



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

RISK AND VULNERABILITY ANALYSIS 2024

The financial sector's use of Information and Communication Technology (ICT)



Risk and Vulnerability Analysis 2024

- 1. SUMMARY 4
- 2. FINANCIAL INFRASTRUCTURE 6
 - 2.1 Importance..... 6
 - 2.2 The financial infrastructure crisis preparedness committee 8
 - 2.3 Significant changes in the financial infrastructure 8
 - 2.4 Collaborative initiatives within the financial industry 9
- 3. THE THREAT LANDSCAPE..... 11
 - 3.1 The cyberthreat landscape is evolving 11
 - 3.2 Measures within the institutions..... 12
 - 3.3 Cooperation in the security area..... 14
- 4. FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS 17
 - 4.1 Supervision of ICT and payment services in 2023 17
 - 4.2 Institutions' assessment of critical aspects related to ICT operations 19
 - 4.3 Summary of the institutions' risk and vulnerability reporting..... 22
- 5. FRAUD 27
- 6. INCIDENT REPORTING..... 29
 - 6.1 Increase in reported incidents..... 29
 - 6.2 Security incidents 30
 - 6.3 Acceptance test of changes carried out by service providers..... 31
 - 6.4 Incidents in systems for detecting money laundering and terrorist financing..... 31
 - 6.5 Incidents by type of institution..... 31
 - 6.6 Analysis of incidents as a measure of availability 34
 - 6.7 Incidents related to dedicated PSD2 interfaces 35
- 7. Outsourcing 36
 - 7.1 Follow-up on outsourced ICT 36
 - 7.2 Model for overseeing and controlling outsourced ICT operations 37
 - 7.3 Monitoring and control of outsourced IT operations 38
- 8. ASSESSMENT OF THE FINANCIAL INFRASTRUCTURE AND INSTITUTIONS' IT OPERATIONS 41

8.1 The financial infrastructure is robust	41
8.2 Risks associated with vulnerabilities in institutions' ICT operations	42
9. THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA)	45

1. SUMMARY

The financial infrastructure in Norway is robust, and institutions' ICT services appear to be well-protected against attacks. Institutions within the financial sector engage in ongoing efforts to fortify their defences and automate their incident response, thereby averting cyberattacks before they inflict consequences on the institutions and their customers. These endeavours are undertaken both internally by the institutions themselves and through collaborative initiatives within the industry and with authorities.

In 2023, there were no ICT incidents with implications for financial stability, although certain incidents attracted significant attention. The number of operational incidents increased, primarily due to the fact that certain incidents impacted multiple banks simultaneously. Overall, Finanstilsynet considers the availability of payment services and other customer services to be satisfactory in 2023, approximately at the same level as observed in 2021 and 2022.

The cyberthreat landscape is evolving, with the threat level remaining high yet stable. The expanding scope of digitalisation widens the scope of action, with both organised criminals pursuing financial gain and state actors engaging in cyberattacks. Cooperation among criminal networks is on the rise, exacerbated by geopolitical tensions. The situation has heightened awareness of the risk of systemic cyber incidents and the importance of digital resilience and robustness within the financial sector. Long and complex supply chains pose vulnerabilities exploited by threat actors. Serious failures in ICT systems could potentially threaten financial stability and impact civil protection.

Each institution within the financial sector bears an independent responsibility for safeguarding its own systems against intentional and unintentional incidents. This obligation applies even if some or all of the institution's ICT operations are outsourced. In this year's report, Finanstilsynet underscores the importance of institutions conducting thorough threat assessments, impact analyses, and establishing contingency plans for their systems. Institutions should ensure that security testing of their systems is conducted and that adequate measures are in place to address attacks, including those targeting their service providers. Participation in forums that share intelligence and facilitate knowledge exchange will enhance institutions' capacity in both preventive efforts and in responding to potential attacks.

Supervisory activities in 2023 uncovered weaknesses and vulnerabilities in the institutions' management of ICT. Finanstilsynet highlighted deficiencies in various institutions' governance and control of ICT operations, as well as inadequate follow-up of ICT risk within the second line of defence. The risk associated with extensive reliance on ICT service providers and inadequate follow-up of the providers constitutes a significant share of the institutions' ICT risk. Outsourcing of ICT operations often involves multiple ICT service providers, data centres, and platforms that institutions must relate to. This can lead to increased complexity and a more intricate risk landscape and make it more demanding to oversee ICT operations.

Through reporting to and dialogue with Finanstilsynet, institutions and service providers have highlighted several key risks and vulnerabilities related to ICT operations. Among these, institutions emphasise the risk associated with increasingly lengthy and complex supply chains, as well as challenges in obtaining acceptance from subcontractors for the institutions' own strategies and guidelines. This is particularly pertinent for services from service providers outside the EEA.

Finanstilsynet regards vulnerabilities related to institutions' defences against cybercrime as the most significant risk associated with their use of ICT in 2023, where the overall risk is deemed to be high. Vulnerabilities related to vendor management, governance model, internal controls, and access control also represent key risks, with the overall risk considered to be medium to high.

Losses resulting from fraud continue to increase. The methods of fraud are numerous and constantly evolving. In 2023, total losses amounted to NOK 928 million, representing a 51 per cent increase from 2022. Through their systems and controls, banks prevent a significant number of fraud attempts. In 2023, banks prevented fraud attempts equivalent to NOK 2,072 million, highlighting the importance of banks taking measures.

The transition from the Regulations on use of information and communication technology (ICT) to the Regulation on Digital Operational Resilience in the Financial Sector (DORA) will entail stricter requirements for institutions in the Norwegian financial sector. This is an important measure to enhance operational resilience and promote robustness, financial stability, customer protection, and safeguarding of vital functions in society. Implementation of common European requirements may impact the trust in international markets regarding Norwegian institutions' risk management and the Norwegian authorities' oversight of the financial sector.

Digital robustness and resilience in the financial sector are crucial for maintaining trust in the financial system. The cyberthreat landscape is increasingly challenging due to geopolitical unrest and an increase in cybercrime. In 2024, Finanstilsynet will oversee institutions' compliance with requirements for secure and resilient ICT systems and assess their preparedness for handling critical situations.

2. FINANCIAL INFRASTRUCTURE

2.1 Importance

A resilient financial infrastructure is crucial for financial stability and well-functioning markets. Secure, efficient, and reliable payment and settlement systems foster trust among participants in the financial system and promote economic efficiency. The Norwegian Directorate for Civil Protection (DSB) has designated financial services as a vital function in society¹, and the Ministry of Finance has defined 'Ensuring society's ability to provide financial services'² as one of three fundamental national functions (FNF) within its sector.

The financial infrastructure is designed to ensure that payments and transactions in financial instruments are recorded, cleared, and settled. The infrastructure is complex and involves several actors and providers, as outlined in Box 2.1. Inadequate resilience or poor security levels at a single actor can constitute a weak link in the value chain, leading to undesirable incidents affecting other actors. The financial sector also relies on infrastructure such as power supply and electronic communication. Failures by key actors can have significant societal consequences and, in the worst case, threaten financial stability, regardless of whether the failure is caused by criminal activity or operational deviations.

If financial transactions cannot be executed, important societal functions will cease to operate satisfactorily within a short period of time. The societal consequences could be particularly serious if major institutions, or those acting on behalf of many others, are affected. Sensitive information going astray or violations of the rules on handling inside information can undermine trust in marketplaces and the financial system. Unauthorised access to customer and account data that compromises or renders data inaccessible will pose significant challenges for both customers and institutions.

Finanstilsynet and Norges Bank collaborate on monitoring the financial infrastructure in Norway, including through joint inspections, investigations, and risk assessments.

¹ Directorate for Civil Protection (DSB), [Vital functions in society](#) (Norwegian only)

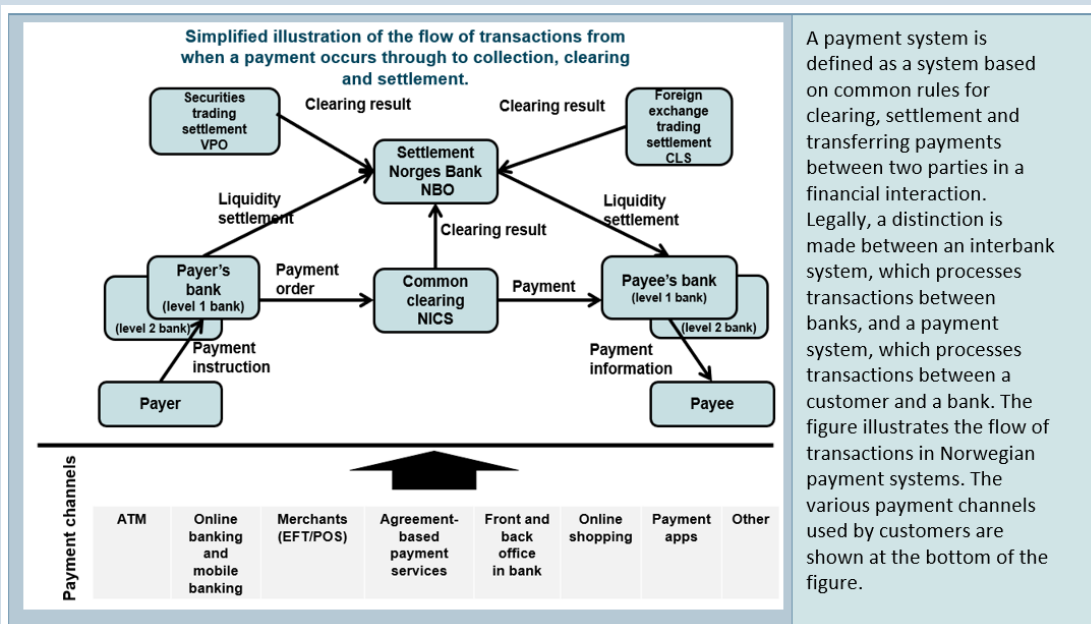
² The Ministry of Finance has defined three FNFs in the financial sector, see section 4.2.2 of [Financial Markets Report 2023](#) (Norwegian only)

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 The financial infrastructure crisis preparedness committee

The Financial Infrastructure Crisis Preparedness Committee (BFI)³ 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 serves as the secretariat for BFI. Other participants include key government authorities and institutions responsible for critical functions within the financial infrastructure. BFI holds regular meetings and conducts annual emergency response exercises. Involvement in BFI helps Finanstilsynet obtain a comprehensive and detailed understanding of the state of the financial infrastructure.

2.3 Significant changes in the financial infrastructure

In 2023, several significant changes in the Norwegian financial infrastructure were both implemented and announced.

In 2020, the Eika Alliance entered into an agreement with Tietoevry for the provision of core banking solutions to the Eika banks. The transition from SDC to Tietoevry was completed in 2023. Verdipapirsentralen AS (Euronext Securities Oslo) transferred its ICT operations to Tietoevry in 2023. Seen in isolation, the transition to Tietoevry for Verdipapirsentralen AS and the Eika Alliance increases concentration risk since Tietoevry already serves several institutions in the financial sector, as an operations service provider.

As a result of mergers between institutions, several ICT systems were also merged in 2023. This process will continue in 2024, including the migration of Sbanken's customers to DNB's systems.

BankAxept aims to launch digital payment cards in the first half of 2024, enabling their payment solution to be used in digital wallets and for e-commerce transactions. As a result of EU requirements, Apple has opened up its contactless functionality for other actors. This enables Norwegian institutions to offer their own solutions for contactless payment with Apple products.

³ See topic page on [BFI](#)

The financial industry has considered improvements to BankID's issuing model and governance structure and is exploring the possibility of implementing a new model for BankID issuance. The model supports the goal of the national eID strategy⁴ that all relevant user groups should be able to easily obtain an eID at the security level they require.

2.4 Collaborative initiatives within the financial industry

Bits AS is the infrastructure company for the banking and financial industry, tasked with modernising the payment infrastructure. The project for transitioning to the ISO 20022 standard for instant payments (Instant 2.1) was completed in 2023, and the banks adopted the solution. The formats are now standardised, and the solution significantly simplifies the technical architecture. Work on adapting the standard for structured customer information, particularly for payments with KID (the OCR service), will commence in 2024.

Bits is also working on modernising the infrastructure surrounding the banks' common clearing system for Norwegian kroner (Norwegian Interbank Clearing System, NICS). In this effort, international functional divisions are implemented between the clearing itself and other functions closely integrated with the clearing solution. Specific projects in 2024 will impact the solutions of banks and ICT service providers, as well as the shared operational infrastructure.

In November 2023, the Ministry of Finance appointed a working group tasked with assessing the preparedness of the payment system⁵. The working group's tasks include mapping functionality and risks and evaluating the need for measures to enhance confidence that electronic payments can be executed under various scenarios. The working group comprises representatives from Finanstilsynet, the Ministry of Finance, and the financial industry and is chaired by Norges Bank. The work is scheduled to be completed by September 2024.

The backup solution for BankAxept's payment cards is part of the electronic payment system's emergency preparedness. In 2021, the backup solution was reinforced by significantly increasing the capacity of payment terminals for providers of vital functions in society in the retail market with wide distribution, such as grocery chains, pharmacy chains, and fuel outlets. Participation in the backup solution is voluntary for merchants. Effective emergency preparedness in the electronic payment system requires the enrolment of more merchants in the solution, including more critical actors in the retail market, and regular testing by merchants to ensure that it functions as intended. The resilience of the payment system may be compromised as an increasing number of merchants adopt payment terminal solutions that do not support BankAxept's backup solution.

⁴ [National strategy on eID in the public sector](#) (Norwegian only)

⁵ [Working group tasked with assessing the preparedness of the payment system](#) (Norwegian only)

The issuance of BankAxept payment cards with 'offline PIN'-support commenced in 2023, and the replacement of existing payment cards will continue over the next three years. The objective is to enhance the resilience of the payment system by introducing functionality that allows the PIN code to be verified against information stored in the payment card in case a payment terminal lacks internet connection.

The public sector and the financial industry collaborate on the digitalisation and streamlining of critical services in society through DSOP⁶ (Digital Collaboration Public-Private). The solutions yield significant benefits for society. Examples include the purchase, financing, and registration of real estate, with an integrated digital process for home buyers, sellers, real estate agents, banks, and the Norwegian Mapping Authority. However, such integrated solutions also introduce new dependencies and vulnerabilities that must be considered in both ongoing operations and contingency planning.

⁶ [BITS' website on DSOP](#) (Norwegian only)

3. THE THREAT LANDSCAPE

3.1 The cyberthreat landscape is evolving

The cyberthreat landscape is constantly evolving. Increased digitalisation in society and technological advancements expand the opportunities for criminal actors. Recent years' changes in the risk and threat landscape, coupled with the rise in cybercrime, have led to greater attention being directed towards the risk of systemic cyber incidents and the importance of digital resilience.

The risk of adverse incidents remains high. State actors are believed to be directly or indirectly involved in digital attacks, and geopolitical tensions are increasing due to Russia's invasion of Ukraine, conflicts in the Middle East, and tensions between China and the US. Criminals continuously develop their methods, including by use of new technology. They often prioritise targets that offer high potential gains at low costs, such as online fraud or ransomware attacks. Collaboration among criminal networks is increasing, including through the provision of services to each other and to state actors, and it can be challenging to distinguish between threats posed by organised criminals and by foreign intelligence.

Both the Norwegian Intelligence Service (E-tjenesten) and the Norwegian Police Security Service (PST) highlight a significant threat from state actors, partly through intelligence and network operations (cyber reconnaissance and sabotage of critical infrastructure). The threats to the financial sector are primarily associated with attacks targeting other institutions, or attacks against a value chain that also affect financial institutions. The Norwegian National Security Authority (NSM) also emphasises the recruitment of insiders within organisations and malicious acquisitions and investments as risk factors. Finanstilsynet has noted an increase in insider-related incidents over the past year.

In its annual threat assessment for the financial sector, Nordic Financial CERT (NFCERT) points out that the overall cyberthreat against the financial industry remains high, but the threat landscape is stable. Criminal groups pose the most serious and likely threat to the Nordic financial sector, with the most common method being data encryption and/or threats of publishing sensitive information with ransom demands. NFCERT also assesses that insider issues are a threat that is often underestimated, and insiders can be current or former employees, partners, contractors, and third parties. With privileged access to an institution's digital assets and knowledge of internal processes and procedures, insiders may unintentionally or deliberately misuse their access and expertise.

Serious failures in ICT systems can have severe consequences for the financial infrastructure. In the worst-case scenario, financial stability may be jeopardised, particularly if critical functions for civil protection are affected, whether the failure is caused by criminal activity, targeted attacks, or operational disruptions. The financial systems are highly integrated, hence there is a high risk that isolated incidents may impact other actors and services.

Long and complex supply chains pose a vulnerability that threat actors exploit. There will still be a risk of attacks on value chains and from actors seeking to exploit security vulnerabilities in widely used software. Security vulnerabilities are exploited by both criminal and state actors. Within the financial sector, threat actors are also able to exploit the expansion of attack surfaces resulting from digitalisation. Financial institutions reported incidents in 2023 where

vulnerabilities in service providers' software were exploited to gain access to the service provider's systems. Such intrusions can result in information leakage, unauthorised changes to the institutions' systems and infrastructure, or data encryption with ransom demands.

Denial-of-Service (DDoS) attacks from hacktivists will continue to pose a threat to institutions. The institutions are well-prepared to withstand this type of attack and promptly implement measures. The impact will typically be limited to temporarily disrupting the availability of online solutions such as customer self-service portals and information websites. The purpose of such attacks is usually not financial gain, but rather to draw attention, spread uncertainty, concern, and disinformation, or demonstrate dissatisfaction with a country or corporation.

Institutions continuously work on enhancing their systems for monitoring unusual activity, automatically detecting and managing incidents, and preventing attacks and fraud attempts. Although incidents are increasingly handled automatically, institutions require manual review of certain detected incidents. Strengthened defences against cybercrime result in attacks being increasingly averted without consequences for the institution. The number of security incidents of high severity has decreased.

3.2 Measures within the institutions

Each institution bears the responsibility for securing its own systems. This includes the parts of the business that are outsourced. The responsibility entails necessary and sufficient competence and capacity to prevent and detect attacks and to develop contingency and crisis management plans, including plans and solutions for restoring systems after attacks.

Institutions must continue their efforts to identify their own risks, vulnerabilities, and assets that may be at risk, implement preventive measures, and be prepared to handle attacks and the consequences of attacks. Protecting confidential information and raising awareness among their employees about the cyberthreat landscape are also important aspects of this work.

In this year's report, Finanstilsynet will highlight the following areas:

The use of threat assessments

The risk of malicious activities cannot be assessed in the same manner as the risk of operational ICT incidents, as the latter typically rely on historical experiences and/or expected frequencies. However, risk assessments of malicious activities must be based on forward-looking threat assessments that take account of the institution's business operations, size, geographical location, and the attractiveness of the assets being protected. Furthermore, an analysis of vulnerabilities in the digital defence of these assets should be conducted. The so-called risk triangle or three-factor model⁷ is an example of such a methodology and can be used to estimate the risk of threat actors succeeding in targeting the institution's assets.

Measures to prevent attacks

A crucial measure to prevent cyberattacks is to ensure that production systems are updated with the latest, verified and authorised versions and security patches. In its supervisory activities, Finanstilsynet emphasised the importance of removing components that are not in

⁷ [The three-factor model](#) (Norwegian only)

use and passive and/or outdated systems. There is also a clear correlation between the use of older systems and increased risk of incidents, as well as costs associated with safeguarding them.

Security testing of internal systems

To uncover attacks, institutions must possess the necessary expertise internally and consider the use of external specialist services.

The Digital Operational Resilience Act (DORA) mandates testing of digital operational resilience, whereby institutions (excluding microenterprises) are required, as part of the ICT risk management framework, to have a comprehensive programme for risk-based testing. The purpose of this testing is to uncover weaknesses, deficiencies, and deviations in digital resilience, assess readiness for handling ICT incidents, and provide a basis for rapid and effective implementation of improvements and corrections.

Threat-led penetration testing (TLPT) is a method used to test institutions' digital resilience, i.e. their ability to detect, protect against, and respond to sophisticated cyberattacks. Threat intelligence and the use of external test specialists ('Red Teaming') contribute to a realistic testing of the institution's defences. The method simulates tactics, techniques, and procedures that real threat actors are assumed to employ. It is emphasised that the institution's staff participating in the tests shall be unaware of when and how the test attacks occur, and the institution should use the experiences gained to strengthen its own systems. The requirement for TLPT testing initially applies to all institutions licensed by Finanstilsynet. When assessing which institutions should be subject to TLPT testing, consideration is given to the institution's size, overall risk profile, and the nature, scope, and complexity of its services, activities, and operations.

Effective contingency plans and exercises

Institutions must ensure that their operations can be restored after cyberattacks and have updated and tested plans for this purpose. In addition to plans for restoring systems and any lost data, the institution must have plans for managing an incident until systems and lost data are restored. The institution must also ensure that it has updated communication plans for various incident scenarios.

Assessments and measures should be carried out to ensure that institutions' contingency solutions and backups of systems and information are protected against cyberattacks.

Institutions should conduct regular scenario-based contingency exercises. Experiences from contingency tests should be reviewed to eliminate weaknesses and deficiencies in contingency systems and procedures. It is also important for institutions to test how quickly their systems can be restored under various scenarios and assess the potential consequences of any downtime for the institution and its customers.

Defences against value chain attacks

Institutions that use external service providers may be exposed to risks associated with complex value chains and should implement specific countermeasures. Institutions must also ensure that their service providers have adequate measures embedded in their solutions. Examples may include:

- micro segmentation⁸ and encryption of internal networks to prevent unauthorised access and code propagation
- monitoring network traffic, including internal network traffic, to detect unusual patterns in data traffic or behaviour
- strengthening control over system deliveries, service providers, and service providers' use of subcontractors as well as outsourcing involving IT dependencies in general
- use of systems and solutions for automated control and verification of program code.

The value to institutions of monitoring network traffic will be reduced as increasingly larger portions of their system portfolios are outsourced to cloud service providers. However, outsourcing requires close control of the service providers' ICT security management and follow-up of subcontractors. Given the threat posed by value chain attacks, Finanstilsynet expects institutions to allocate necessary resources to ensure proper oversight of their service providers.

Other measures to protect enterprise assets

The use of information and experience-sharing services, as well as collaboration through CERTs⁹, has proven to be beneficial in enhancing institutions' capacity in terms of both preventive measures and support during actual attacks.

NSM develops general principles¹⁰ and measures that institutions in the financial sector should refer to in order to protect information systems against unauthorised access, damage, or misuse. These principles are based on recognised standards and are universally applicable to ICT security regardless of the type of business. NSM has also developed a range of other advice and recommendations within cyber security¹¹.

3.3 Cooperation in the security area

Various arenas and forums for cooperation in the area of security are important to strengthen defences against cybercrime. This includes cooperation between authorities at national and international levels, between authorities and institutions, and among institutions.

Assessment of critical institutions in the financial sector

The Security Act specifies economic stability and freedom of action as one of several national security interests. The responsible sector ministry is tasked with identifying and keeping track of fundamental national functions (FNFs) as well as institutions that are of vital or material importance to these functions. For the financial sector, the Ministry of Finance decides whether institutions that are of vital importance to FNFs should be fully or partially subject to the Security Act. Finanstilsynet, in collaboration with Norges Bank, provides input to the Ministry of Finance's work.

⁸ 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 compared with more established approaches, such as network segmentation and application segmentation.

⁹ CERT: Computer Emergency Response Team

¹⁰ [NSM ICT Security Principles](#)

¹¹ [NSM's advice and recommendations](#) (Norwegian only)

Institutions that are of vital or material importance to an FNF may be more attractive targets for cybercrime and attacks by foreign intelligence.

Better risk understanding through cooperation and information sharing

Financial institutions in the Nordic region cooperate through Nordic Financial CERT (NFCERT). The purpose is to enhance the resilience against cyberattacks of the Nordic financial industry. Cooperation and information exchange among financial institutions contribute to raising awareness of the current threat and risk landscape, strengthening resilience against cyberattacks, and enhancing the ability of the institutions to respond quickly and effectively to cyber security threats and cybercrime. NFCERT regularly produces and distributes threat reports to its members. Finanstilsynet observes that institutions that do not participate in this cooperation may be less prepared to handle cyberthreats and adverse incidents and encourages institutions to consider the use of information sharing and experience-sharing services and CERTs. The use of such services has proven beneficial in enhancing the capacity of institutions to implement proactive measures and as support during actual attacks.

Finanstilsynet has been designated by the Ministry of Finance as sectoral response environment (SRE) responsible for managing ICT security incidents in the financial sector within Finanstilsynet's area of responsibility. This role is performed in collaboration with NFCERT.

Finanstilsynet is a partner in the Norwegian National Cyber Security Centre (NCSC), which serves as a platform for national and international cooperation on identification (detection), management, analysis, and advice related to cyber security. The Norwegian National Security Authority (NSM) established NCSC to enhance Norway's resilience and preparedness in the digital domain. Participation provides Finanstilsynet with access to updated knowledge about the risk landscape in the cyber security domain, as well as the opportunity to interact with other stakeholders to address cyberthreats and attacks.

Finanstilsynet also participates in NSM's collaborative forum for authorities responsible for supervising ICT security within their respective sectors. This forum is valuable for exchanging information and sharing experiences among regulatory authorities.

Security testing in the financial sector

Finanstilsynet and Norges Bank established a framework for cyber security testing in the financial sector in 2021, known as TIBER-NO¹² (Threat Intelligence-based Ethical Red-Teaming). This framework, based on the European Central Bank's TIBER framework, provides guidelines for testing financial institutions' ability to detect, protect against, and respond to advanced cyberattacks.

The framework aims to promote financial stability by increasing resilience against cyberattacks in institutions critical to the Norwegian banking and payment systems. Critical functions and the institutions responsible for these were identified in 2022. The first tests under the framework were conducted in 2023.

¹² Finanstilsynet's news item 21 October 2021: [Norges Bank and Finanstilsynet establish framework for testing of cybersecurity in the financial sector \(TIBER-NO\)](#) (Norwegian only).

Cooperation on framework for assessing systemic ICT risk

Given that systemic ICT incidents can jeopardise financial stability, Finanstilsynet collaborates with Norges Bank to develop a framework and a process for assessing systemic ICT risk. In this endeavour, recommendations and definitions from the European Systemic Risk Board (ESRB)¹³ and other relevant authorities will be considered and incorporated where deemed appropriate.

European cooperation and information exchange during cyber incidents

The European Systemic Risk Board (ESRB) published a strategy in January 2022 for reducing the risk of financial instability resulting from cyber incidents. It highlights the need to develop macroprudential tools that capture systemic cyber risk. The ESRB has established a working group (ESCG) tasked with mapping systemic cyber risk and assessing how a cyber incident could trigger a systemic crisis. Furthermore, the ESRB recommends that a European framework for coordination in the event of systemic cyber incidents (EU-SCICF) be established, in accordance with the provisions for cross-sectoral cooperation in DORA (Art. 49). The purpose is to facilitate rapid communication and coordination between supervisory authorities and other relevant bodies to prevent systemic failure in the event of a serious incident. While awaiting the establishment of EU-SCICF, ESCG has set up a forum for exchanging information on cyber incidents.

Cyber security roadmap for the financial industry

To address cyber threats and assist institutions in better complying with an increasingly complex and detailed regulatory framework in the ICT domain, the financial industry, through Finance Norway, has established a cyber security roadmap for the financial sector.¹⁴ The aim of this roadmap is to ensure that all actors, regardless of size, have equal capabilities for a robust cyber defence. A key aspect of this initiative is to develop a comprehensive approach to cyber security and establish appropriate forums for cyber security within the industry and/or with other sectors.

¹³ [Systemic cyber risk](#) 2020, [Mitigating systemic cyber risk](#) 2022, [Macroprudential tools for cyber resilience](#) 2023

¹⁴ [Cyber security roadmap for the financial sector](#) (see page 13) (Norwegian only)

4. FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS

Chapter 4 consists of three main parts. The first part addresses Finanstilsynet's supervisory activities concerning ICT and payment services in 2023 (chapter 4.1). The second part addresses the institutions' assessment of key aspects related to their ICT operations (chapter 4.2). The third part covers Finanstilsynet's summary of institutions' reporting on risk and vulnerabilities, in accordance with the Regulations on Payment Services Systems and the ICT Regulations (chapter 4.3).

4.1 Supervision of ICT and payment services in 2023

In 2023, 21 inspections focusing on ICT and payment services were conducted. Among these, ten were in banks, two in payment institutions, two in insurance undertakings, two in fund management companies, one in a debt collection agency, two in real estate agencies, and two in audit firms. Two of the inspections at banks were part of thematic inspections on anti-money laundering which encompassed the banks' systems for electronic monitoring of suspicious transactions.

Reports from the inspections have been published on [Finanstilsynet's website](#). Finanstilsynet will highlight the following topics:

Inadequate governance of ICT operations

In 2023, inspections revealed deficiencies in the institutions' overall management of ICT operations. At several inspections, it was pointed out that the institution's strategy, frameworks, and guidelines in the ICT domain, including security requirements, had not been considered by the board of directors, and that the reporting of ICT risks to the board was inadequate. Finanstilsynet emphasised the importance of clear and well-defined frameworks and guidelines to ensure that the institution operates in line with the board's risk tolerance. In some inspections of smaller financial institutions, Finanstilsynet found fundamental deficiencies in the management of ICT operations, such as a lack of documentation and procedures for compliance with the requirements of the ICT Regulations.

Inadequate follow-up of ICT risk in the second line of defence

During inspections in 2023, Finanstilsynet identified inadequate follow-up of ICT risk in the second line of defence¹⁵ in some institutions and questioned whether this function conducts sufficient independent controls of ICT. Finanstilsynet emphasised the importance of the second line of defence having adequate ICT expertise to control and set requirements for the first line of defence, including the ability to assess whether the IT security policy is operationalised.

Inadequate resources and expertise

At several inspections, Finanstilsynet questioned whether the institution has adequate resources and expertise in the ICT area in both the first and second lines of defence. Key person risk was also highlighted at some inspections.

¹⁵ Finanstilsynet's mention of three lines of defence in section 4.1 of [Risk and vulnerability analysis 2023](#)

Shortcomings in vendor management

Finanstilsynet found shortcomings in the institutions' follow-up of outsourced activities during inspections in 2023. Institutions must ensure that they have adequate expertise and procedures to monitor and verify that outsourced ICT activities meet the requirements of the ICT Regulations. It is particularly important to monitor service providers' change management and to verify that they comply with the institution's security requirements. Furthermore, Finanstilsynet pointed out that the assessment of service providers' compliance with the institution's requirements should also include second-line controls or audit reviews by the third line of the outsourced ICT activities.

Concentration risk

Finanstilsynet points out that high concentration risk, arising from the use of the same service provider for many or all applications, can render an institution particularly vulnerable to intrusions into its ICT infrastructure. This is especially relevant if the same access management system is used in all or in large parts of the institution's application portfolio. In such instances, it is imperative that the institution ensures, for instance, that production and administrative systems are segmented in a manner that prevents intruders from seizing control of the institution's entire ICT operations. Furthermore, the institution must ensure that users with strong privileges and broad access are subject to stringent requirements governing their usage.

Deficiencies in crisis preparedness

During inspections in 2023, several deficiencies related to crisis preparedness were identified. Some institutions had not analysed the consequences of interruptions to their operations and lacked adequate contingency solutions. Finanstilsynet also highlighted insufficient training, exercises, and testing of crisis preparedness, as well as the absence of emergency drills involving cyberattack scenarios.

Business impact analysis

Business impact analysis (BIA) is an analysis conducted to assess the potential impact of an incident on an institution's business processes and services. The analysis begins with the identification and evaluation of processes and services critical to the institution's operations. The assessment also involves identifying and classifying activities and resources necessary for business-critical processes and services. The analysis of the business serves as the foundation for the institution's business continuity and crisis plans. The institution must ensure that testing and exercises, including those involving outsourced operations, are based on the institution's business impact analyses to ensure continuity in critical business processes and services in the event of an adverse incident. The institution should establish procedures for conducting business impact analyses to ensure the continuity of business-critical services and processes.

Both the European Banking Authority's (EBA) guidelines on ICT security and risk¹⁶ and the European Insurance and Occupational Pensions Authority's (EIOPA) guidelines on ICT security and governance¹⁷ specify that institutions should develop a business impact analysis for their operations.

¹⁶ EBA: [Guidelines on ICT and security risk management](#)

¹⁷ EIOPA: [Guidelines on information and communication technology security and governance](#)

Incomplete access control and follow-up of logging

During inspections in 2023, Finanstilsynet found that several institutions had deficient procedures for monitoring employee access at service providers, including inadequate reporting from the service providers on this matter. Finanstilsynet also pointed out that the access granted to service providers to institutions' operating environments should be time-limited, allocated, and monitored for each assignment. Furthermore, Finanstilsynet pointed out that the institutions lacked procedures for monitoring logs of access activity.

Inadequate quality of the configuration management database

Several institutions utilise solutions to document changes in their systems, known as configuration management databases (CMDBs). If the information is of high quality and provides a sufficient level of detail, the CMDB can contribute to mitigating the risk associated with changes and enhance preparedness and continuity efforts. At several inspections in 2023, Finanstilsynet raised questions regarding the quality and level of detail in the institutions' CMDB solutions and whether the process for subsequent updates of the information was adequately automated.

4.2 Institutions' assessment of critical aspects related to ICT operations

Institutions and ICT service providers have highlighted several critical aspects related to ICT operations in discussions with Finanstilsynet.

Governance

Several institutions indicate an increased understanding of the importance of a well-functioning governance model in the ICT domain and are in the process of establishing such a model. As in 2022, institutions claim that their size impacts on their ability to establish an organisation with a clear division of first and second-line internal control tasks. Smaller institutions find it challenging to ensure compliance with all regulatory requirements.

Several institutions disclose weaknesses in the governance of outsourced ICT operations. While institutions receive reports from service providers according to contract, the content is not adequately reviewed, processed, or followed up within the institution. For instance, there is little assessment of whether the reports adequately cover the institution's service purchases.

Skills and skills management

Institutions report that it has generally become easier to recruit ICT expertise due to a less tight job market and weaker demand in the consulting industry. The availability of good candidates has improved, and the hiring of ICT specialists on a permanent basis has increased. However, institutions still highlight challenges in accessing and renewing expertise in older technologies. As a result, several institutions have initiated processes to transition to newer technologies. Many institutions also report increased internal understanding of the importance of ICT for the business and the opportunities ICT provides for business development.

Vendor management

The trend towards longer and more complex supply chains presents institutions with greater challenges in adequately managing their service providers. This requires increased resources, which is particularly demanding for smaller institutions. Furthermore, institutions sometimes struggle to gain acceptance for their strategies and policies among subcontractors. Several institutions have indicated that they use provisions in the forthcoming DORA regulation to tighten the requirements imposed on service providers and their deliveries.

Cybercrime

Institutions assess that phishing and ransomware pose the greatest threat to their operations. This is partly due to the increased sophistication of the methods used, making fraud attempts harder to detect for both the institutions and their customers.

With respect to cybercrime, it is mainly Distributed Denial of Service (DDoS) attacks that target internal systems directly. Institutions refer to such attacks as part of the 'normal noise' and state that they have robust solutions in place to handle such incidents.

Several institutions highlight insider threats as a new and growing risk. While cyber security within institutions has improved, fraudsters and malicious actors view recruiting of insiders as a method to bypass security measures. Such recruitment efforts may target both the institutions and their service providers.

Information leaks

Institutions emphasise the importance of classifying information and monitoring information sent via email or copied to external storage devices or private cloud services to prevent unauthorised access to information and mitigate potential harm to the institutions or their customers.

Classification

It is important for entities to classify their documents based on factors such as confidentiality and criticality, enabling them to establish solutions that help prevent data extraction or sharing.

ICT operations

The institutions report that operational stability has been good over the past year. Most of them report little change in operational deviations from 2022 to 2023. Incidents affecting operational stability have often arisen at service providers. Nevertheless, there have been some issues related to DDoS attacks and similar incidents, but these have had minimal impact on the availability of the institutions' solutions. Several institutions are working on cost-efficiency measures, including migrating their entire operating environment to cloud services, decommissioning legacy systems to reduce technical debt, or re-establishing internal expertise.

Geopolitical conditions

Institutions continue to place significant emphasis on country risk and other geopolitical factors in their risk assessments due to the global security situation. 2024 is election year in several countries with substantial ICT service exports, and the institutions will closely monitor the outcomes. Institutions have assessed that the risk associated with outsourced services from foreign providers, particularly those outside the EEA, has increased in recent years. If the risk is deemed to exceed the institution's established risk tolerance, service delivery has, in several instances, been brought back from abroad to providers in Norway or handled by the institution itself.

Emergency preparedness and crisis management

In discussions with institutions, it emerges that the lack of analyses of the consequence of a crisis, insufficient training and exercises in crisis management, shortcomings in testing crisis solutions, and inadequate crisis solutions can pose challenges for institutions in maintaining critical ICT services during severe disruptions at their usual operating sites. Monitoring preparedness solutions is challenging, particularly when institutions must develop and communicate the framework for testing these solutions to service providers. Several institutions have now established preparedness processes but will continue efforts to ensure that testing and exercises are at an acceptable level.

Change management

Lack of control over changes in operating configurations can lead to disruptions in critical business processes and expose the institution to cybercrime. Institutions have become more resilient through standardised procedures for managing changes, including those involving service providers. Smaller institutions state that they have less control over changes implemented by service providers and that long value chains complicate control processes.

With respect to the use of artificial intelligence (AI), institutions emphasise the importance of a cautious approach and the need for clear guidelines for the use of such solutions. Changes in AI solutions must be made in accordance with the institution's change management procedures to ensure that the risks associated with their use do not exceed the institution's established risk tolerance.

Access management

Lack of control and monitoring of extended access rights for employees and service providers' personnel can harm the institution due to intentional or unintentional operational errors. This can also lead to information leaks. Institutions consider it crucial to closely monitor service providers' access rights. Access is typically granted on a need basis to perform tasks, activities are logged, and there are alerts for activities outside the scope of the assignment. However, several institutions report that they do not always monitor service providers to the same extent as internal users with respect to the assignment and use of extended access rights.

Data quality

Inadequate or incorrect data can lead to analyses, controls, and decisions being made on incorrect or insufficient grounds. This may include errors in credit assessments, errors in controls to detect money laundering or fraud, and errors in risk assessments. All institutions emphasise the importance of data governance. Several institutions state that data collection and accurate data labelling are crucial for future value creation within the business, particularly when using AI.

4.3 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, in accordance with the Regulations on Payment Services Systems, Section 2 third subsection, cf. the ICT Regulations, Section 3. The risk reporting for 2023 included more institutions than in previous years. Some questions in the reporting form have been modified from previous years, and a new risk category, 'Very High', has been added¹⁸. For further details, please refer to Appendix 1.

Areas with the highest risk

In the reporting, institutions were asked to identify their highest perceived risks. Several institutions highlighted fraud where fraudsters obtain customers' Bank-ID as a major risk. Many also pointed to the danger of cyberattacks, with some referring to geopolitical factors. Complex infrastructure was also a significant concern for several institutions, particularly the challenge of maintaining oversight of supply chains and the difficulty in anticipating errors that may arise from changes. Some institutions also highlight challenges in retaining expertise and key personnel risk, particularly in connection with legacy systems.

Governance

The reporting indicates that most institutions generally estimate the risk associated with governance as low, also in 2023. Finanstilsynet has noted that a larger proportion of small and medium-sized enterprises (SMEs) than large enterprises assess the risk as moderate or high, which coincides with Finanstilsynet's experience from its supervisory activities.

More than three out of four institutions believe that their ICT systems provide a solid foundation for managing and controlling operations, that the risk analysis process is well-established, and that management has approved documented goals and procedures for ICT security. The majority of institutions report compliance with the principle of the three lines of defence. However, more than 40 per cent report that the risk is moderate or high when it comes to keeping an overview of the controls the institution relies on within the three lines of defence, broken down to controls that help ensure integrity, confidentiality, and availability. It is evident from the institutions' comments that they still have varying degrees of complete and uniform documentation of controls within the individual areas of responsibility and lines of

¹⁸ This category has been added so that the risk categories will correspond to the categories used when assessing the overall risk level and capital requirement (SREP) where relevant.

defence. Most of the institutions reporting moderate or high risk on this question indicate a positive or stable trend.

As in 2022, approximately three out of four institutions reported low risk associated with ongoing monitoring of service providers and deliveries with respect to the quality of delivery in 2023. Just under two out of three institutions assess that there is low risk associated with procurement competence. Although several institutions report resource and competence-enhancing measures during 2023, several also highlight dependence on external expertise, both technical, legal, and professional.

More than one out of three institutions believe there is moderate or high risk associated with missing or inadequate guidelines related to ICT security, including risk assessments of payment services and measures to protect users from identified risks. While the risk was assessed to be increasing in 2022, most consider it stable in 2023. The majority of institutions still believe there is low risk associated with adequate awareness and security training for employees.

Data protection

More than half of the institutions assess the risk associated with data protection as low. Several institutions consider the risk to be moderate or high with respect to the existence of robust guidelines for the classification and protection of structured and unstructured data. Institutions that assess the risk as high point out that data classification is either lacking or still in progress, and unstructured information is sorted manually.

The risk associated with segmenting the network into security zones based on a security classification of data and systems is the risk most institutions regard as high. Nevertheless, over half of the institutions assess this risk as low. One of the reasons why institutions assess the risk as high is that the network has not been segmented into zones, which has been deemed critical over time. One institution has assessed the risk as very high.

A significant majority of institutions also report low risk of unauthorised changes being made to the institution's systems, and of services no longer functioning as intended in 2023. When developing new solutions, the majority of institutions take the needs of all business areas into consideration. Institutions report low risk associated with securing data during both transmission and storage.

Institutions collect information on operations, transactions, and fraud, using this information to make services more secure and stable. The scope and impact of errors in applications and data affecting data integrity are both reported to be low.

Change management

Overall, change management is an area where more than half of the institutions consider the risk to be low. The risk associated with complexity in ICT systems is the one most institutions

consider high, with approximately half being banks, of which the majority are savings banks. At the same time, less than half of the institutions assess the risk as high or moderate.

About half of the institutions assess the risk of new regulatory requirements necessitating changes in systems as moderate or high. Institutions that assess the risk as high refer to a significant volume of new regulations with limited implementation time, including PSD2, AMLD, GDPR, and DORA. Furthermore, institutions mention that new regulations bring about new reporting requirements that necessitate updates to systems and procedures. The overall scope of requirements is also highlighted, along with the challenges of complying with many of these requirements.

Operations

More than half of the institutions assess operational risk as low. However, most institutions assess the risk that plans, processes, and procedures for continuity and recovery of critical ICT systems and services are not regularly reviewed, as moderate or high. Institutions that assess the risk as high indicate, among other things, that reviews are conducted only annually, but could be done more frequently, or that reviews are conducted on an ad hoc basis.

Approximately one-third of the institutions assess the risk associated with maintaining an up-to-date register of outsourced activities as moderate or high. The same assessment applies to whether there are sufficient resources and expertise in the second and third line of defence, including whether deliveries are regularly monitored. Institutions that assess the risk as high point to the increasing scope of outsourcing, a lack of resources or the presence of key person risk, and to the second line of defence lacking competence or being involved only in the largest contracts.

Security

More than half of the institutions assess the security risk associated with operations as low. However, most institutions assess the risk as high with respect to the lack of regular security testing of services. Institutions that assess the risk as high indicate that tests are either not conducted or not conducted regularly. Additionally, they point to the absence of penetration testing, the lack of other necessary tests, or the institution being unaware of to which extent tests are carried out as ICT is outsourced. Overall, however, fewer than half of the institutions assess the risk as moderate or high.

Approximately half of the institutions assess the risk as moderate or high that it will be challenging to access ICT security expertise, including the expertise needed to set requirements for service providers and monitor deliveries. Institutions that assess the risk as high point to a tight job market for skilled and appropriate ICT security professionals, making both recruitment and the hiring of consultants difficult. Furthermore, they indicate that duplicating security expertise in a small institution is challenging, which increases key person risk.

ID theft

Several institutions state that the risk of institution theft remained one of the highest risks for their operations in 2023. The risk associated with inadequate measures to prevent an attacker from taking over and misusing a customer's and/or a system user's ID is assessed by many as high and/or increasing. Especially, the risk of a fraudster taking over a customer's BankID is frequently mentioned. However, the overall risk level remains unchanged from 2022, indicating stability. The institutions report a strong focus on control measures, including anti-fraud initiatives, and the use of robust customer authentication methods.

Internal misconduct

Feedback suggests that institutions remained vigilant about this threat in 2023. The risk of internal irregularities was assessed by several institutions as one of the highest risks they face. Nevertheless, well over half of the institutions considered the risk of internal irregularities and misconduct scenarios to be low, representing a slight increase from 2022. The risk associated with inadequate logging and reporting is deemed to be low by two-thirds of the institutions, while one-third consider the risk to be moderate. This is somewhat lower than in 2022 when half of the institutions assessed this risk as moderate. Institutions utilise segregation of duty ('four eyes principle') wherever possible.

ICT support for anti-money laundering and counter-terrorist financing

Traditionally, money laundering and terrorist financing have been areas where institutions have acknowledged significant risk. However, unlike the reporting in 2022, institutions now perceive the risk of money laundering and terrorist financing to a lesser extent as one of the major risks.

For 2023, institutions generally assess the risk as moderate that ICT systems do not provide a comprehensive view of customers, customer relationships, and customer behaviour. Although some institutions refer to many false positive alerts, the risk associated with insufficient precision in flagging suspicious transactions has decreased from moderate to low in 2023.

Slightly fewer than one in three banks, mortgage companies, and finance companies believe there is moderate risk that transaction monitoring systems do not capture all payment transactions that should be investigated further. A few assess the risk as high, with some citing incidents resulting from errors in core system conversions.

A significant majority of institutions believe there is low or moderate risk associated with the AML systems' recognition of suspicious patterns over time. Unlike in the 2022 reporting, none of the institutions in 2023 assessed the risk as high that the sanction screening system lacks high precision in matching listed individuals and institutions. Four out of five institutions assess the risk as moderate.

Other observations

In the reporting, several institutions have indicated that certain statements are not relevant to them. Finanstilsynet agrees with the assessment for several of these statements, but for others, Finanstilsynet believes that the statement is relevant for all institutions. For example:

- 21 institutions have responded that the risk associated with challenges in accessing ICT security expertise, including the expertise needed to set requirements for service providers and monitor deliveries, is not relevant.
- 32 institutions have responded that the risk associated with whether an adequate regular awareness and security training programme is implemented for employees, is not relevant.
- 19 institutions have responded that the risk associated with regular testing of service security (e.g. penetration testing, testing according to internationally recognised standards, vulnerability scanning) is not relevant.

It is possible that the institutions responding that the statement is not relevant to them assumed that it poses no risk. However, it is important to note that the risk must be assessed even when ICT is outsourced, as the institution still bears responsibility when ICT is fully or partially outsourced.

5. FRAUD

Payment service providers, i.e. banks, credit institutions, electronic money institutions and payment institutions, and branches of such institutions headquartered in other EEA states, report fraud statistics to Finanstilsynet every six months. The results and trends are presented in separate [reports on Finanstilsynet's website](#). Some key findings from 2023 are described below.

In 2023, there was a significant increase in total losses compared to previous years, as shown in table 5.1. The increase in losses from 2022 to 2023 amounted to NOK 314 million, representing approximately 51 per cent. The largest increase in losses was observed in fraud involving account transfers, around 64 per cent. For fraud involving the use of payment cards, the increase was approximately 28 per cent. When measured as a proportion of total transaction value, total losses amount to 0.0014 per cent, which is consistent with the previous year.

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 the card issuer	Total losses
2023	647	281	928
2022	395	219	614
2021	347	162	508

Source: Finanstilsynet

Market participants are actively working on anti-fraud measures to detect and prevent fraud. Banks intercept a significant portion of fraud attempts, and in total, prevented losses amounting to NOK 2,072 million in 2023, with account transfers accounting for NOK 768 million and card payments for NOK 1,303 million.

There are several fraud methods, and vulnerabilities are exploited. For example, inadequate configuration of email settings can allow fraudsters to send emails impersonating financial institutions.¹⁹ The extensive use of BankID and various login contexts can lead to a form of 'fatigue' in the user's critical judgment during BankID logins.

In addition to the fact that automation and streamlining have led to faster transfers of defrauded amounts, fraudsters are continually developing new methods of fraud. So-called 'safe account' fraud, which has been used in Sweden and Denmark, also took place in Norway in 2023. In this scam, the victim is contacted by the fraudster, who pretends to be from the bank or the police and is told that unauthorised persons have accessed their bank account. The victim is then instructed to move their funds to a 'safe' account supposedly belonging to the bank or the police but actually controlled by the fraudster. If the fraudster claims to be from the police, the victim is informed that the bank must not be notified as there is an ongoing police investigation.

¹⁹ [Inadequate configuration of email settings](#) (Norwegian only)

New technologies such as artificial intelligence and 'deepfake' are increasingly being used by fraudsters. So far, their use has been linked to making fraud methods more credible through improved language, more convincing content, and voice impersonation. It is reasonable to assume that the use of such tools will continue to increase.

A higher number of fraud-attempts and increased losses have societal consequences and are burdensome for the customers who fall victim to fraud. It is crucial that the public maintains trust in both electronic communication and electronic payment services. This requires service providers to continue developing effective anti-fraud measures. Fraud involving account transfers where the fraudster initiates the payment, has been reduced to nearly zero after service providers implemented targeted measures.

In addition to measures implemented by individual institutions, the industry and the authorities must collaborate to address these challenges. Banks, Finance Norway, telecom operators, and authorities regularly warn the public about current fraud methods. In Finance Norway's report 'Secure consumers', the financial sector has proposed implementing various anti-fraud measures under the auspices of either the banks themselves, BankID BankAxept A/S, or Finance Norway.²⁰ The Norwegian Communications Authority (Nkom), Økokrim (the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime), and Finance Norway have established a national expert group to prevent digital fraud, focusing on voice telephony and SMS communication.²¹

A common denominator in many fraud attempts in Norway is the use of electronic communication fraud (e.g. phishing) and telephone fraud (vishing).

The European Banking Authority (EBA) has analysed reported fraud data and published an opinion on April 29, 2024, with recommendations to further strengthen provisions related to anti-fraud in the proposed Payment Services Regulation (PSR) and the Third Payment Services Directive (PSD3)²².

²⁰ [The financial industry's anti-fraud efforts](#) (Norwegian only)

²¹ [Nkom, Økokrim and Finance Norway's expert group on cyber fraud](#) (Norwegian only)

²² [EBA's opinion on fraud mitigation](#)

6. INCIDENT REPORTING

According to the ICT Regulations, operational or security incidents are required to be reported to Finanstilsynet without undue delay. Incident reporting plays a crucial role in ensuring an accurate and timely assessment of the risk level in the financial sector and in uncovering patterns and connections that may be challenging for individual institutions to detect. Also in 2023, certain incidents were specifically monitored by Finanstilsynet.

However, the most crucial aspect lies in how the individual institution, along with its service providers, manages incidents to ensure swift recovery and follows this up with relevant preventive measures. Moreover, the institution must ensure that appropriate actions are taken by the service providers when they are responsible for the incident.

6.1 Increase in reported incidents

Institutions reported 408 ICT incidents to Finanstilsynet in 2023, which marks an increase of approximately 40 per cent from the previous year, as shown in Fig. 6.1. The increase was mainly attributed to more incidents affecting multiple institutions simultaneously, and ten incidents across different service providers were the basis for 95 reports to Finanstilsynet. These incidents included errors in balances, deficiencies in AML systems, deviations in BankID, or the same logical application errors.

Out of the 408 reported incidents, 15 were security incidents, while the rest were operational incidents.²³

Fig. 6.1 Number of reported ICT incidents



²³ Security incidents are defined as intentional events, i.e., events where the purpose is to harm/attack. Operational incidents are defined as unintentional events caused by errors or deficiencies.

For further information about the figures, see appendix 4. Source: Finanstilsynet

Certain banks were affected by incidents resulting in limited access to parts of the payment services for 5–11 hours. However, overall, there were few incidents resulting in more than three hours of downtime for payment services.

Many incidents led to customers experiencing incorrect balances in their accounts due to duplicated or missing transactions. These incidents occurred at service providers utilised by several banks, and each of them was reported by multiple banks. Finanstilsynet considers incidents resulting in incorrect balances, where customers cannot rely on their account statements, as particularly serious. Correct account balances were not restored until several days later. Most of these transactions were associated with instant payments. There were also some such transactions related to card payments, including the incident involving duplicated Visa and Mastercard transactions that affected several banks after Easter 2023.

6.2 Security incidents

There were 15 reported security incidents in 2023, which is slightly fewer than the previous year. Some of these incidents were serious for the affected institutions, but none of them impacted the financial infrastructure or had severe consequences for the major financial institutions.

Six of the incidents were Distributed Denial of Service (DDoS) attacks reported by various institutions at different times.

Several incidents involved attacks on foreign subcontractors in the value chain. Vulnerabilities in software were exploited to gain access to the subcontractor's systems, and ransom was demanded to unlock the systems or refrain from publishing or stealing data. Such incidents are challenging to handle even for the institutions indirectly targeted through their subcontractor. It is necessary to thoroughly examine servers and systems to determine if the compromise at the subcontractor may have spread. None of the incidents in 2023 had serious consequences for the Norwegian financial institutions using services from the subcontractors that were attacked.

Two of the security incidents involved compromised email accounts used as a basis for fraud or to send spam.

One bank reported an incident where the bank discovered a security vulnerability in its own systems that had been exploited. Fraudsters exploited a delay in the updating of balances to transfer funds from accounts created for fraudulent purposes while simultaneously withdrawing cash from the same accounts, resulting in overdrafts. The fraudsters were arrested.

6.3 Acceptance test of changes carried out by service providers

A number of incidents were reported concerning errors in solutions following planned changes implemented by service providers. The errors were associated with interest calculations, reminder fees, and other charges, cost calculations for loans, notification letters, tokenisation of payment cards, and coding in AML systems. These errors should have been detected during the testing process and underscore the importance of thorough testing by service providers, acceptance testing, and internal controls within institutions. Each institution is responsible for its systems and services, regardless of whether they were developed by the service provider or the institution itself.

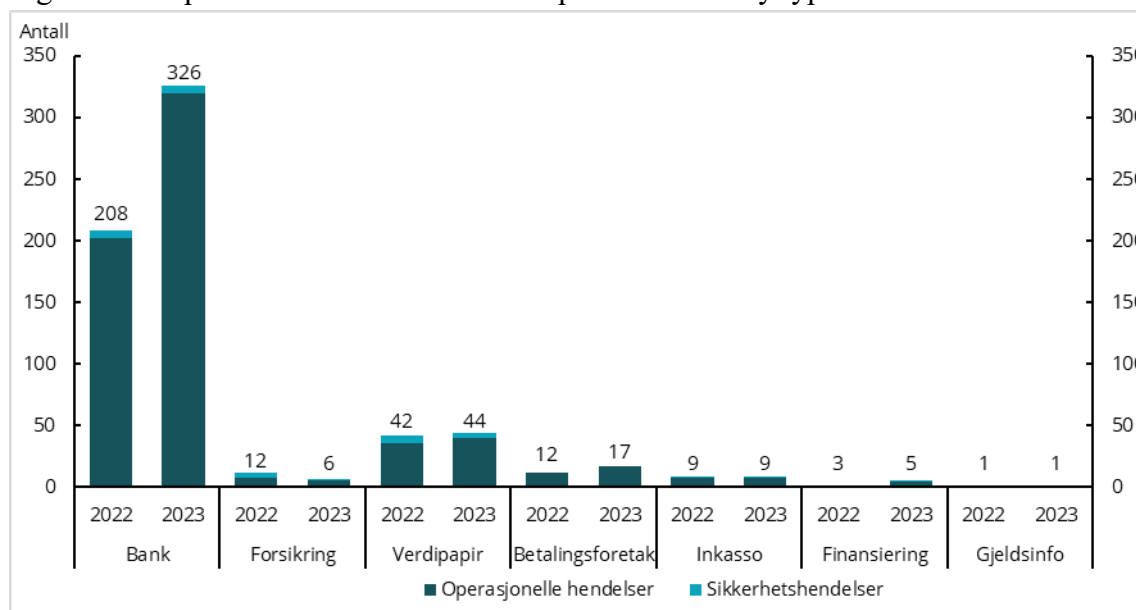
6.4 Incidents in systems for detecting money laundering and terrorist financing

In 2023, there were 26 reported incidents concerning deviations in institutions' electronic solutions for transaction monitoring to detect money laundering and terrorist financing. Several of the reported incidents were caused by the same error from a common service provider. Often, the reason for deviations is that changes have led to incorrect labelling of transactions, causing them not to be monitored based on the correct rule sets. Particularly common are errors or missing labels on international transactions, causing them to be monitored as domestic transactions. There were also incidents where transactions were inadvertently no longer subject to transaction monitoring due to mergers or the transition to new systems. None of the incidents in 2023 revealed a lack of monitoring over several years.

6.5 Incidents by type of institution

Figure 6.3 provides an overview of the number of incidents by type of institution, divided into operational incidents and security incidents. The incidents are described in further detail below.

Figure 6.3 Reported incidents in 2023 compared to 2022 by type of institution



Source: Finanstilsynet

Banks

The increase in the number of reported incidents in 2023 was primarily attributable to a higher number of reports from banks. Several banks submitted their own reports, and many reported the same incident involving a common service provider. While there were fewer severe incidents affecting the availability of payment services, there was a significant increase in incidents resulting in incorrect account balances.

Incidents with incorrect balances on customer accounts

Finanstilsynet received 60 reports regarding incorrect balances on customer accounts. Six of the reports concerned incidents that affected only one institution, while 54 of the reports pertained to six incidents occurring at different service providers. Seven of the incidents were related to instant payments, three to card payments, and two to other issues involving duplicated files. In many of the incidents, it took several days before the balances were corrected. Finanstilsynet considers incidents resulting in incorrect balances to be particularly serious.

Card payments

Capacity issues arose in handling Visa and Mastercard transactions after the Easter holidays in 2023. This led to duplicate transactions and incorrect balances on customers' accounts.

Instant payments

Operational errors related to instant payments accounted for a significant increase in incidents resulting in incorrect account balances. The cause appears to be operational issues such as lack of completeness checks on the number of files, incorrect sequencing of file runs, lack of procedures for interruptions in batch runs, database issues, and certificate problems.

For Finanstilsynet, it appears that the relevant operating environments are struggling to handle deviations due to the increased complexity associated with operating instant payments, where payments require instant settlement. This has increased the risk of serious errors. According to Finanstilsynet's assessment, institutions must implement measures to improve operating procedures and training to ensure the secure operation of instant payments. Finanstilsynet will follow up on this with the relevant actors as part of its ongoing supervision.

Payment institutions

The majority of the 17 operational incidents reported by payment institutions were from Vipps. The main cause of most incidents was issues with access for some or all customers to some or all services. Some of the reported incidents were due to non-conformances at banks and therefore coincided with similar reporting from one or more banks. This particularly applied to three incidents related to instant payments, where issues in the interface between Vipps and the bank(s) resulted in delays and duplicated transactions, leading to multiple reports from the banks.

Securities

In 2023, approximately half of the 44 reported incidents in the securities area were related to the central securities depository Euronext Securities Oslo (VPS) and the regulated marketplaces. None of them were particularly severe. Three incidents resulted in delayed securities settlement. Other incidents were related to errors in account labelling, settlement notices, cancellation of settlement instructions, instrument registration, dividend payments, product issues, or breaches of confidentiality in reporting. The remaining reports on operational incidents in the securities area were dominated by problems with access to online trading of financial instruments and short service disruptions related to services on the marketplaces. Four security incidents were reported in the securities area, three of which were attacks on subcontractors and one was a DDoS attack.

Insurers

Six incidents were reported by insurers and pension funds. This included one security incident and five operational incidents affecting customer access to web or telephony services.

For a long time, Finanstilsynet has received relatively few incident reports from insurers and has questioned whether the industry's understanding of the reporting obligation under the ICT Regulations is adequate. After Finanstilsynet sent a letter to insurers in 2024 with examples of incidents that should be reported, the number of reports has increased.

Debt collection agencies

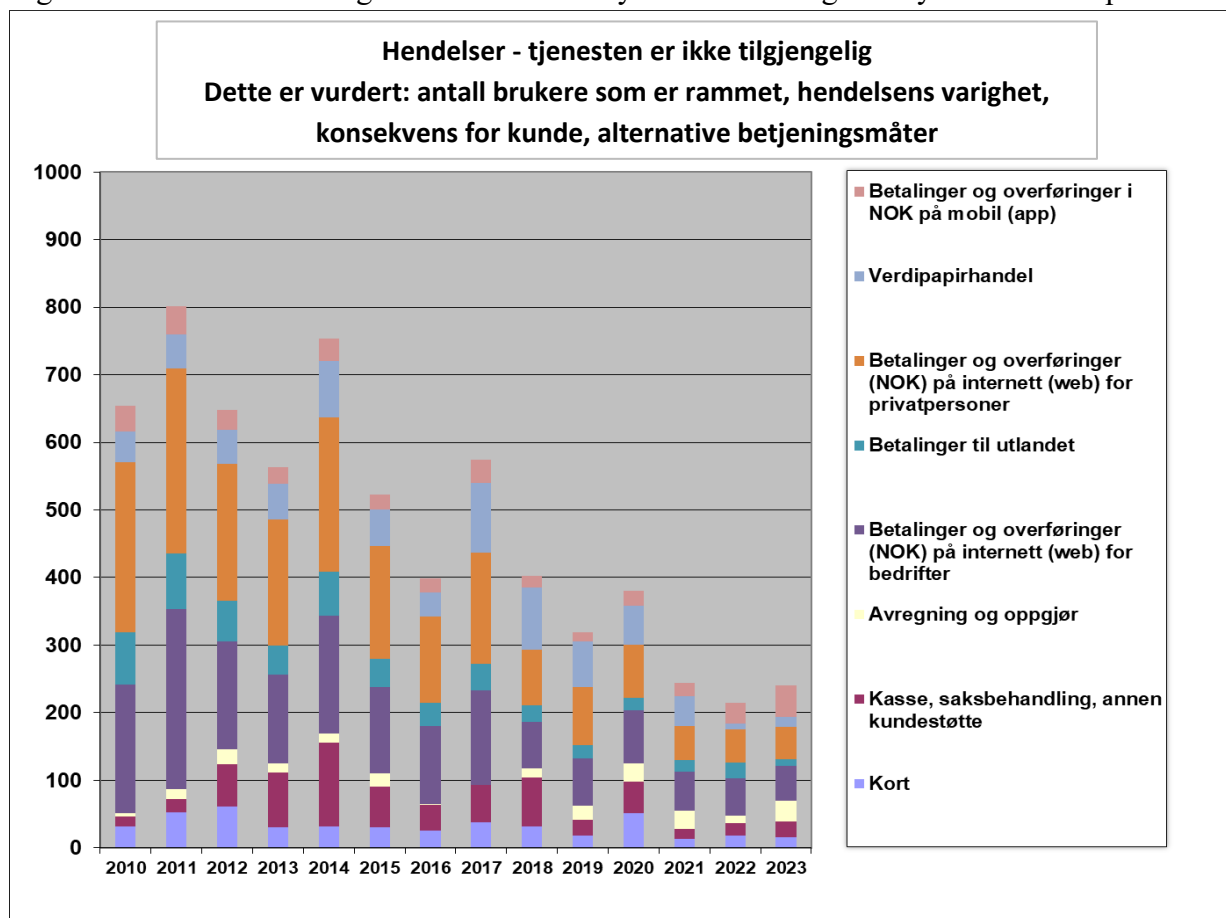
Incidents reported by debt collection agencies arose following system changes, leading to deviations in their case processing with errors related to payment deadlines or invoiced amounts, or breaches of confidentiality where customers could see other customers' data. There was one security incident in which a subcontractor was attacked through the exploitation of a software vulnerability.

6.6 Analysis of incidents as a measure of availability

The reported incidents vary in severity. For incidents that resulted in reduced availability of payment services and customer services, Finanstilsynet evaluated and weighted the incidents based on the timing and duration of the disruption, the number of affected institutions, the number of impacted customers, and whether alternative services were available to meet customer needs. When considering alternative services, for instance, the availability of internet-based services is assessed if mobile app services are not functional. It is also considered that the alternatives may not offer the same range of services, for instance that mobile payment solutions often do not provide all the services available through web-based solutions. The weighting of incidents produces an index represented on the vertical axis in figure 6.4. The findings are compiled into a time series to track developments over time.

Figure 6.4 shows that the availability of payment services and customer solutions is assessed as largely unchanged from 2022 to 2023. The overall availability of services in 2023 was somewhat lower than in 2022 and comparable to 2021. Despite this, the overall availability of services in 2023 is considered satisfactory.

Figure 6.4 Incidents causing reduced availability for users. Weighted by estimated impact*



* The vertical axis scale is an index based on the weighting of each incident. A lower index value indicates a lower occurrence of operational disruptions with consequences for users. For more detailed information on the data used, see appendix 4. Source: Finanstilsynet

The figure shows an increase in deviations within the category 'Clearing and settlement', which are deviations occurring after the payer has registered the payment. These include issues related to double transactions, reservations not processed at the correct time, and banks failing to meet clearing deadlines. These deviations can result in incorrect available balances for customers, making their funds inaccessible.

The category 'Retail banking via mobile app (NOK)' also shows reduced availability. This is partly explained by the substantial increase in mobile payments compared to internet banking payments, meaning that deviations in mobile apps have a more significant impact on the assessment.

Deviations caused by expired certificates also led to service outages.

6.7 Incidents related to dedicated PSD2 interfaces

Both account servicing payment service providers and payment service providers are required by regulations to report to Finanstilsynet any issues with dedicated interfaces for third-party service providers' access to customers' payment accounts. In 2023, DNB provided weekly updates on its dedicated interface, including any issues with availability or functionality. Other banks reported any problems with the interfaces, whether related to availability or functionality. Third-party service providers also frequently reported observed downtime and lack of functionality in banks' dedicated interfaces. Lack of functionality was specifically addressed with account servicing payment service providers based on reported deficiencies. Finanstilsynet has, on the basis of its follow-up of reported deficiencies, [published clarifications and explanations regarding the regulations](#) (Norwegian only).

7. Outsourcing

In 2023, Finanstilsynet also received a significant number of notifications regarding outsourcing. Similar to previous years, these notifications indicate increased use of cloud services for both application and infrastructure services. Outsourcing often leads to an increase in the number of platforms that institutions need to manage, which can result in greater complexity and a more intricate risk landscape.

The risks associated with the extensive use of ICT service providers constitute a substantial portion of the institutions' ICT risk. In 2023, several inspection reports highlighted deficiencies in the monitoring of outsourced ICT operations. Finanstilsynet considers vulnerabilities related to vendor management to be among the highest risks in the institutions' ICT operations, with the risk level deemed higher in 2023 than in previous years.

7.1 Follow-up on outsourced ICT

The financial sector has outsourced a significant part of ICT operations to service providers, who in turn often rely on one or more subcontractors. This can result in longer and more complex supply chains that are vulnerable to attacks or operational failures. Such supply chains impose greater demands on institutions during contract negotiations and require ongoing monitoring and control of outsourced ICT activities, including the use of subcontractors.

Prominent service providers often have more resources and higher expertise to develop robust solutions compared to smaller providers and the institutions themselves. These prominent providers can help reduce costs and exposure to technical errors and attacks for the institutions, although the concentration risk increases when many institutions depend on the same provider for critical financial services.

Institutions outsource activities to a considerable number of ICT service providers and data centres. The increase in the number of service providers heightens the complexity of interactions, particularly during incidents and in the monitoring and control of outsourced activities.

The fundamental principle for overseeing and controlling outsourced ICT operations is that the institution (the principal) must manage these outsourced activities as if they were conducted by its own organisation, in accordance with, among other things, Sections 2 and 12 of the ICT Regulations. The institution's responsibility for overseeing outsourced ICT operations applies both to external outsourcing and where services are outsourced to another institution within the group or alliance, with the group's or alliance's ICT function acting as the service provider (referred to as internal outsourcing). Specific and detailed requirements for institutions' oversight of ICT service agreements, including outsourced ICT operations, are

also outlined in chapter V, 'Managing of ICT third-party risk'²⁴, in the Regulation on Digital Operational Resilience (DORA) along with associated regulatory technical standards.

Based on observations from its supervisory activities, Finanstilsynet's assessment is that institutions do not sufficiently fulfil their responsibility for overseeing and controlling outsourced ICT operations. Below are Finanstilsynet's expectations regarding institution's control measures for overseeing ICT outsourcing^{25,26}.

7.2 Model for overseeing and controlling outsourced ICT operations

The ICT Regulations require that the institution establishes overarching goals, strategies, and security requirements for its ICT operations, as well as describes how the institution will ensure its ICT deliveries. Finanstilsynet expects ICT service providers and deliveries to be systematically and regularly followed up through forums at operational (day-to-day monitoring), tactical (contractual follow-up), and strategic levels (business-level monitoring). To ensure effective governance of outsourced ICT operations, clear responsibilities need to be defined across these three levels, both within the institution and between the institution and the ICT service provider. Clear guidelines for communication and escalation will be necessary to ensure correct and efficient processes. Such procedures should apply to both internal and external ICT outsourcing. The main intention behind the monitoring of ICT outsourcing at these three levels is to ensure holistic governance.

Regular meetings at a *strategic level* between the institution's management (client) and the management of the ICT service provider should be held to ensure that the service provider will support the institution's long-term goals and strategies, thus ensuring predictable ICT deliveries. The purpose of such meetings would typically be to present the institution's plans and expectations, the service provider's business model, changes in the business model, and any changes in ownership that may affect future ICT deliveries.

Meetings at a *tactical level* between the institution and the service provider should be held to ensure that ICT services are delivered according to agreed frameworks and requirements (SLA²⁷), and to ensure that agreements on ICT outsourcing can be continuously adapted to the institution's changing needs. Examples of other topics in such meetings include a review of the risk associated with the ICT outsourcing, the contractor's compliance with the institution's security requirements according to the institution's security policy, and the service provider's handling of the institution's requirements for continuity in case of disruptions in ICT service delivery.

²⁴ [DORA, Chapter V, 'Managing of ICT third-party risk'](#)

²⁵ [First Batch of technical standards](#)

²⁶ [Second Batch of technical standards](#)

²⁷ Service Level Agreement (SLA)

At an *operational level*, the focus is on the daily monitoring and control to ensure that ICT service deliveries are in line with contractual arrangements. Here, the institution must ensure that a delivery manager is appointed at the service provider's end, and that reporting, and escalation procedures are established to ensure prompt handling of deviations in ICT service deliveries. The need for follow-up meetings for the daily monitoring must be clarified on an ongoing basis.

7.3 Monitoring and control of outsourced IT operations

In daily operations, the first line of defence is responsible for managing ICT outsourcing, cf. the governance model based on the three lines of defence²⁸, stipulating that management of ICT risks and the control of ICT outsourcing shall be based on documented operational procedures, as per Section 2 of the ICT Regulations. Finanstilsynet expects the management and control of ICT outsourcing to be included in the annual internal control certification. This will ensure robust management and control of the institution's outsourced ICT operations.

Major ICT service providers often develop, either independently or with the assistance of external parties, reports on the maturity of ICT processes and controls, such as ISAE 3402²⁹. Through its supervisory activities, Finanstilsynet has found that such reports do not always provide an accurate picture of the situation. In Finanstilsynet's opinion, maturity reports prepared by ICT service providers can be a good starting point for the risk-based assessment by the second and third line of defence of the need for controls. When institutions use such reports, it must be verified that the reports adequately cover the institution's ICT service purchases, or whether there is a need for additional and expanded controls at the ICT service providers. If weaknesses highlighted in such reports persist over years, the institution should pay particular attention to these.

Below are two tables outlining aspects that can serve as a basis for the institutions' monitoring and control. The first table covers aspects that the institution should have control over in its own operations, while the second table covers aspects related to service providers and subcontractors.

²⁸ Finanstilsynet's [Risk and vulnerability analysis 2023, Section 4.1](#)

²⁹ ISAE 3402 is an independent verification of processes and controls at the ICT service provider that is intended to secure financial information.

Table 7.1 Examples of aspects that the institution should have control over in its own operations

Internally within the institution (principal)	Description
Risk management	Assess and manage the risk associated with dependence on the service provider and its subcontractors and maintain an overview of alternative ICT service providers and ICT systems available for the outsourced ICT operations.
ICT strategy	Assess whether the outsourced ICT services provided by the service provider and its subcontractors are in alignment with the institution's own business and ICT strategy.
Security testing	Assess whether the first line has ensured sufficient vulnerability and penetration tests, as well as other types of security tests, at ICT service providers.
Continuity testing	Assess the level of contingency and continuity testing of critical and important processes both at ICT service providers and of outsourced ICT services.
Industry-wide services	Ensure that outsourced industry-wide ICT services, provided by institutions such as Bits, Vipps, and Finance Norway Insurance Operations (FNF), are monitored as outsourced ICT.
Agreements	Ensure that ICT outsourcing agreements give the institution the right to be consulted before ICT subcontractors are replaced, and that the institution is guaranteed access to any documentation from a due diligence review that can be used when considering the replacement of ICT subcontractors.
Inspection/control/supervision	Ensure sufficient transparency with subcontractors in accordance with the ICT Regulations Section 12.
Governance	Ensure that adequate mechanisms are established for governance of outsourced ICT addressing the increased complexity that the use of ICT subcontractors may entail.
Requirements and policies	Ensure that the institution's requirements and policies are adhered to in ICT outsourcing arrangements.
Quality	Ensure that the institution maintains control over the quality of ICT deliveries both from ICT service providers and ICT subcontractors, as this can directly impact user experience and the institution's reputation.
Assess the need to conduct independent audits at service providers and subcontractors (see next table)	The second and third line of defence should assess the need to conduct their own ICT audits at ICT service providers and their ICT subcontractors on selected topics, rather than rely uncritically on the service provider's reporting.

Source: Finanstilsynet

Table 7.2 Examples of aspects at service providers and subcontractors the institution should have control over

With contractors - ICT service providers - ICT subcontractors	Description
Governance	Ensure that adequate governance is established.
Risk management	Ensure that adequate risk management is in place.
Incident/response	Ensure that an appropriate regime is established to respond to various types of incidents at the service provider and its subcontractors, so that the principal can report any reportable incidents to Finanstilsynet in accordance with the ICT Regulations Section 9 and Finanstilsynet's Circular 15/2009.
Continuity testing	Ensure that the institution's recovery requirements (RTO/RPO/MTPD) ³⁰ are met and documented in reports from completed contingency and continuity tests for critical and important processes.
Security testing	Ensure that sufficient vulnerability and penetration tests, as well as other types of security tests, are conducted.
ICT security policy	Ensure that the requirements of the institution's ICT security policy are upheld.
Change management	Ensure that the quality of change management is upheld. The institution should, among other things, keep track of the number of errors resulting from changes.
Risk and threat monitoring	Ensure that adequate risk and threat monitoring is established.
Access management	Ensure that systems and procedures for Identity and Access Management (IAM) ³¹ are established.
Logging	Ensure that the established system and application logging is of sufficient scope and quality.

Source: Finanstilsynet

³⁰ **RPO (Recovery Point Objective):** A measure of how much data a company can lose before experiencing issues due to data loss.

RTO (Recovery Time Objective): The amount of downtime that can be tolerated before services must be restored to normal.

MTPD (Maximum Tolerable Period of Downtime): The maximum amount of downtime a company can accept.

³¹ **Identity and Access Management (IAM):** A framework consisting of procedures, policies, and controls designed to ensure governance of users and their access rights.

8. ASSESSMENT OF THE FINANCIAL INFRASTRUCTURE AND INSTITUTIONS' IT OPERATIONS

8.1 The financial infrastructure is robust

Finanstilsynet considers the Norwegian financial infrastructure to be robust. Institutions' services appear to be well protected against attacks. In 2023, there were no major IT incidents affecting financial stability, although some incidents garnered significant attention, as discussed further in section 6. The institutions' operational stability was satisfactory and is assessed to be approximately on a par with the previous two years.

More incidents were reported in 2023 compared to 2022. This increase was mainly due to some incidents affecting multiple institutions simultaneously. The proportion of security incidents was lower than in 2022, while there was a certain increase in operational incidents. Based on the incidents' duration, timing, and the number of affected users, Finanstilsynet has assessed the availability of payment services and other customer services to be roughly at the same level as in the previous two years, see section 6.6.

In 2023, regularity in the clearing and settlement systems was generally good, despite a few individual incidents. The regularity of the communication with the international payment and securities transfer notification network, SWIFT³², and the international settlement system, CLS³³, was also good.

Although attacks on the financial infrastructure were fewer in 2023 than in 2022, the extent of cybercrime impacting the financial sector continues to increase. Notably, there was a significant rise in phishing and vishing (telephone fraud), such as 'secure account' scams. So far, cybercrime has not led to systemic crises or severe incidents within firms in the Norwegian financial sector.

In 2023, there were security incidents at service providers that affected the institutions concerned. Vulnerabilities and security breaches pose risks such as information leakage or unauthorised changes in the systems and infrastructure of institutions or their service providers. Institutions must also contend with a continuously evolving cyberthreat landscape, influenced in part by Russia's invasion of Ukraine and the conflict between Israel and Hamas.

A digital incident can occur suddenly, leading to a breakdown in the financial infrastructure and having far-reaching societal consequences. Institutions' efforts in the ICT domain, both to

³² SWIFT'S website: [About us](#)

³³ CLS' (Continuous Linked Settlement) [website](#) – A US financial institution that provides settlement services to its members in the foreign exchange (FX) market.

reduce the likelihood of disruptions and to enhance ICT security in general, help ensure stable operational solutions, prevent cybercrime, and mitigate the impact of incidents. This includes crisis solutions and preparedness, recovery plans, and IT security work, including defences against cybercrime.

8.2 Risks associated with vulnerabilities in institutions' ICT operations

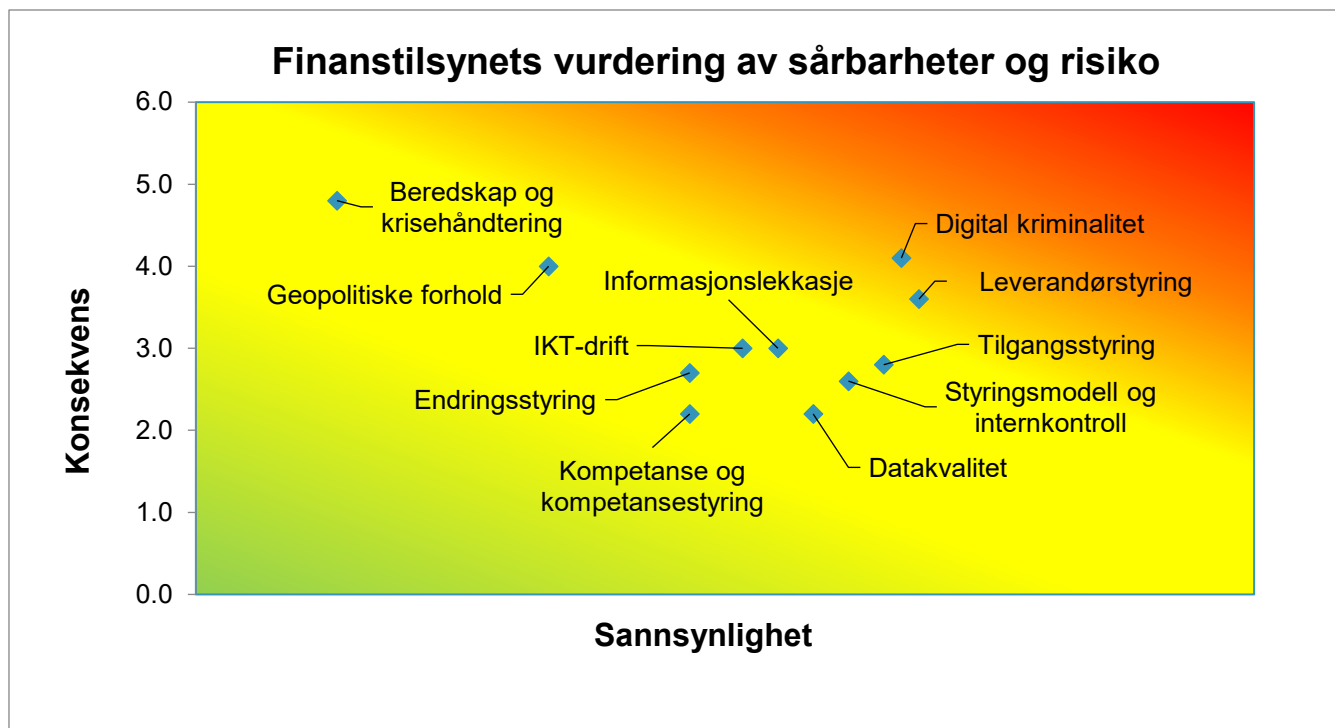
Figure 8.1 summarises Finanstilsynet's assessment of the most critical vulnerabilities in the financial sector. These vulnerabilities are classified based on the likelihood of a severe adverse incident occurring and the severity of the resulting consequences for each institution. The observations and assessments underlying this classification are detailed in table 8.1 and further discussed in appendix 2.

Finanstilsynet regards vulnerabilities related to institutions' defences against cybercrime as the most critical risk associated with their use of ICT in 2023, with the overall risk deemed to be high. Examples of such vulnerabilities include serious weaknesses in defence mechanisms that remain undetected due to inadequate security testing. The cyberthreat landscape suggests that such vulnerabilities will be exploited by malicious actors, potentially having severe consequences for the institution.

Vulnerabilities associated with vendor management, governance models, internal control, and access management are also significant risks, with the overall risk considered moderate to high. These vulnerabilities may arise from ambiguity in roles between the institutions' first and second lines of defence and the compliance function's failure to identify weaknesses. Experience from inspections has shown examples of inadequate follow-up of ICT risks in the second line of defence, and inadequate controls of the quality and robustness of solutions have been the cause of some of the reported incidents. This suggests that the risk associated with inadequate vendor management, governance models, and internal control is considered somewhat higher in 2023 than the previous year. With respect to access management, the risk is assessed as lower than last year due to increased attention from institutions and measures implemented by the industry.

Risk associated with vulnerabilities in institutions' preparedness and crisis management, as well as geopolitical factors, is considered moderate to high. For vulnerabilities related to institutions' change management, information leaks, ICT operations, skills and skills management, and data quality, the risk is assessed as moderate. The risk associated with geopolitical factors is considered higher in 2023 than the previous year. For institutions' follow-up of competence and competence management, the risk is considered somewhat lower in 2023 than the previous year, and the same applies to the risk associated with following up information leaks.








Figure 8.1 Finanstilsynet's assessment of vulnerabilities and risks for 2023



Source: Finanstilsynet

Table 8.1 Vulnerabilities that could represent a risk of adverse incidents

Area	Vulnerabilities that may represent a risk for adverse incidents (The degree of risk, probability, and consequence are shown in Figure 8.1)	Trend
Governance and internal control	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.	↗
Skills and skills management	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 skill needs. Problems and errors that occur may be difficult to resolve. Dependence on foreign assistance may increase.	→
Vendor management	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.	↗
Cybercrime	Inadequate security testing, security updates, training and awareness 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 institution.	
Information leaks	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.	
ICT operations	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.	
Emergency preparedness and crisis management	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.	
Geopolitical factors	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.	
Change management	Development at a fast pace, 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 configurations within operations may result in interruptions to critical business processes and the institution being exposed to cybercrime.	
Access Management	Inadequate control and monitoring of extended access rights for employees and service provider personnel may harm the institution and its customers due to information leaks and deliberate or unintentional operational errors	
Data quality	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. THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

Regulation (EU) 2022/2554 on digital and operational resilience in the financial sector (DORA)³⁴ was adopted by the European Parliament and the Council of the European Union in November 2022. The regulation will apply in the EU on 17 January 2025. The proposed regulation is considered EEA-relevant. In Norway, the Ministry of Finance has proposed to implement DORA through a new act on digital operational resilience in the financial sector. The proposal has been subject to consultation.³⁵ A bill will later be submitted to Stortinget (Norwegian parliament) for consideration. In parallel, DORA is being assessed for inclusion in the EEA Agreement. Finanstilsynet advises institutions to prepare for DORA to take effect in Norway in 2025, although several unresolved issues may delay implementation.

In addition to the regulation, ten regulatory and implementation technical standards (RTS and ITS) as well as some guidelines will be developed. This work is ongoing in the EU and expected to be completed by the end of 2024, whereby they will also apply from 17 January 2025. In Norway, a delay is expected due to the EEA process. As of May 2024, the first RTSs have been submitted to the Commission for processing and are expected to be adopted with minor adjustments. Additionally, technical reporting solutions will be developed.

The regulation will strengthen the requirements for institutions in the financial sector, even though current Norwegian regulations and supervisory practices are based on the same principles as the new requirements. Institutions that currently comply with the requirements in existing regulations and relevant guidelines are well-positioned for the changes. The regulation has been known for some time, allowing Norwegian institutions time to prepare.

The regulation will strengthen the requirements for institutions in the financial sector, even though current Norwegian regulations and supervisory practices are based on the same principles as the new requirements. Institutions that currently comply with the requirements in existing regulations and relevant guidelines are well-positioned for the changes. The regulation has been known for some time, allowing Norwegian institutions time to prepare.

Up to now, the financial sector has assessed the outsourcing of ICT operations according to the ICT Regulations or equivalent frameworks. DORA applies to the use of ICT services and entails an expansion of regulations concerning the use of ICT service providers. DORA imposes strict and detailed requirements on the contents of contracts and requires that institutions maintain a register of all ICT service providers. Institutions covered by DORA must review all outsourcing agreements, as well as other ICT service agreements, to ensure compliance with the DORA requirements. The scope of the contract register will increase compared to the current outsourcing overview, cf. the requirements in the Notification Obligation Regulations. The task of reviewing all contracts will be extensive and demanding.

³⁴ [Finanstilsynet's website on DORA](#) (Norwegian only)

³⁵ [Public consultation](#) (Norwegian only)

At a minimum, Finanstilsynet expects entities to have a plan for bringing agreements into compliance with DORA.

What entities can prepare

Entities should prepare for the transition from complying with the principle-based ICT Regulations, or equivalent regulations, and guidelines from the European Supervisory Authorities (ESAs) to DORA with level 2 regulations that are significantly more comprehensive, detailed, and rule-based. Entities should consider the following measures in their preparation for DORA:

- Review the requirements set by DORA, taking into account proportionality and risk level, where many of the requirements are absolute.
- Assess the need for updating frameworks, processes, policies, procedures, registers, etc.
- Pay particular attention to areas that will be part of the risk management framework.
- Involve management and the board of directors.
- Assess the need for changes in management and board reporting.
- Assess the need to strengthen vendor management, including enhanced oversight of subcontractors.
- Assess the need to strengthen work on ICT security to reduce the likelihood and consequences of incidents.
- Assess the need for adjustments in the organisation and/or changes in roles and responsibilities.
- Review contracts for ICT services, assess the need for updates in accordance with the regulation, and make a plan for this work.
- Assess the need for supporting tools and ICT development.
- Assess the need for competence and information initiatives.
- Prepare for and conduct business impact analyses (BIA) and assess the entity's dependence on ICT systems.
- Consider changes in the entity's risk appetite, taking into account assessments from the business impact analysis.
- Review the entity's three lines of defence or equivalent and assess the need for changes, particularly regarding oversight of service providers and subcontractors, whether sufficient independence is ensured, and the level of expertise is adequate.
- Consider the possibility of embedding risk management and compliance controls into the entity's operational activities.
- Consider participation in collaboration and information sharing forums related to cyberthreats if the entity is not already a part of such collaborations.
- Familiarise themselves with level 2 regulations as they come up for consultation and are later adopted.