and have far-reaching social consequences. The institutions' work on ICT, with respect to both reducing the likelihood of non-conformances and strengthening ICT security in general, helps ensure stable operational solutions, avert cybercrime, and mitigate the consequences of incidents. This includes emergency preparedness and crisis management plans, restoration plans, and ICT security work, including defences against cybercrime.

## 8.2 RISK ASSOCIATED WITH VULNERABILITIES IN INSTITUTIONS' ICT OPERATIONS

Figure 8.1 summarises Finanstilsynet's assessment of the main vulnerabilities in the financial sector. The various vulnerabilities are classified according to the probability of a serious adverse incident occurring and

---

<sup>33</sup> SWIFT's website: [About us](#)

<sup>34</sup> CLS' (Continuous Linked Settlement) website: [About us](#). A US financial institution that offers settlement services to its members in the foreign exchange market (FX).

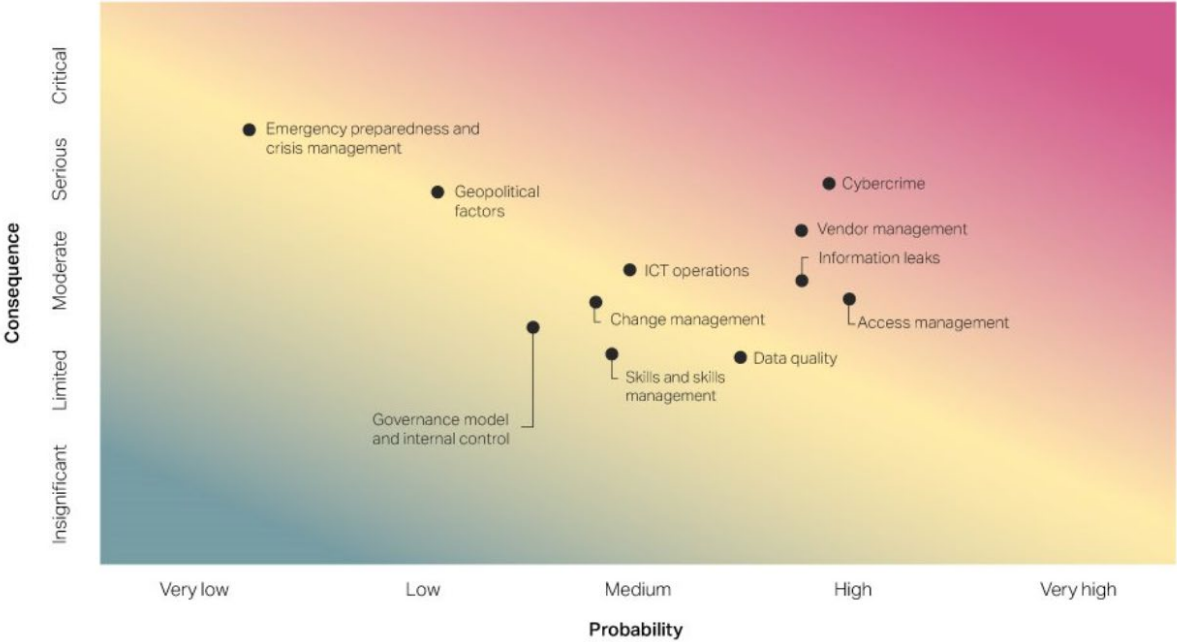
<sup>35</sup> Digi.no 18 March 2023: [Samarbeid er det beste forsvar i cyberkrigen](#)

the severity of the resulting consequences for the individual institution. The observations and assessments the classification is based on are provided in table 8.1 and discussed in more detail in appendix 2.

Finanstilsynet considers vulnerabilities related to institutions’ defences against cybercrime to be the main risk associated with the institutions’ use of ICT, where the overall risk is considered high. Vulnerabilities in relation to vendor management, access management and information leaks are also key risks, and the overall risk is considered moderate to high. The risk associated with vendor management was regarded as higher in 2022 than in the year before. While the risk associated with institutions’ defences against cybercrime was regarded as slightly higher, the risk associated with institutions’ defences against information leaks was regarded as slightly lower than in 2021.












The risk associated with vulnerabilities in the institutions’ emergency preparedness and crisis management, as well as geopolitical factors, is considered moderate to high. The risk associated with vulnerabilities in the institutions’ change management, governance model and internal control, ICT operations, skills, and skills management, as well as data quality, is considered moderate. The risk associated with an institution’s monitoring of skills and skills management was regarded as somewhat lower in 2022 than in the year before, while the risk associated with monitoring ICT operations was regarded as lower.

Figure 8.1 Finanstilsynet’s assessment of vulnerabilities and risks for 2022



Source: Finanstilsynet

Table 8.1 Vulnerabilities that could represent a risk of adverse incidents

Area	Vulnerabilities that could represent a risk of adverse incidents (Degrees of risk, probability and consequences are stated in figure 8.1)	Trend
<b>Governance model and internal control</b>	An inadequate overview of which controls are included in the institution's internal control environment and how the controls should be performed, monitored and audited may result in factors that represent an operational risk not being identified and risk-mitigating measures in line with the institution's risk tolerance not being implemented.	
<b>Skills and skills management</b>	A scarcity of resources in Norway within operations, architecture, security and new technology, as well as inadequate skills management, may lead to institutions being unable to meet current and future skills needs. Problems and errors that occur may be difficult to resolve. Dependence on foreign assistance may increase.	
<b>Vendor management</b>	Complex supply chains, with multiple service providers and subcontractors in the value chain, demanding cooperation models (strategic, administrative and operational) and a lack of expertise may result in weaker monitoring and control over critical and outsourced ICT services.	
<b>Cybercrime</b>	Inadequate security testing, security updates, training and awareness raising among employees, and insufficient monitoring of activities in its own technical infrastructure, including networks and systems, may result in criminals inflicting damage on the institution through digital attacks. Fraud related to the use of financial services can also inflict losses on the enterprise.	
<b>Information leaks</b>	Inadequate information classification, including documentation, and controls for monitoring information that is sent by email, copied to external storage devices or copied to private cloud services may cause the institution or its customers damage if unauthorised people get their hands on the information.	
<b>ICT operations</b>	Complex integration between systems from different service providers, integration between old and new systems, multiple integration points between systems, increased functionality in self-service channels and increased use of cloud services may result in challenges in maintaining stable and secure operations.	
<b>Emergency preparedness and crisis management</b>	Inadequate analyses of the consequences of a crisis, inadequate training and exercises in crisis management, shortcomings in disaster recovery solutions/backup solutions and inadequate backup solutions may result in challenges for institutions when it comes to maintaining critical ICT services in the event of severe disruptions at operating locations.	
<b>Geopolitical factors</b>	Geopolitical factors or interruptions in communications with other countries, where service providers are prevented from maintaining deliveries of critical ICT services from abroad, may result in challenges in maintaining stable and secure operations.	
<b>Change management</b>	A fast pace of development, where quality is sacrificed at the expense of time, may result in functional errors in applications and systems, and in security holes not being identified. Inadequate control of changes to operating configurations may result in interruptions to critical business processes and the institution being exposed to cybercrime.	
<b>Access management</b>	Inadequate control and monitoring of broader access rights, for employees and service provider personnel, may harm the institution and its customers as a result of information leaks and deliberate or unintentional operational errors.	
<b>Data quality</b>	Deficiencies or errors in data may result in analyses and controls being performed based on incorrect or insufficient information. This may include errors in credit ratings, errors in controls aimed at detecting money laundering or fraud, errors in risk assessments and errors in monitoring operations.	

Arrow categories: Increasing, slightly increasing, unchanged/stable, slightly decreasing and decreasing. Source: Finanstilsynet

## 9. NEW REGULATIONS ON DIGITAL RESILIENCE – THE DORA REGULATION

In September 2020, the European Commission presented a digital finance package that included a digital financial strategy and regulations for ensuring user access to innovative financial products, while simultaneously safeguarding consumer protection and financial stability. The Regulation on digital operational resilience for the financial sector (DORA) was launched as part of this package.<sup>36</sup> DORA was finally approved by the European Parliament and the European Council in November 2022, and the date for its entry into force has been set as 17 January 2025. The proposed regulations are considered EEA relevant.

DORA is intended to help ensure that all participants in the financial system have the necessary measures in place to reduce the risk of cyberattacks and other risks associated with ICT operations. The proposed legislation will require all institutions to be able to deal with all types of disruptions and threats to institutions' ICT operations. The proposal also introduces an oversight framework for ICT service providers, such as providers of cloud services.

To ensure the comprehensive implementation of the requirements for the financial sector's ICT risk management, the proposed legislation covers various types of institutions regulated at the EU level. It will make it possible to achieve homogeneous application of the requirements for ICT risk management, considering that there are significant differences between institutions in terms of size, business profiles and exposure to cyber risk.

In Norway, the use of ICT in the financial sector is mainly regulated via the ICT Regulations. For some types of institutions, the use of ICT is regulated elsewhere. The scope of DORA is more extensive than the scope of the ICT Regulations, although it does not fully cover all areas. Furthermore, Finanstilsynet's supervisory activities are regulated by the Financial Supervision Act. DORA contains provisions that overlap with both the ICT Regulations and the Financial Supervision Act. DORA also contains provisions that are currently not covered by Norwegian law.

The proposed legislation sets requirements for governance of ICT operations, risk management, incident reporting, operational resilience testing, and monitoring of service providers. The ICT Regulations, corresponding special regulations, and the European supervisory authorities' guidelines already contain a number of these requirements, which means that in practice the new regulations will generally not result in any material changes for Norwegian institutions.

The regulations allow information and intelligence related to cyberthreats and vulnerabilities to be shared, as Norwegian institutions already do through their interaction with Nordic Financial CERT (NFCERT).

DORA will necessitate amendments to several Regulations within the finance area. These are stipulated as amendment provisions in DORA. In addition to the DORA Regulation, the DORA Directive<sup>37</sup> has also been approved. The Directive is also EEA relevant. The DORA Regulation entails a need to amend a number of Directives within the finance area. Directives cannot be amended through regulations, meaning that amendment provisions must be issued in the form of directives. The relevant amendment provisions concern changes in operational risk or risk management requirements or cross-references, including in

---

<sup>36</sup> [The Digital Operational Resilience Act](#)

<sup>37</sup> [Directive \(EU\) 2022/2556 of the European Parliament and of the Council](#)

the Capital Requirements Directive (CRD), the Markets in Financial Instruments Directive (MiFID II), the Undertakings for the Collective Investment in Transferable Securities Directive (UCITS) and the Directive on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).



**FINANSTILSYNET**

Revierstredet 3  
P.O. Box 1187 Sentrum  
NO-0107 Oslo

Tel. +47 22 93 98 00  
post@finansstilsynet.no  
finansstilsynet.no

