



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

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

RISK AND VULNERABILITY ANALYSIS

2020



CONTENTS

1. SUMMARY	4
2. FINANCIAL INFRASTRUCTURE	11
2.1. The importance of the financial infrastructure	11
2.2. The financial infrastructure is robust	12
2.3. Financial Infrastructure Crisis Preparedness Committee (BFI)	12
2.4. The coronavirus pandemic	13
2.5. Cooperation in the area of security	14
3. FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS	16
3.1. Governance model and internal control	16
3.1.1. Board and management	16
3.1.2. Internal control functions	17
3.1.2.1. Operational management	17
3.1.2.2. Risk management	17
3.1.2.3. The compliance function	18
3.1.2.4. The internal audit	19
3.1.3. Regulatory requirements	19
3.1.4. Policies and guidelines (governance framework)	20
3.1.5. Change management and digital transformation	20
3.2. Skills and skills management	21
3.2.1. Skills management	21
3.2.2. The skills situation in Norway	21
3.2.3. Comprehensive understanding of architecture and digital business processes	22
3.2.4. Measures implemented by institutions and the authorities	22
3.3. Vendor management	23
3.4. Information security and cybercrime	24
3.4.1. Cyberattack trends	24
3.4.2. National threat and vulnerability assessments	25
3.4.3. The institutions' defences	26
3.4.4. Security culture and training	26
3.4.5. Vulnerabilities and threats – the human factor	27
3.4.6. Information leaks	28
3.4.7. Cyberattack response times	29
3.4.8. Cybercrime using artificial intelligence	29
3.4.9. Quantum technology – a security threat	29
3.4.10. Vulnerability and security tests (TIBER)	30
3.4.11. Cyber insurance as risk-mitigating measures	30
3.5. ICT operations	31
3.5.1. Operating complex ecosystems	31
3.5.2. Phasing out of outdated systems	31
3.6. Business continuity management and crisis management	32
3.6.1. Survey of the banks' crisis management capacity	32

3.6.2.	Geopolitical factors	33
3.6.3.	Working from home as part of disaster recovery solutions	34
3.6.4.	National and international lines of communication	35
3.7.	Development and innovation	35
3.7.1.	Development goals	35
3.7.2.	Agile development methodology	36
3.7.3.	Digital transformation through the use of an application programming interface (API)	37
3.7.4.	Use of new technology	38
3.8.	Logical access management and control	39
3.9.	Physical security and access control	39
3.9.1.	Physical access control	39
3.9.2.	Intruders	40
3.10.	Change management and security updates	40
3.10.1.	The change process	40
3.10.2.	Security updates (patches)	41
3.11.	Data and information	41
3.11.1.	Data management	41
3.11.2.	Securing data (backups)	42
3.12.	Transaction monitoring (AML)	42
3.12.1.	Quality of customer and transaction controls	43
3.12.2.	Quality assurance and follow-up of the rules	43
3.12.3.	Operation of electronic customer and transaction monitoring systems	43
3.12.4.	Transaction monitoring and customer assessments using artificial intelligence	44
3.13.	Risk associated with the institution's customers	44
3.13.1.	Login information going astray and fraudulent use of BankID	44
3.13.2.	Measures for reducing fraud and fraudulent use	44
3.13.3.	Social engineering	45
3.13.4.	Customer interface through new service providers	45
3.13.5.	Communication with customers via email	45
3.13.6.	Analogue customers	46
3.13.7.	Identification controls for analogue customers	46
3.13.8.	Lack of trust resulting from operational incidents	46
3.13.9.	The institutions' integrity as a result of cybercrime	47
4.	FRAUD AND FRAUD STATISTICS	48
4.1.	New reporting of fraud statistics	48
4.2.	Losses associated with the fraudulent use of payment cards	48
4.3.	Losses from online banking fraud	51
4.4.	Losses from social engineering fraud	52
5.	INCIDENTS REPORTED IN 2019	54
5.1.	Incident statistics	54
5.2.	Incidents with particularly serious consequences	55
5.3.	Analysis of incidents as a measure of availability	57
6.	NOTIFICATIONS FROM THE INSTITUTIONS	59

6.1.	Notifications of outsourcing	59
6.2.	Notifications regarding payment service systems.....	59
6.3.	Reauthorisation and licence to provide payment services.....	60
6.4.	Risk reporting for payment service providers.....	61
APPENDICES	62
1 – Institutions’ response to the questionnaire on vulnerability		62
2 – Basis for the risk matrix		67
3 – Finanstilsynet’s monitoring activities.....		75
4 – Internal control functions		78
5 - International frameworks relating to ICT security		80

Cut-off date 13 May 2020

1. Summary

Norway's financial infrastructure is robust. There were no ICT incidents that impacted financial stability in 2019. A slightly higher number of ICT incidents were reported in 2019 than in 2018. Nevertheless, Finanstilsynet believes that the availability of payment services and other customer services was better in 2019 than in 2018. While the incidents had negative consequences for the customers affected, the overall availability of the services was regarded as satisfactory.

During the coronavirus crisis, Finanstilsynet and the Financial Infrastructure Crisis Preparedness Committee (BFI) have paid particular attention to entities that support important functions, including the critical social functions defined by the Norwegian Directorate for Civil Protection (DSB). The key institutions in Norway's financial infrastructure have good emergency response plans. They have maintained good control of the operational situation so far and have quickly taken the required measures.

The scale of cybercrime continues to increase but so far it has not resulted in major incidents in institutions in the Norwegian financial sector. The institutions' defences have been reinforced and attacks are generally averted before they can have serious consequences. Only six of the 206 reported ICT incidents in 2019 were security incidents.

Finanstilsynet has through incident reports and its supervisory activities noted vulnerabilities that may represent a risk of serious incidents in the financial sector. Finanstilsynet has pointed out factors such as the inadequate follow-up of service providers by banks and payment institutions, especially with respect to service providers' compliance with an institution's security requirements, and risk analyses of ICT operations failing to adequately identify the actual risk. Weaknesses have also been identified within banks' business continuity and crisis management. Both banks and investment firms were found to have inadequate information classification and protection routines for exchanging and handling information, as well as inadequate routines for testing security.

Finanstilsynet believes that in order to ensure the financial infrastructure's resilience, institutions should improve their ICT efforts both to reduce the likelihood of non-conformance and to enhance ICT security.

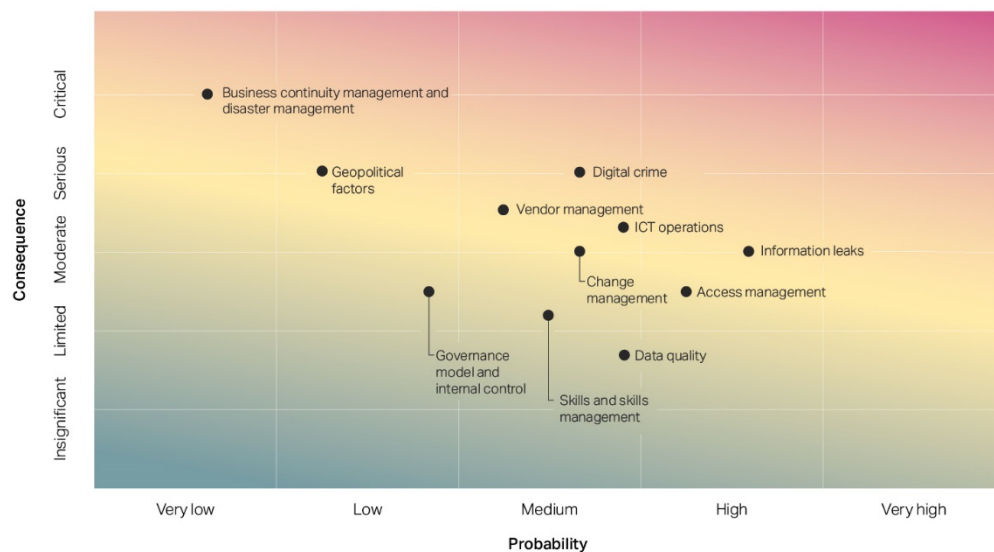
Finanstilsynet’s assessment of the risk associated with threats and vulnerabilities in the institutions’ ICT operations

Finanstilsynet believes that vulnerabilities in the institutions’ defences against cybercrime and information leaks, as well as ICT operations, are the most important threats associated with the institutions’ use of ICT. The risk is considered to be high.

The risk associated with vulnerabilities in the institutions’ business continuity and crisis management, geopolitical factors and access management is considered to be moderate to high. The risk associated with vulnerabilities in vendor management, change management, the institution’s governance model and internal control, skills and skills management, and data quality is considered to be moderate.










Figure 1.1 summarises Finanstilsynet’s assessment of the most important threats and vulnerabilities in the financial sector. In the figure, the various risk areas are classified according to the probability of a serious negative incident occurring and the severity of the consequences for the individual institution. The observations and assessments the classification is based on are provided in table 1.1 and discussed in more detail in chapters 3 to 6. The methodology and details on which the assessments are based are discussed in Appendix 2.

Figure 1.1
 Finanstilsynet’s assessment of the risk associated with threats and vulnerabilities



Source: Finanstilsynet

Table 1.1

Area	Vulnerabilities and threats that could represent a risk of adverse incidents (Degrees of risk, probability and consequence are stated in chart 1.1)	Trend
Governance model and internal control	An inadequate overview of which checks are included in the institution's internal control and how the checks should be performed, monitored and audited may result in factors that could 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 skills 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 oversight of critical and outsourced ICT services.	
Cybercrime	Inadequate security testing, security updating, training and awareness-raising among employees, and inadequate monitoring of activities in its own technical infrastructure, including networks and systems, may result in criminals inflicting damage on the institution through digital attacks.	
Information leaks	Inadequate information classification, including documentation, and checks 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.	
Business continuity management 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 normal 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	A fast pace of development, where quality is sacrificed at the expense of time, may result in functional errors in applications and systems, and security holes not being identified. Inadequate control of changes to operating configurations may result in interruptions to critical business processes and the institution being exposed to cybercrime.	

Access management	Inadequate control and monitoring of broader access rights, for employees and service provider personnel, may harm the institution as a result of deliberate or unconscious operational errors. It can also lead to information leaks.	→
Data quality	Deficiencies or errors in data may result in analyses and checks being performed based on incorrect or insufficient information. This may include errors in credit ratings, errors in checks aimed at detecting money laundering or fraud, errors in risk assessments and errors in monitoring operations.	→

Source: Finanstilsynet

The risk assessments in the table are based on the observations and assessments made by Finanstilsynet that are discussed in chapters 3 to 6. The arrows indicate Finanstilsynet's assessment of the trend (increasing, unchanged or decreasing risk). Further details about what the assessments are based on are provided in Appendix 2.

The institutions' assessment of risk

The dialogue with the institutions and their responses to the annual digital vulnerability survey showed that the increasing complexity of the systems portfolio results in risk in a number of areas, although the risk is nevertheless considered to be decreasing. The increasing complexity results in challenges such as:

- Designing good disaster recovery solutions is more complicated
- Comparing logs from different systems can be difficult, impairing the ability to make use of the information in the logs
- Challenges with respect to establishing comprehensive defences against cyberattacks
- Complicated and time-consuming troubleshooting
- Complicated, comprehensive and demanding risk analyses
- Inadequate data quality

Many institutions see cyberattacks as a present and serious risk and believe that inadequate security awareness among employees increases the danger of successful attacks. Delivery pressure also represents a risk, although institutions believe that this risk will lessen. Many institutions also identify challenges with respect to good, comprehensive data and systems support for analyses of suspicious transactions.

The institutions consider the scope of regulatory requirements, including new requirements with short implementation deadlines, to represent a significant challenge and risk. New regulations can entail extensive, demanding modifications to systems. There is often a need to interpret new regulations and requirements and make them operational, and the institutions believe that clarifications from the authorities affected arrive too late.

Risk associated with customers' access to digital services

Digitalisation has resulted in the institutions' customers having to start using solutions for identification and authorisation, where services like BankID have become a form of 'universal key' for accessing both private and public services. This is efficient, although the widespread use of BankID

entails risk. BankID can be used for many different services and often without further controls being imposed to prevent misuse. This creates a vulnerability for both customers and institutions alike. Risk-mitigating measures should be considered for various services, adapted to the individuality of the service and the potential for misuse.

Advances in digital solutions have also resulted in most financial services being based on self-service. This makes great demands on the institutions' ICT operations and information security when it comes to ensuring availability, confidentiality and data integrity, so that customers will feel confident about using them. It also requires good follow-up of customers who, in the event of irregularities, will be, or will perceive themselves to be, injured parties. The digitalisation of financial services has also presented challenges for some groups of customers. It is important that the institutions establish good solutions for these customers as well, either by maintaining manual solutions or by offering simple digital solutions.

Losses from fraud

Following the introduction of the revised Payment Services Directive (PSD 2), the reporting of fraud has changed slightly from previous years and the reported numbers for the second half of 2019 are therefore not directly comparable with previous reports.

Total losses from card fraud amounted to around NOK 190 million in 2019. This is an increase of 28 per cent since 2018. The losses were evenly distributed across the first and second halves of the year. The fraudulent use of card details in online transactions was subject to the most pronounced increase. The figures for the first half of 2019 also indicate an increase in the number of payment cards subject to fraudulent use. (Corresponding figures were not reported for the second half of the year due to the changes resulting from PSD 2).

Losses due to card fraud in the second half of the year corresponded to 0.02 per cent of the total value of transactions and the number of fraudulent transactions amounted to 0.007 per cent of the total number of transactions.

Losses related to online banking amounted to NOK 3.6 million in the first half of 2019, which is low compared with previous years. In the second half of the year, losses from account transfers where the fraudster issues the payment order amounted to NOK 46.5 million. The figures are not directly comparable with previous reports.

Social engineering fraud increased further in 2019 and is the most lucrative method for criminals. The reported figures indicate losses of more than NOK 500 million, compared with just under NOK 300 million in 2018.

Outsourcing of ICT and notifications about payment services

Finanstilsynet processed 135 notifications of ICT outsourcing in 2019, which was fewer than in 2018. Finanstilsynet can see that the institutions have become better at handling outsourcing contracts,

including risk analyses of outsourcing, board consideration of outsourcing relationships and the quality of the agreements with subcontractors. The notifications in 2019 also showed a clear trend towards increased use of cloud services.

In 2019, Finanstilsynet received 21 notifications about changed or new payment services, in particular about the cooperation between banks on payment solutions and new solutions for payments via mobile phone. Finanstilsynet also received 30 applications for reauthorisation¹ and/or a licence to provide payment services. The applications showed that many institutions have an inadequate understanding of the regulations and need to significantly improve their procedures.

Finanstilsynet's monitoring of the institutions

The main themes for supervisory activities in 2020 will be:

- the institutions' governance of ICT operations
- the organisation of ICT/cyber security work
- the security surrounding the institutions' ICT solutions
- the institutions' preparedness work and testing of business continuity and disaster recovery solutions
- the institutions' governance and monitoring of outsourced ICT operations
- the institutions' payment services, including compliance with the revised Payment Services Directive
- Finanstilsynet will also monitor the institutions' ICT solutions in order to identify money laundering and terrorist financing, as well as the banks' range of cash services and cash preparedness.

ICT incidents at the institutions will be followed up. The emphasis will be on ensuring that institutions identify causes and take steps to prevent repetition. The threat picture for cybercrime is monitored and the institutions' preparedness work targeting digital vulnerability and digital security is reviewed.

Finanstilsynet believes that it is important that the institutions properly address the security of their services so that customers do not suffer losses. It will also check that the institutions do not share their customers' data without consent and that these data do not fall into the hands of unauthorised parties.

Finanstilsynet heads, and is the secretariat for, the Financial Infrastructure Crisis Preparedness Committee (BFI). The committee follows up preparedness and incidents in the financial infrastructure. In special circumstances, such as the coronavirus crisis, BFI will monitor the ICT operations of the most important entities especially closely.

¹ Approval under the transitional arrangements in connection with the revised Payment Services Directive.

Brief summary of the appendices

The institutions' responses to the vulnerability survey, the basis for Finanstilsynet's assessment of risk and Finanstilsynet's monitoring of the institutions are described in separate appendices. In addition, the appendices describe the European supervisory authorities' international framework for ICT security and the framework for information security and security testing.

2. Financial infrastructure

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

The payment system consists of 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 governed by laws and regulations and by the financial services industry's self-regulatory system, which is administered by Finance Norway (FNO) and Bits AS. As a result of the revised Payment Services Directive (PSD 2), a number of regulatory amendments were adopted with effect from 1 April 2019. The most important changes relate to the Act on Payment Services, the Regulations on Systems for Payment Services and the Regulations on Payment Services.

The new infrastructure for real-time payments, also known as immediate payments, where the funds are available on the payee's account immediately, was adopted by Norwegian banks in 2019.

The securities area is regulated by a number of key laws and regulations, including the Securities Trading Act, the Securities Trading Regulations and the Norwegian Central Securities Depository Act. The securities area includes actors involved in securities transactions related to equity instruments such as shares and equity certificates, including the execution of trades and related settlements.

2.1. The importance of the financial infrastructure

Effective, robust and stable payment services are a fundamental prerequisite for financial stability and well-functioning markets. The financial infrastructure is designed to ensure that cash payments and transactions in financial instruments are registered, cleared and settled.

The Norwegian Directorate for Civil Protection² has designated financial services a critical social function. The Ministry of Justice and Public Security has defined financial stability and freedom of action as one of several national security interests in the new Security Act³.

Failures suffered by key actors in the financial services industry or in the infrastructure can have substantial social consequences. If payments or securities trades cannot be executed or settled, important social functions will quickly stop working satisfactorily. Sensitive information going astray or breaches of the rules for processing inside information may undermine confidence in marketplaces and the financial system. If criminals gain access to large quantities of customer and account data and

² [DSB: Samfunnets kritiske tjenester](#)

³ [Sikkerhetsloven §1-5 Definisjoner](#)

compromise them or make them unavailable, customers and institutions could face significant challenges. Such incidents could also impact financial stability. The social consequences could be particularly severe if institutions operating on behalf of many or all institutions are affected. The financial sector is also dependent on shared infrastructure such as power supplies and telecommunications, including networks.

Finanstilsynet and Norges Bank cooperate on the supervision and surveillance of the financial infrastructure in Norway, including through reports, risk assessments and joint supervision.

2.2. The financial infrastructure is robust

Finanstilsynet believes Norway's financial infrastructure is robust. There were no major ICT incidents that impacted financial stability in 2019. The operational stability of the services was satisfactory. There were fewer reported ICT incidents that affected the availability of payment services and other customer services in 2019 than in 2018. Even though there were a number of incidents that resulted in negative consequences for the customers affected in 2019 as well, the overall availability of the services was viewed as satisfactory and better in 2019 than in 2018.

The reliability of the clearing and settlement systems was generally good in 2019 and there were no critical incidents. The reliability of the communication with SWIFT, the international payment system, and CLS, the international settlement system, was also good.

The scale of cybercrime is increasing year-on-year, but so far has not resulted in major incidents in institutions in the financial sector. Although vulnerabilities have been identified and serious operational failures with major consequences have occurred, no systemic crises have arisen so far.

A digital incident can occur suddenly, result in collapse and have wide-ranging social consequences. The institutions' ICT work, both with respect to reducing the likelihood of irregularities and generally improving ICT security, is important for ensuring stable, robust operational solutions and thus the robustness of the financial infrastructure. This includes business continuity solutions, disaster recovery solutions and emergency preparedness, recovery plans and ICT security work.

2.3. Financial Infrastructure Crisis Preparedness Committee (BFI)

The Financial Infrastructure Crisis Preparedness Committee (BFI)⁴ was established in order to:

- design 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.

⁴ [Beredskapsutvalget for finansiell infrastruktur \(BFI\)](#)

- perform the necessary coordination of preparedness matters within the financial sector, including, based on the civil preparedness system, coordinating the preparation and implementation of notification plans and preparedness measures in the event of national security policy crises and war.

Finanstilsynet obtains a good, broad picture of the status of the financial infrastructure through its supervisory activities and work in BFI, which reviews severe and critical incidents that impact the infrastructure's various components.

2.4. The coronavirus pandemic

Finanstilsynet has been monitoring the financial infrastructure closely since the coronavirus pandemic escalated in Norway. BFI has held frequent meetings to follow up how the key institutions in Norway's financial infrastructure are ensuring good, stable and secure operations, ref. the committee's remit. The meetings have contributed to the sharing of information on factors that could result in disruptions to the financial infrastructure or impact financial stability, as well as measures that the institutions have taken or are planning to take. So far, the actors have maintained good control over the operational situation and have implemented the required measures. Finanstilsynet finds this reassuring.

Experience to date shows that the key institutions in Norway's financial infrastructure have good emergency response plans that can be implemented quickly. The institutions established crisis management teams in line with the development of the coronavirus pandemic and government measures for curbing its spread.

Finanstilsynet and BFI have paid particular attention to entities that support critical functions, including the social functions defined as critical by the Norwegian Directorate for Civil Protection (DSB). These are the ability to:

- i) maintain secure transfers of capital in the financial markets between national actors and to and from abroad
- ii) execute payments and other financial transactions securely
- iii) maintain the public's access to the necessary means of payment.²

As part of the infection control for their employees, many institutions reviewed critical roles, functions and staffing, and implemented measures such as splitting up the organisation and readying or using backup locations. The institutions expanded capacity for system connections from home. Permission was given to perform some functions when working from home that can normally only be reached from an office location, and strict security measures and enhanced monitoring were introduced to increase security when working from home. Strict regimes were implemented, with the ability to make changes to ICT systems being restricted or halted. Critical operations and critical service providers of these were monitored very closely. The banks' and their service providers' handling of the range of cash services was monitored. In line with the disaster recovery plans, some institutions brought operations back home from abroad and maintained a limited amount of operational capability abroad

as a contingency arrangement. Many institutions reviewed their plans for the physical security of premises, including locations for ICT operations.

2.5. Cooperation in the area of security

Institutions with critical social functions in the financial sector

The operation and security of the financial institutions' ICT systems have been designated critical social functions in connection with the ongoing coronavirus pandemic.⁵ Measures are implemented at the national level to ensure that the financial institutions in Norway deliver functioning payment and trading systems.

The new Security Act⁶, which came into force on 1 January 2019, defines financial stability and freedom of action as one of a number of national security interests³ that must be monitored by the responsible sectoral ministry. Ministries must identify and maintain an overview of entities that are of crucial or significant importance to basic national functions (BNF) and report these to the Norwegian National Security Authority (NSM). For institutions that are of *crucial importance* to BNF, the responsible ministry must decide whether the Act shall fully or partly apply to the institution. Ministries must also maintain an up-to-date overview of institutions of *essential importance* to BNF.

In 2019, Finanstilsynet produced analyses and advice to the Ministry of Finance relating to the identification of basic national functions, as well as assessments of entities that may be of significant importance to basic national functions. This work will continue in 2020.

Institutions that support basic national functions may be at greater risk of threats from foreign intelligence services. Stricter requirements have, therefore, been set for the institutions' security work, including subcontractors and partners. Threats from foreign state actors are described in 3.4.2.

Cooperation and information sharing result in a better understanding of risk

Cooperation and exchange of experience on information security between financial institutions in Norway will help to improve knowledge about the relevant threat and risk picture, and better equip the institutions to handle cyber threats and adverse incidents.

In 2019, Finanstilsynet was designated a sectoral response environment (SRE)⁷ by the Ministry of Finance and tasked with handling ICT security incidents in that part of the financial sector for which Finanstilsynet is responsible. Finanstilsynet performs this role in cooperation with Nordic Financial CERT (NFCERT)⁸.

Finanstilsynet participates as a partner in the Norwegian National Cyber Security Centre, which was established by the Norwegian National Security Authority (NSM) in 2019 to strengthen Norway's

⁵ [Koronaviruset: Samfunnskritiske virksomheter i finanssektoren](#)

⁶ [Lov om nasjonal sikkerhet \(sikkerhetsloven\)](#)

⁷ [Rammeverk for håndtering av IKT-hendelser, NSM](#)

⁸ [Nordic Financial CERT](#)

cyber resilience and preparedness. Participation provides Finanstilsynet with access to up-to-date knowledge about the risk picture in the area of cyber security. Finanstilsynet has access to the centre and can interact and share information with other partners and actors when managing cyber threats and attacks.

3. Finanstilsynet's observations and assessments

In addition to findings, observations and assessments from supervisory activities, the institutions' own assessments of the most conspicuous vulnerabilities and threats collected via questionnaires and interviews are discussed. These are discussed in more detail in Appendix 1.

ICT security, cyber threats and the development of the threat picture, as well as how the institutions should prepare against cyber threats, are also discussed. This includes threat and risk assessments from national security services and authorities of special relevance for the financial services industry. Other areas that are discussed include access management, change management, business continuity management and crisis management, skills management, as well as planning and organising ICT operations. Technology trends considered to be of potential significance for the risk associated with the financial institutions' use of ICT are also discussed.

3.1. Governance model and internal control

3.1.1. Board and management

The institutions have a responsibility to ensure that their ICT operations satisfy all of the requirements in the Regulations on Use of Information and Communication Technology (ICT). This responsibility also applies where all or parts of ICT operations are outsourced.

Finanstilsynet expects the institutions' boards and executive management to be familiar with the contents of the Regulations and ensure that policies, guidelines and service provider agreements support the requirements of the Regulations. It is the responsibility of the board and management to ensure that internal control is established with a structure and format, in line with the institution's size and operations, that ensures that operational units perform the necessary controls. The compliance function must monitor and control that the requirements are adhered to and report the status to the board and management. The board, and any audit committee, must also assess whether the institution's internal audit is carrying out adequate audits that correspond to the institution's operational risk tolerance in the ICT area.

Boards are expected to have the expertise and insight necessary to help ensure that IT investments support the institution's strategy and needs. It is an important prerequisite for ensuring stable and secure ICT operations that the board and management understand and acknowledge the risk picture.

Finanstilsynet believes that the ICT maturity of the institutions' boards and management has increased in recent years. Increased digitalisation and the need for change resulting from this (digital transformation) have in the opinion of Finanstilsynet increased the awareness of boards and management, especially with respect to the digitalisation of business processes and information security.

The institutions' boards and management must continuously assess whether or not the expertise and understanding of technology necessary for the governance of the institution's ICT operations are in place.

3.1.2. Internal control functions

Cooperation between operational units and the independent functions in the institutions' first and second lines of defence, including risk management, compliance and internal audit, is important for ensuring good, effective internal control in the institutions. Institutions that do not ensure independent monitoring and oversight run the risk of underreporting and errors in reporting. This in turn entails a risk of significant non-conformance in relation to compliance with laws and requirements not being uncovered, and significant risks not being identified.

At the same time, it is important to underscore that it is the operational management in the institution's first line that must ensure that guidelines and instructions issued by the board and management are adhered to and complied with. The institution's strategy, policies and guidelines (governance framework) and underlying instructions, as well as service provider agreements, are key to the institution's internal control.

The internal control functions are described in more detail in Appendix 4.

3.1.2.1. Operational management

As a rule, the institutions allocate most resources to control functions in operational units in line with good practice. Finanstilsynet is of the impression that the first lines have strong expertise and a good understanding of the control function. However, in Finanstilsynet's experience, smaller institutions have limited ICT resources and expertise. Such institutions often depend on good cooperation models within an alliance.

Nonetheless, it is stressed that each institution has a responsibility to obtain information about compliance with the requirements set out in the governance framework, see 3.1.4.

3.1.2.2. Risk management

ICT risk is part of an institution's operational risk and includes the risk of information leaks (breaches of confidentiality), unauthorised changes (breaches of integrity) or sabotage of the institution's technical infrastructure (unavailability). The risk picture includes all internal and external vulnerabilities and threats to an institution's systems, technological infrastructure and staff. Risks associated with strategic choices, the institution's organisation, expertise and security are also included.

The ICT risk picture is extensive, complicated and constantly changing. This means that the institutions must adopt and revise strategies, policies and guidelines, and that new controls must be established. Therefore, risk management is fundamental to the company's administration of the governance model for the ICT area and the exercise of internal control. The ICT risk picture must be prioritised by the institution's board and management on a par with other operational risk.

Finanstilsynet is of the impression that the maturity of the institutions in relation to the exercise of risk management is generally acceptable. Nevertheless, its supervisory activities have revealed that this risk management has not always encompassed the entire risk picture in the area of ICT. One of the reasons for this may be that the risk management function in the institution's second line does not have sufficient resources, expertise or understanding of the complexity of the risk picture. Finanstilsynet has found that institutions lack procedures that instruct operational units in IT departments and business areas, as well as the risk management function, to take a methodical and coordinated approach to ICT risk.

Finanstilsynet has also noted inadequate or missing risk assessments of key ICT service providers, including risk assessments linked to service providers' financial stability, organisation, expertise, cooperation and other relevant factors linked to outsourced services. Finanstilsynet believes that relevant parts of the ICT service providers' risk assessments should be included in the basis for the institution's own assessments.

Finanstilsynet stresses that institutions' boards and management have a responsibility to ensure that risk assessments take a comprehensive approach. Institutions that do not take a comprehensive approach to the ICT risk picture could, naturally, be exposed to serious risks without this being known to the board and management, and there will be great uncertainty about whether the actual risk exposure is within the institution's risk tolerance.

3.1.2.3. The compliance function

Inadequate monitoring, including monitoring of the operational units' oversight of compliance with the requirements as formulated in policies, guidelines and service provider agreements, constitutes a risk of an institution's board and management not receiving an independent assessment that sufficiently confirms or refutes whether or not the institution's operations are being carried out in line with the established requirements.

In its supervisory activities, Finanstilsynet has observed compliance functions that perform limited monitoring and controls of the operational units' compliance with the aforementioned requirements. Finanstilsynet believes that this is largely due to the compliance function lacking resources, as well as insight into, and understanding of, the ICT control regime. Furthermore, the compliance function is not adequately involved in the work of establishing the controls that must be carried out by the operational units and which are a prerequisite for the compliance function's monitoring ability.

Even if the controls that are carried out by the operational units are regarded as good by the board and management, inadequate monitoring and control by the compliance function will result in a significant weakening of the institution's internal control, for example where operational units report errors or fail to perform critical controls. In the opinion of Finanstilsynet, independent control is absolutely necessary and a prerequisite for satisfactory internal control.

3.1.2.4. The internal audit

An institution's internal audit is the board's independent monitoring function. The duties of the internal audit include assessing whether the description of the controls that must be performed in the ICT area are consistent with the institution's risk tolerance and the requirements set out in the governance framework, see 3.1.4. Furthermore, the internal audit must assess the quality of the operational units' performance of the controls and whether these have actually been carried out. The internal audit must also assess whether the internal control reporting to the board and management matches the actual situation. Finanstilsynet also emphasises the internal audit's responsibility for raising awareness and improving the knowledge of members of the audit committee, board members and management about threats and vulnerabilities within the areas of ICT and security.

Section 12 of the ICT Regulations states that institutions must ensure that agreements with ICT service providers provide a right to control, including through auditing, the service providers' contractual activities. Finanstilsynet has found that the internal audit often restricts audits to covering vulnerability and security tests. These are important, but only cover a small proportion of the operational risk. Banks in some banking alliances have chosen to cooperate on audits of service providers, which is an appropriate model where institutions use the same outsourced services.

In some inspections, Finanstilsynet has established that audits are not carried out of the institution's second line, which results in inadequate assessments of how functions such as risk management and compliance address their roles and responsibilities. Finanstilsynet believes that it is important to conduct independent assessments of all ICT control functions in an institution.

Through its supervisory activities, Finanstilsynet has seen institutions' internal audit fail to fully embrace the entirety in their audit work, which weakens a board's ability to obtain an independent assessment of the control status. Finanstilsynet believes that the internal audit should audit all areas regarded as having high operational risk, both internally in the institution and with respect to the outsourced ICT services. An institution's board, and any audit committee, should, together with the internal audit's management, establish an audit cycle that shows which operational risks must be covered by the internal ICT audit.

The service providers' independent audit statements, such as ISEA 3402, can be included as a basis for assessing the control situation at the service providers.

3.1.3. Regulatory requirements

Regulatory requirements for personal data protection (GDPR), anti-money laundering (AML) and terrorist financing, payment services (PSD 2) etc. make it necessary for the institutions and their service providers to implement the required changes and modifications to their ICT systems.

The institutions regard new regulations as representing a considerable challenge and risk. The regulations may entail major changes to systems, often with little time to adapt. There may also be a

need to interpret and clarify the regulations, and the impression given is that the clarifications etc. from affected authorities arrive too late.

Finanstilsynet believes that more attention should be paid to compliance with the ICT Regulations by the institutions' boards and management. Breaches of the ICT Regulations may result in serious consequences for stable and secure operations. Serious incidents can result in loss of reputation and, in the worst case scenario, incidents can ultimately threaten the very existence of an institution.

3.1.4. Policies and guidelines (governance framework)

Finanstilsynet has observed through its supervisory activities that the quality of the institutions' ICT frameworks differs. The distinction between policy (guidance) and guidelines and instructions (orders) is not always clear enough. The institutions lack routines for ensuring that policies are operationalised as guidelines and procedures; there are omissions in instructive documents and documentation that is not up-to-date.

In its supervisory activities, Finanstilsynet has noted that institutions lack an overview of controls and descriptions of controls that must be carried out by operational units internally in the institution and controls that must be carried out by the service providers. This results in, among other things, the institution's compliance function, see 3.1.2.3, not having a sufficient basis for monitoring, controlling and assessing the institution's compliance.

A well-functioning internal control function requires that the board and management obtain the necessary confirmations that controls have been carried out in line with the requirements set, both by operational units, including service providers, and by the compliance function and the institution's internal audit. If the controls are not carried out, there is a danger of serious vulnerabilities not being identified and institutions thereby not implementing the necessary risk-mitigating measures.

Finanstilsynet stresses the responsibility the board and management have for ensuring that the framework is subject to good development, implementation, operationalisation and administrative procedures. Management must also ensure that controls are established that provide the board and management with confirmation that the framework requirements are being complied with. Breaches of the institution's risk tolerance may be one of the consequences of inadequate governance.

3.1.5. Change management and digital transformation

The ongoing digital transformation is making great demands on the institutions' change management. However, Finanstilsynet has through its dialogue with the institutions noted that they lack routines and processes that adequately address the digital transformation of the business processes, including the changes in the organisation being implemented in line with the digitalisation.

Changes in mindset, culture, organisation and expertise are challenging for the institutions. Restructuring can create uncertainty, insecurity and a reluctance that can grow in strength if the

restructuring processes are not clearly anchored throughout the entire organisation. Organisational development where an organisation has to be changed in line with technological advances can also be very demanding. Changes in skills needs also challenge individuals, at the same time as the institution must find a balance between advances through the use of new technology, and the development, administration and operation of existing infrastructure and technology.

Finanstilsynet believes that an institution that does not have a clear strategy in its governance model for how the organisation must be changed and adapted in line with technological advances represents a not insignificant risk.

3.2. Skills and skills management

How an institution manages its employees' ICT skills will greatly affect the institution's ability to maintain stability, security, targeted innovation, change management through digital transformation, and vendor management. It will also be of importance with respect to identifying future needs, resource management, motivation and recruitment, and, not least, retaining critical skills during a restructuring phase and ensuring that employees are retrained.

3.2.1. Skills management

Skills management in the area of ICT should be included in an institution's governance model and be part of the institution's change management, see 3.1.5. Skills management will better enable the institution to continuously assess the skills it has available against what the institution needs to achieve its objectives, as well as which skills are no longer necessary. The use of new technology, which results in increased digitalisation and digital transformation, greatly affects skills requirements and needs.

A greater degree of outsourcing is making demands on the institutions' procurement competence, which is important for ensuring that the institution's requirements are reflected in agreements with service providers and that vendor management is performed in line with the institution's governance requirements.

Through its supervisory activities, Finanstilsynet has noted that skills management within the area of ICT is inadequate. There are risks associated with the fact that boards and management have an inadequate overview of the employees' skills and also lack an overview of current and future needs. Finanstilsynet believes that institutions that lack a proper overview run the risk of encountering major challenges in the digital transformation process and challenges in vendor management when it comes to both procuring new ICT services and control of service providers.

3.2.2. The skills situation in Norway

Over the years, many institutions have moved ICT tasks out of their own operations to both Norwegian and foreign ICT service providers. For their part, service providers have outsourced all or parts of their tasks to providers outside Norway, in part due to a scarcity of skills resources in Norway.

As Finanstilsynet discussed in last year's RVA, vulnerabilities attributable to an inadequate supply of ICT skills in Norway constitute a risk of further dependence on foreign providers. This is especially true within operations and information security. Finanstilsynet remains of the view that ICT skills that are no longer managed and developed in Norway can constitute a significant risk, partly due to uncertain geopolitical factors. See a more detailed discussion in 3.6.2.

The institutions' responses to the vulnerability survey show that they consider the skills situation in areas such as ICT operations to be challenging.

Finanstilsynet believes that the institutions must thoroughly assess the scope of ICT skills that must always be available in order to maintain the stable and secure operation of the institutions' infrastructure, systems and applications during a crisis. This includes having to assess the degree to which institutions operating in Norway must be able to manage operations in situations where foreign providers are prevented from performing critical ICT services.

Finanstilsynet stands by its recommendation from last year that the institutions and their service providers should assess what the consequences of a lack of skills in Norway could entail, both in the short term and the long term.

3.2.3. Comprehensive understanding of architecture and digital business processes

The institutions express concern that they lack a sufficiently comprehensive understanding and overview of their architecture and digital business processes. This is due to factors such as a lack of access to IT architects, the increasing complexity of the solutions and the increasing number of ICT service providers involved in the value chain. The institutions also express a concern that the high proportion of personnel with specialist skills at ICT services providers has been at the expense of the service providers' overall understanding of the ICT services that have been outsourced.

Finanstilsynet believes that an inadequate overview of the complex infrastructure of an institution's technological ecosystem, including architecture and systems portfolio, is a serious matter. It could result in security systems being incorrectly configured, inadequate capacity management and errors in the configuration of disaster recovery solutions. It could also result in demanding error rectification in the case of serious incidents, which there were examples of in 2019, and it could result in institutions prioritising the wrong things in their ICT investments and when choosing security solutions.

3.2.4. Measures implemented by institutions and the authorities

Some institutions have established schemes for retraining IT personnel, and other personnel, to facilitate the transition from old to new technology. The Ministry of Education has started work on a new digitalisation strategy for the university and university college sector.⁹ The strategy will be

⁹ [Ny digitaliseringsstrategi for universitets- og høyskolesektoren - invitasjon til åpen innspillsrunde](#)

launched on 1 January 2021. In Official Norwegian Report 2019: 2¹⁰, the Norwegian Committee on Skill Needs points out relevant factors regarding the future need for ICT skills. Finanstilsynet views this as an important measure for meeting the skills challenges in the years to come.

As a consequence of the coronavirus pandemic, the government is establishing 4,000 new student places in autumn 2020, a proportion of which will be student places for technology studies.

3.3. Vendor management

Section 12 of the ICT Regulations states that an institution is responsible for complying with the requirements of the ICT Regulations, including when all or parts of their ICT operations have been outsourced to a third party.

The increased number of service providers whose services are included in institutions' value chains is resulting in more complicated cooperation models with individual service providers, joint cooperation models with multiple service providers and cooperation models between service providers. The cooperation models are managed and coordinated through the institution's vendor management and make great demands on the institution's strategic, administrative and operational functions. If strategically important service providers choose to use subcontractors for parts of their deliveries, this further complicates vendor management. In Finanstilsynet's opinion, this complexity increases the associated risk, which can become especially apparent if serious incidents occur.

Institutions subject to supervision have a responsibility to ensure the necessary governance of their service providers. Good vendor management requires knowledge about current laws and regulations, as well as the establishment of agreements that address the institution's obligations. Therefore, Finanstilsynet expects institutions subject to supervision to have the necessary and adequate procurement competence, including the competence to stipulate requirements for the formulation of the agreements that are entered into with providers of ICT solutions or services and the competence to control compliance with the agreements.

In Finanstilsynet's experience, the institutions have generally documented good management and cooperation models in their agreements with service providers. As a rule, the agreements ensure that the institutions' ICT and information security policies apply. As mentioned in 3.1, institutions may experience challenges in obtaining confirmation of service providers' compliance with contractual requirements.

The institutions' responses to the vulnerability survey also indicate that weaknesses exist in the cooperation model with the service providers and that procurement competence, which is required to follow up the service providers in line with the provisions of the ICT Regulations, is challenging. Finanstilsynet's supervisory activities indicate that alliances of multiple institutions face challenges in

¹⁰ [NOU 2019: 2 Fremtidige kompetansebehov II — utfordringer for kompetansepolitikken](#)

establishing cooperation models that ensure that the individual institution can, on an independent basis, report on the control status of outsourced services to its own board and management.

Finanstilsynet has found through its supervisory activities that some institutions have not established an adequate coordinating control regime between the institution and strategically important ICT service providers. Finanstilsynet believes that institutions should, to a greater extent, obtain service provider confirmations that controls are being carried out in areas with the highest operational risk in line with the requirements of the agreements. For its part, an institution's compliance function can monitor that the confirmations are received, see 3.1.2.3. Where institutions have their own internal audit, enhanced controls, and assessments of the quality of the controls, can be carried out by the internal auditor, see 3.1.2.4. Such an approach will make institutions better able to identify serious failings in a service provider's internal control. It would also strengthen the institution's internal control reporting.

Finanstilsynet believes that the institutions, in cooperation with the service providers, should consider establishing integrated control systems where the institutions can retrieve information and documentation regarding the service providers' internal control of the services being delivered, like the largest cloud service providers offer.

3.4. Information security and cybercrime

Financial institutions are seeing a continuing significant increase in attacks, i.e. cybercrime, against their systems year-on-year. At the same time, the institutions' monitoring and protection systems are becoming increasingly effective, and attacks are usually stopped before they have consequences for the institution.

Finanstilsynet has seen a growing awareness on the part of the institutions of the fact that forms and methods of attack are constantly changing. Finanstilsynet stresses that the boards and management of all institutions should pay particular attention to changes in the threat picture, and the institutions must continue their work of surveying risks and vulnerabilities, implementing preventive measures and having emergency responses plans in place for tackling attacks and their consequences.

3.4.1. Cyberattack trends

The Norwegian National Security Authority (NSM) and the National Criminal Investigation Service (Kripos) have registered a sharp increase in targeted cyberattacks using ransomware against institutions and published a special report on the subject in 2019.¹¹ Financial institutions in Norway face constant attacks of this type, see 5.2, but manage to avert the vast majority of them. Finanstilsynet expects institutions to establish the measures necessary to deal with this type of threat and to carry out the necessary exercises.

¹¹ [NSM og Kripos gir ut temarapport om løsepengevirus](#)

3.4.2. National threat and vulnerability assessments

The Norwegian Intelligence Service (NIS), the Norwegian Police Security Service (PST) and the Norwegian National Security Authority (NSM) issue annual reports containing information about threats, vulnerabilities and risks faced by Norway and Norwegian interests.

In its Focus 2020¹² report, the NIS describes the Chinese and Russian intelligence services as constituting the greatest threat to Norwegian interests. It highlights threats related to China's global involvement in the development of digital infrastructure and states that this could lay the groundwork for a global intelligence capacity on a grand scale.

In its National Threat Assessment 2020¹³, the PST defined the digital mapping and sabotage of critical infrastructure as one of the three most current threats to Norway and Norwegian interests. These are threats to major institutions and their service providers, but are also threats to smaller institutions and niche companies and their service providers. Given the limited resources they have for their security work, small institutions can be particularly vulnerable. A useful tool for institutions may be the NSM's guide on tackling threats from foreign intelligence services.¹⁴

In its report, Comprehensive Cyber Security Risk Assessment 2019¹⁵, the NSM highlights that the digitalisation of public and private sector services contributes to making Norway more dependent on the international digital infrastructure. This is particularly relevant for the financial infrastructure, where many basic financial services are based on international cooperation or are performed from other countries, see 3.6.2.

The NSM points out that organised criminals and state actors constitute the greatest threats to Norwegian targets, including entities that perform important social functions. Computer network operations are used to carry out reconnaissance and collect information about critical social functions, vulnerabilities in infrastructure, recovery and resolution, and emergency preparedness that can be exploited at a later time. Norwegian institutions are also at risk from the theft or manipulation of sensitive information that actors can use later to disrupt or destroy critical infrastructure.

Foreign intelligence services may also try to recruit personnel in order to gain access to information about vulnerabilities in digital infrastructure or other information about an institution, see the NSM's report on insider risk¹⁶ and 3.4.5.

¹² [Focus 2020, Norwegian intelligence service](#)

¹³ [Nasjonal trusselvurdering 2020, PST](#)

¹⁴ [Handtering av digital spionasje, NSM](#)

¹⁵ [Helhetlig digitalt risikobilde 2019, NSM](#)

¹⁶ [NSM publiserer temarapport om innsiderisiko](#)

Cybercrime operations are becoming increasingly difficult to detect and the methods used are complex. Finanstilsynet recommends that institutions make use of the NSM's guide and advice on how to prevent and tackle cyberattacks.¹⁷

The distinction between foreign intelligence services and organised criminals with financial motives is becoming ever more blurred. Foreign intelligence services will want to conceal their penetration of systems and may mislead by giving the impression that the purpose of the attack was to gain access to financial funds, e.g. through ransomware attacks.

The reports also describe 'Cybercrime as-a-Service' where expert hackers map vulnerabilities in, and establish access to, institutions and then sell these on to other criminals or state intelligence services that exploit the vulnerabilities.

3.4.3. The institutions' defences

The dialogue with institutions and the institutions' responses to the vulnerability survey show that cyberattacks are viewed as a serious and present risk, and that the risk associated with attacks is increasing. Establishing comprehensive defences against cyberattacks is demanding due to the use of new technology and the complexity, breadth and scope of digitalisation. The survey also shows that there are weaknesses in network segmentation, perimeter protection¹⁸ and encryption, as Finanstilsynet has also noted in its supervisory activities.

The institutions have mainly focused on securing their networks against external attacks, but it has been discovered that many entities, nationally and internationally, have experienced that attackers have operated from inside their networks over longer periods. As attack methods develop, the institutions' ability to detect and remove unwanted internal actors will be crucial to reducing risk and potential harm.

Finanstilsynet believes it is important that financial institutions ensure that their monitoring and control do not merely consist of the traditional perimeter security but that they also assume that criminals may have established one or more digital footholds inside their network.

3.4.4. Security culture and training

An institution's board and management have a responsibility to ensure that the necessary security culture has been established in the institution through training programmes and ongoing awareness raising efforts, and that the controls necessary to ensure that individuals comply with current security requirements have been established.

¹⁷ [Hvordan forebygge, oppdage og håndtere målrettede digitale angrep, NSM NorCERT](#)

¹⁸ Basic protection of ICT infrastructure components, such as firewalls and switches in networks

Finanstilsynet's supervisory activities show that the institutions have established training programmes that primarily focus on fundamental attitudes with a view to limiting the risk of employees inadvertently breaching current security requirements due to, for example, social engineering.

The institutions' responses to the vulnerability survey indicate that weaknesses exist with respect to employee alertness to threats and attacks, and that the problem is growing. Some institutions face particular challenges.

Finanstilsynet believes that the institutions must ensure that employees are made aware of the institution's policies within areas such as information security and the guidelines that apply. An institution's operational units should carry out controls to ensure that the requirements of the guidelines are being met by employees, and the compliance function must monitor this work.

3.4.5. Vulnerabilities and threats – the human factor

Disloyal employees represent a threat, and negligent employees represent a vulnerability that could undermine the security of the assets of an institution and its customers. Unconscious or deliberate acts can inflict significant harm on institutions.

Vulnerabilities

Employees and personnel at service providers with roles and responsibilities within technical architecture, systems development and security, and those with broader access rights, may be in the target group for criminals. Criminals participate on social platforms, especially for technicians, in order to identify relevant individuals and gain an insight into institutions' technical infrastructure.

Finanstilsynet notes that the institutions have not established special measures to shield personal information from the wider world, including information about the institution's employees and service provider personnel, whose roles may be of interest to, and exploited by, criminals. Nor is it clear what measures the institutions have established to reduce the risk of information that could be exploited by criminals being posted on social media, such as LinkedIn¹⁹ and Reddit²⁰. Finanstilsynet believes that institutions should improve employee awareness through the institution's security programme.

Finanstilsynet refers to Appendix 5 concerning the European Banking Authority's (EBA) standard for identifying employees with a material impact on an institution's risk profile, to which institutions should pay special attention.

Threats

Finanstilsynet believes that there is still a growing risk of criminals working with, and also successfully planting, people inside an institution or its service providers. Insiders with broader access rights to payment systems can with ingenuity carry out frauds without being detected, and insiders can

¹⁹ <https://www.linkedin.com/>

²⁰ <https://www.reddit.com/>

execute operational acts that result in serious business disruption. Finanstilsynet also views the fact that insiders are working with criminals to funnel funds through banks' systems as a risk.

The dark web

There is a risk that criminals may use the 'dark web' (Darknet²¹) to exchange information provided by an insider²². This could be sensitive information about an institution that can be used in planning cyberattacks, including lists of email addresses and login information, sensitive information about an institution's internal affairs, or sensitive information about an institution's customers. Finanstilsynet believes it is difficult to identify such situations, nor is it aware of any institutions that have been exposed to this type of crime. Institutions can reduce insider risk through preventive measures, see 3.4.6.

Control of personnel

Finanstilsynet believes that the institutions should pay special attention to, and consider extended background checks of, personnel who are going to perform critical functions in areas such as operations, information security and transaction monitoring. Finanstilsynet recommends following the advice in 'Sikkerhet ved ansettelsesforhold – før, under og ved avvikling' [*Security in connection with employment relationships – before, during and upon terminating such relationships*] published by the PST, the NSM, the police and the Norwegian Business and Industry Security Council.²³

There is little analysis of employees' activities in the ICT systems. Finanstilsynet believes that institutions should introduce proactive controls to detect abnormal activities, within the framework established by GDPR and the institution's code of conduct. In Finanstilsynet's opinion, this would be an important means of preventing and detecting criminal acts committed by employees or by service provider personnel.

The institutions' responses to the vulnerability survey show that institutions have difficulties adequately analysing logs to detect abnormal activities and react to irregularities.

3.4.6. Information leaks

The institutions take a trust-based approach and assume that employees who are given access to confidential information about an institution's customers and about the institution's internal affairs will act diligently and loyally. This trust also applies to the institution's service providers and personnel with access to confidential information.

Finanstilsynet has through its supervisory activities observed that institutions lack adequate information classification and controls for monitoring documents sent by the institution via email and documentation that is copied to external storage devices or private cloud services. The institutions'

²¹ <https://en.wikipedia.org/wiki/Darknet>

²² www.darkreading.com

²³ [Sikkerhet ved ansettelsesforhold \[Security in connection with employment relationships\]](#)

responses to the vulnerability survey indicate that shortcomings exist in relation to the classification of structured and unstructured data. Inadequate classification makes it difficult to carry out controls to prevent information leaks. Given the current practices, Finanstilsynet regards it as unlikely that sensitive information that is sent unauthorised, deliberately or unconsciously, to external sources will be detected. In addition to the obvious consequences this could have, Finanstilsynet believes that there is a risk that employees are unconsciously contributing to information leakage as a result of social engineering.

Finanstilsynet has noted through its supervisory activities that institutions run a high risk of deliberate or unconscious information leaks to the public domain, media, competitors or individuals. Loss of reputation, loss of customers and substantial fines, e.g. due to breaches of personal data protection, could be some of the consequences. This form of risk can be mitigated through employee awareness campaigns and training. Finanstilsynet believes that it is indefensible for institutions not to have established controls to mitigate the risk of sensitive information leaks.

3.4.7. Cyberattack response times

Response times and effective measures are crucial for limiting damage when an attacker is in the process of gaining, or has established, a foothold inside an institution's network. Identifying and isolating infected systems to limit spreading requires predetermined procedures that should be included in the institution's business continuity and disaster recovery plans, which set out the actions that must be taken and specify the people empowered to make decisions on implementation. Institutions should, as far as possible, identify the potential consequences of a network being shut down entirely or partly, which might be necessary to limit the damage. Predetermined, well-considered measures will facilitate quick decisions and help ensure that they are taken in the right order.

In general, Finanstilsynet believes that many institutions are not adequately prepared to tackle serious cyber incidents. Each institution has a responsibility to assess whether it needs to strengthen its organisation and collaboration with service providers in order to be as well prepared as possible should such an incident occur.

3.4.8. Cybercrime using artificial intelligence

Finanstilsynet stands by its assessment from last year's RVA that 'fake news' could affect institutions through the use of artificial intelligence. This could take the form of fake presentations targeting employees, management, board members or the institution's customers. It could also be fake news aimed at harming an institution or affecting the share price of listed institutions. Artificial intelligence can be used for both attack and defence, and the institutions should also be aware of these types of threats.

3.4.9. Quantum technology – a security threat

Cybersecurity researchers and analysts are concerned about developments in quantum technology, including quantum computers and quantum communications. The technology is based on quantum physics, while today's computers are based on standard electronics. The concern is due to the current

cryptography used in internet communications and data storage not being sufficiently robust if quantum technology is used for decryption. This will represent an extremely severe security threat when the technology is adopted by criminals. The current security architecture in most areas of society is based on the same building blocks, and if these are broken down, the social consequences will be very serious. However, the advances in quantum technology are not far enough along for it to represent a threat yet.

Finanstilsynet believes that the institutions and their service providers should already be monitoring these advances and building up the necessary competence to meet this threat. Finanstilsynet believes that it is important that the industry is at the cutting edge so that the security in the technological infrastructure is developed in line with the advances in quantum technology.

3.4.10. Vulnerability and security tests (TIBER)

Many of the foreign banks with branches or subsidiaries in Norway conduct or plan security testing of the institution's defences in their respective home countries based on the European Central Bank's (ECB) TIBER framework²⁴. The security tests are facilitated and coordinated by each country's authorities.

The TIBER framework gives institutions access to threat information from, and the expertise of, national intelligence services, the expertise of the entire European security industry and the security expertise of the largest European financial institutions.

Norges Bank and Finanstilsynet are working together to establish a security testing framework based on the TIBER framework for the financial services industry in Norway. Norwegian financial institutions are small on a European scale, and naturally have less resources than large European institutions. Competence sharing between Norwegian institutions in such a testing framework could result in significant improvements, especially with regard to the prevention of adverse incidents.

The TIBER framework is discussed further in Appendix 5.

3.4.11. Cyber insurance as risk-mitigating measures

Finanstilsynet encourages the institutions to consider the need to protect themselves both financially and operationally in the area of ICT. In addition to cyberattacks, various other scenarios should be included in assessments, such as business disruptions. To ensure that an institution has insurance cover tailored to its needs, the institution should systematically review its own and its service providers' insurance cover to detect any weaknesses, e.g. a service provider not being insured against failures/fraud by its own employees.

Finanstilsynet emphasises that insurance cover does not reduce the importance of risk-mitigating measures in line with the institution's risk tolerance.

²⁴ Threat Intelligence-based Ethical Red Teaming

3.5. ICT operations

Finanstilsynet regards the challenges discussed in the points below as the biggest operational risks to the institutions' ICT operations. The importance of institutions identifying circumstances, both organisational and technical, that could threaten stable and secure operation is underscored.

3.5.1. Operating complex ecosystems

The integration of different service providers increases the risk of operating problems, partly because the service involves more systems that may fail and thereby make the service unavailable, and partly because multiple ICT service providers make it more complicated to maintain an overview of vulnerable components. New and more integrated solutions increasingly expose weaknesses in integrations with existing core systems. The number of integration points between different systems is increasing, partly because of the increased functionality of self-service channels. Extensive outsourcing and the use of cloud services create operational complexity and increased vulnerability. The pressure on the institutions' and service providers' delivery systems caused by large-scale changes also increases the risk of errors occurring.

The institutions' responses to the vulnerability survey show that systems portfolios are becoming increasingly complex, a fact that carries with it risks in a number of areas. Troubleshooting and problem-solving appear complex and demanding, and establishing good disaster recovery solutions is challenging. The institutions also see challenges in establishing comprehensive defences against cyberattacks. They also point out that compiling and analysing logs is demanding.

The complexity of the technological infrastructure also results in challenges with respect to carrying out thorough, comprehensive risk assessments of operations.

3.5.2. Phasing out of outdated systems

Inadequate documentation and access to personnel with the right expertise in outdated systems are creating challenges in the work of both phasing out and migrating functionality to modern development platforms. Maintenance costs for outdated systems are usually high, and maintenance support has ended for some systems. The system code has vulnerabilities due to the systems being developed at a time when security requirements were very limited.

In the dialogue with the institutions, it emerged that the phasing out of old systems entails complex operations and requires thorough planning. A high degree of integration between different systems and systems in the portfolio whose functionality and areas of application are unknown make the phasing-out work very difficult. Systems developed with modern technology and methods that are intended to replace old systems, present challenges because the systems that are being phased out have to be in operation while the new systems are put into production and undergo acceptance processes. In the experience of the institutions, these factors represent a risk of serious business disruption.

Finanstilsynet is aware that institutions are choosing to implement organisational changes in parallel with replacing outdated systems. However, this has been shown to present the institutions with additional and unnecessary challenges in their technological transformation. Finanstilsynet believes this is a factor that institutions must take into account in their risk assessments and planning to ensure the necessary coordination between technological and organisational restructuring projects.

3.6. Business continuity management and crisis management

3.6.1. Survey of the banks' crisis management capacity

In 2019, Finanstilsynet conducted a comprehensive survey of business continuity management and crisis management in Norwegian banks and international banks with branches in Norway. The purpose was to obtain information that would provide Finanstilsynet with a basis for assessing the extent to which banks are prepared for, and able to cope with, crisis situations.

The main focus was on managing serious ICT incidents in which a disaster recovery plan and possibly disaster recovery solutions would have to be deployed. The institutions also responded to questions about governance and organisation aimed at addressing the institution's overall efforts to prepare the institution for, and enable it to deal with, serious incidents defined as a crisis or disaster that will impact the institution's normal level of activity. This included, in addition to operational incidents, cyberattacks, natural disasters, terror, disease outbreaks affecting a large proportion of employees, threat situations, serious breaches of infrastructure such as networks and power, and disruption to critical ICT services.

Identified weaknesses

The analysis of the responses showed that the banks have generally established disaster recovery systems that will be implemented if normal operating systems are not available. The analysis clearly indicates that shortcomings exist that could present banks with challenges in dealing with a crisis, especially if the disaster recovery solutions must be deployed. This especially applies to banks with inadequate governing documents, training, practice, exercises and testing of disaster recovery solutions. The analysis also showed that the banks prepared few scenarios for training and exercises.

A business impact analysis (BIA) is a process used to identify the consequences of losing access to business-critical services and processes and to define the order in which services and processes should be re-established based on business criticality. BIAs provide a basis for preparing an institution's business continuity and disaster recovery plans. The analysis should include various scenarios and possible consequences of these scenarios.

Through its supervisory activities and dialogue with institutions, Finanstilsynet has found that it is difficult for the business side to understand and define the extent and impact serious incidents could have if they occur, including loss of data. The business side has little risk appetite for downtime, but identifying which business processes are the most important has proved to be challenging. The

analysis showed that institutions lack BIAs for critical business processes. The survey also showed that only one in three banks have assessed and analysed social consequences as part of their BIAs.

The analysis showed that most banks have made arrangements for alternative worksites, but one in three of the banks had not established procedures for implementing such a relocation process. One in four banks had not assessed the bank's ICT emergency preparedness. One in five banks lacked an overview of alternative personnel if, for a variety of reasons, employees are unavailable when the crisis occurs, or during the course of the crisis.

In Finanstilsynet's experience, the digitalisation of business processes has resulted in the business side entrusting even more of the work on BIAs to the IT department. It also appears that the institutions lack an overview of the impact studies that have been prepared, and the extent to which institutions have made aggregate and adequate assessments to maintain business operations in the event of breaches or disruptions in critical systems, and in cases where the institution is subject to a serious cyberattack. The impression was also given that the institutions do not have the necessary understanding of how a serious ICT incident should be handled in partnership with service providers. Furthermore, Finanstilsynet is left with the impression that the institutions focus too little on assessing changes in the impact study due to changes in the threat and risk picture.

The survey shows that the institutions must improve their efforts within business continuity management and crisis management, including risk assessments and impact studies, and emergency preparedness. Finanstilsynet points out that it is the responsibility of the board and management to ensure that an institution has established an organisation and infrastructure that ensures stable operating solutions, adequate emergency preparedness and effective disaster recovery systems, including in the event of serious crises.

3.6.2. Geopolitical factors

Finanstilsynet has previously pointed out the dependence on external service providers as a vulnerability if serious crises or disasters affect global operators that provide critical ICT services to the financial services industry. This is especially true if operational personnel in other countries are prevented from performing their tasks. Such incidents could present significant challenges in maintaining critical social services in a proper and secure manner, especially if the crisis persists. There was similar uncertainty concerning administration, including the management of serious failures and security incidents that could result in a need for close cooperation with multiple involved service providers in Norway and abroad.

Finanstilsynet found through the incident reporting that the institutions in partnership with their service providers are generally able to resolve quite serious interruptions to services. The coronavirus crisis has also shown that the institutions have maintained stable operations, see 2.4. However, there is some uncertainty about the degree to which the institutions would be able to restore operations in the event of ICT incidents or cyberattacks that cause serious disruption.

Finanstilsynet believes that institutions must take into account the fact that similar and more serious crises may occur in the future, and that in such situations the industry must be capable of maintaining the stable and secure operation of the financial infrastructure. This also entails verifying that emergency response personnel, technical infrastructure and disaster recovery plans are at all times at the level necessary to handle this type of situation. The institutions must also be capable of handling serious ICT incidents during any crises that occur. This will also apply to crises, including geopolitical factors, that result in foreign service providers being prevented from performing critical ICT services, see 3.4.2.

Finanstilsynet believes that the experience gained by the institutions and authorities from the coronavirus pandemic will be of great value in the institutions' evaluation and future strategies for outsourcing ICT services abroad.

Finanstilsynet expects the institutions and their service providers to conduct thorough evaluations of vulnerabilities, risks and consequences in light of the coronavirus pandemic. At the same time, Finanstilsynet underscores the importance of the institutions taking geopolitical uncertainty into account in their risk assessments and decision-making processes.

3.6.3. Working from home as part of disaster recovery solutions

Many companies have established solutions that allow tasks to be carried out by employees working from home. The solutions can also be used as part of an institution's disaster recovery solutions, where access rights to the institution's systems will depend on the specific situation.

To deal with the situation that arose with the coronavirus pandemic, many institutions allowed their employees and service provider personnel, including ones abroad, to carry out tasks while working from home. This included tasks within monitoring and operation of critical infrastructure. Such personnel often have broader access rights and may, in the event of misuse or errors, inflict damage to the institutions, e.g. interruptions to critical services. Finanstilsynet believes that allowing service provider personnel in high-risk countries to access an institutions' critical infrastructure and systems from their homes represents a particularly high risk.

Even with enhanced security measures, Finanstilsynet believes that vulnerability to unauthorised acts and cyberattacks may increase with the widespread use of working from home. Home networks usually have weaker security mechanisms than the institutions' internal networks. Technology connected to employees' home networks may have vulnerabilities that expose the network to cybercrime. A cyberattack on an institution's infrastructure combined with DDoS attacks on the home networks of emergency response personnel who perform important operational and security tasks with the objective of preventing task execution, may be a relevant threat scenario. Such attacks could also impact employees performing important business tasks.

Finanstilsynet assumes that the institutions have ensured that traffic is encrypted through VPN connections, that enhanced security measures, including monitoring and control, have been established, and that broader access rights cannot be used when using open networks.

3.6.4. National and international lines of communication

The financial sector relies on well-functioning electronic communication networks, both domestically and abroad. The fact that almost all traffic abroad is carried by a limited number of fibre connections from the Oslo area via Sweden represents a vulnerability for institutions that have their own or outsourced activities abroad, see report from the Norwegian Communications Authority (NKOM)²⁵. Reference is also made to the fact that climate change could result in serious natural disasters in Norway and our neighbouring countries, but also in India and regions such as the Baltics and Eastern Europe.

In 2019, the EFTA Surveillance Authority (ESA) approved support for increasing capacity by laying new sea fibre cables to other countries, which will help reduce the vulnerability of electronic communications to and from Norway.

Finanstilsynet points out that the vulnerabilities to which NKOM refers should form an important part of the institutions' risk assessments for disaster recovery solutions, and that the institutions must establish disaster recovery solutions that take into account interruptions to communications in Norway or to and from Norway. Finanstilsynet believes that 5G should be regarded as an important part of the emergency preparedness for communications for critical services.

3.7. Development and innovation

Technological advances are paving the way for new business models and increased digitalisation and automation. New actors with modern technical platforms are being established, and the competitive situation for the institutions has been changed by new actors establishing solutions in the interface between the institutions and the institutions' customers. The systems portfolio is complex and composed of old and new technology, different platforms and many providers in the value chain. These are factors that make great demands on development and management methodology.

Nevertheless, the responses to the vulnerability survey show that the institutions believe the risks associated with the complexity of the ICT systems are decreasing.

3.7.1. Development goals

Finanstilsynet believes it is important for boards and management to maintain a critical eye on which stakeholders create expectations and the need for faster and more extensive digital transformation, both within the institution and by external actors. If decisions are made on the wrong basis, it may cause institutions to establish strategies and change processes that result in costly, unnecessary and/or unsuccessful organisational and technological change projects.

²⁵[NKOMs årsrapport 2017](#) and [NKOMs årsrapport 2019](#)

Finanstilsynet believes that it is important that thorough analyses be conducted at an early stage of change and development projects in order to detect factors that constitute a risk of it not being possible to carry out projects as planned, or factors being identified that mean they cannot or should not be realised. This applies especially where new technology will be used.

3.7.2. Agile development methodology

Using agile development methodology, such as DevOps²⁶ (Development and Operations), requires the institutions and their service providers to adhere to strict guidelines to reduce the risk of applications being put into production with vulnerabilities, including security holes that can be exploited by criminals. In the traditional waterfall method, vulnerabilities in code have been identified by methods such as code audits and penetration testing, and through good change management.

The institutions' responses to the vulnerability survey show that increased requirements and the need for new solutions with short time to market can lead to high delivery pressure and poorer quality in the solution being developed.

The increased use of agile development methodology, where new functionality in the application is tested and put into production on an ongoing basis in order to be able to deliver new solutions and functionality to the market more quickly, may entail an increased risk of errors. This creates a need to adapt and incorporate the security aspect through the various development stages and in operational setups to reduce the risk of rapid development being at the expense of security. Finanstilsynet regards the failure to give the security aspect sufficient priority in demanding development projects with short deadlines in an increasingly competitive situation as a genuine risk.

Finanstilsynet underscores that it is the responsibility of management to ensure that security is a key function in all development projects, and that the necessary resources are provided to ensure that the level of security in all of the institution's systems is in line with recommendations and good practice. This also applies where third parties offer systems in the customer interface that are integrated through the bank's APIs.

Finanstilsynet believes that code reviews, which involve a thorough analysis of the source code with the aim of identifying vulnerabilities to unauthorised access or the exposure of personal data, for example through the use of security technology for scanning, should figure prominently in development processes and that these should be carried out in all stages of development. A code audit should also verify that the code complies with the standard used. Code reviews should also be carried out for systems and applications in production, as should penetration tests.

²⁶ <https://en.wikipedia.org/wiki/DevOps>

3.7.3. Digital transformation through the use of an application programming interface (API)

The use of APIs has become an important part of the financial services industry's digital transformation. Institutions communicate in 'dialogue mode' via system applications by making requests and receiving responses in real time. This enables institutions to distribute their services to their customers in new ways via partners. Subject to the customer's consent, other institutions (third-party providers) may provide services using other institutions' data, whether through regulated access, contractual access or in other ways.

APIs are increasingly being used in banking, insurance and payment and securities services, and this is often called 'open banking' or 'open insurance'. The regulation has come furthest within the area of payment services, where strict security requirements apply to the institutions, both those that hold the data and third-party providers who want access to the data, and the lines of responsibility are regulated. In sectors without established regulations, access to data must be secured through agreements that also address security and responsibilities.

While GDPR gives customers ownership of, and the right to access, their own data, it is important that this access is provided in a proper manner. The obligations of the institutions are clear when it comes to storing and protecting customer data, see section 5 of the ICT Regulations, and include ensuring that these do not fall into the hands of unauthorised people and are not used for purposes other than those for which consent has been given. If a customer has given a third party consent to access his/her data, whereby it is authorised to act on behalf of the customer, the institution holding the data is nevertheless required to ensure that the third party identifies itself on a par with the requirements for proxy situations in general.

Where access is regulated, strict requirements apply stating that third-party providers that are granted licences must have well-documented procedures, including with respect to ICT security. Where access is not regulated, the institutions that hold data through agreements have a responsibility to assure themselves that ICT security is being addressed and that third-party providers are also adequately addressing ICT security.

Although the use of APIs has several advantages, its use also carries risks and challenges, both for the institutions and for customers. The institutions must manage the risks that come with more sharing of customer data and increasing connectivity to other institutions, and take appropriate risk-mitigating measures in line with assessments made in risk analyses, balancing security against user-friendliness. The use of APIs can complicate the design of good disaster recovery solutions and make it challenging to establish comprehensive defences against cyberattacks. The overview of third parties may be limited, especially where access is not agreement-based. Many technical service providers, also those from different legal jurisdictions, may be involved in the value chain, which can make it complex to monitor. The lines of responsibility become more complicated when the number of actors increases. Even if rules are established for the delegation of responsibilities, the institutions' reputational risk may increase.

The more institutions the data are shared with, the more vulnerable the systems become to data breaches. The attack surface will be changed in that criminals will also be able to target third-party providers. Attacks may take place through the exploitation of vulnerabilities in third-party applications, and customers may be more exposed to social engineering. The institutions' challenge is first and foremost to ensure that the security requirements in the new ecosystem are understood correctly by the institution holding the data, the individual third party and the customers who use third-party solutions.

3.7.4. Use of new technology

Data-driven institutions take a fact-based approach where the institution uses the available internal and external data (big data) to support decisions rather than using judgement and speculating. The available technology is used to help with this work with the goal of reducing costs, increasing revenues, improving customer experiences and/or improving the precision of decision support. The technologies and services intended to ensure goals are achieved include cloud services and technologies (Cloud), robotic process automation (RPA), big data, efficient analysis tools (including the use of artificial intelligence and machine learning), blockchain and the Internet of Things (IoT).

The aforementioned technologies, and the services that were developed based on the technology, each have their own complicated risk picture. When institutions link up multiple new technologies in system solutions, a multifaceted risk picture arises. The risk picture is further complicated if the institution receives or procures the same type of service/technology from multiple suppliers. At the same time, it is important to underscore that new technologies will also mitigate risk, e.g. by replacing manual analyses and tasks.

When institutions assess the risk picture for the services and technologies that are in use, it will be difficult to establish an overview and control of all of the risks. The risk picture must be viewed in relation to how the technology is used and the degree to which the technology's potential is utilised. Therefore, in their risk work, the institutions should identify the risks associated with the services and technical solutions in use. One practical approach is to assess the risks in individual business processes, ensuring that you identify risks that span IT systems, technologies and service provider relationships.

Regulatory development

Technological advances and changes to the risk picture are resulting in a need for regulatory changes. In order to meet the institutions' challenges associated with the implementation and use of new technology, Finanstilsynet plays an active role in European supervisory authorities' (EBA, EIOPA, and ESMA) projects and working groups that develop and establish regulations, guidelines and technical standards for the application of technology. Relevant topics include PSD 2, open banking, secure customer identification (KYC), safe payment card usage, big data, advanced analysis (AI, ML), ethical use of ICT, incident reporting and security work (TIBER/TLPT).

Finanstilsynet's regulatory sandbox enables institutions to try out new, innovative products, technologies and services under the supervision of Finanstilsynet. The regulatory sandbox can also help to improve Finanstilsynet's understanding of new technological solutions in the financial market and provide Finanstilsynet with valuable insight into the associated risk.

Irrespective of which new technologies the institutions adopt, the principles of prudent business, usage control, solution security and business continuity apply, and equal risks should be treated equally.

3.8. Logical access management and control

Vulnerabilities associated with inadequate access management represent a risk of breaches of data security, including breaches of confidentiality, integrity and availability. The consequences of such breaches may include reputational loss, fines due to breaches of regulatory requirements, unauthorised acts that can lead to serious business disruption and cybercrime.

Finanstilsynet has identified cases where the distinction between development environments and test environments is lacking and where there are no periodic reviews of all critical access rights.

The institutions' responses to the vulnerability survey show that the risk associated with access control is increasing. Finanstilsynet believes this may be due to the fact that the institutions are increasingly outsourcing services and purchasing services where external consultants are granted temporary access.

Finanstilsynet underscores the importance of people with broader access rights being subjected to special background checks prior to their allocation, and that continuous controls are made on who has received the access rights and whether the needs correspond at all times with the tasks that must be carried out. This is especially relevant where employees change tasks, switch departments or leave. Finanstilsynet assumes that an institution and its service providers will utilise special systems for managing these types of access rights.

3.9. Physical security and access control

3.9.1. Physical access control

Through its supervisory activities, Finanstilsynet has observed that visitors to institutions who must be granted temporary access to the institution's premises are not asked to provide a valid ID upon registration, which may entail a risk to the institution's ICT operations.

Finanstilsynet believes that there is a real risk of devious criminals, for example, pretending to be consultants or advisers from reputable companies and exploiting the institutions' lack of visitor controls. Criminals may be able to acquire information through physical social engineering that they could use for planning criminal acts, including cyberattacks.

Finanstilsynet advises institutions to consider the need to tighten controls in cases where, for example, visitors could acquire information that may be used to harm the institution or connect to the

institution's ICT systems without permission using, for example, a keylogger²⁷(also referred to as keyboard or key stroke logs).

3.9.2. Intruders

It is difficult to determine or anticipate how exposed an institution is to terrorist attacks or unstable individuals who choose to inflict harm on employees or service provider personnel or damage critical infrastructure by entering the institution's premises. At the same time, Finanstilsynet believes that institutions cannot disregard the fact that this type of incident may occur.

Through its supervisory activities, Finanstilsynet has observed that institutions have few physical safeguards that would limit the ability of intruders to enter premises by force. The institutions do not consider hardened protection, for example using Mantrap²⁸, for access to locations where critical functions are performed to be necessary and have given little or no consideration to establishing procedures, including for shutdown and evacuation of employees, for this type of situation.²⁹ As far as physical access control for data centres is concerned, Finanstilsynet believes that this is generally well addressed.

In the worst case scenario, vulnerabilities in physical security can result in, for example, critical IT personnel being impacted, with severe consequences for people and ICT operations. Finanstilsynet believes that the institutions should consider establishing shutdown and evacuation procedures, and that these should be part of the institution's business continuity plan on a par with procedures in case of fire and bomb threats.

3.10. Change management and security updates

3.10.1. The change process

Vulnerabilities associated with inadequate change management represent a risk of unauthorised changes occurring, and of changes with vulnerabilities or faults being released into production. New regulatory requirements, a faster pace of change and more rapid development of new solutions, see 3.7.2, are all factors that increase the risk of vulnerabilities being introduced in connection with changes to ICT systems as a consequence of too weak governance.

Both functional and non-functional changes represent a risk if the changes are not subject to control at all stages, from the change being proposed to the change being tested and put into production. Good change management is one of the most important factors in ensuring continuity of the institutions' business processes.

²⁷ https://en.wikipedia.org/wiki/Keystroke_logging

²⁸ [https://en.wikipedia.org/wiki/Mantrap_\(access_control\)](https://en.wikipedia.org/wiki/Mantrap_(access_control))

²⁹ [Example of key and important aspects of a terrorist situation](#)

In Finanstilsynet's experience, both serious and less serious errors that arise from changes, see chapter 5, are often due to deficiencies in the controls that are expected to be carried out, or a failure to adequately comply with the institution's guidelines. The institutions and its service providers usually have documented processes and tools to ensure that the controls cannot be bypassed. Finanstilsynet found that the incident reporting indicates that unauthorised changes occur without this necessarily being detected until afterwards and that the controls carried out are not of the required quality. The consequences are instability and downtime.

Finanstilsynet believes that a fast pace of change increases the risk of development and test teams not being given the time necessary to ensure that all aspects of the solutions have been addressed with the expected quality. The institutions' responses to the vulnerability survey show that the institutions find the scope of changes challenging. They also indicate that delivery pressure and new regulatory requirements represent a risk for development processes.

3.10.2. Security updates (patches)

Inadequate procedures for security updates (patches) constitute a major vulnerability for the institutions' ICT operations. This, therefore, makes great demands on the institutions' and service providers' governance with respect to security updates (patch management). Since vulnerabilities that are identified in applications, operating systems and hardware components are made public, criminals will quickly attempt to exploit the security holes. Response times, i.e. the time from when a vulnerability becomes known to when the security update has been tested and put into production, are critical for avoiding that institutions are exposed to attacks targeting identified vulnerabilities.

In Finanstilsynet's experience, institutions choose to postpone security updates for a variety of reasons. It is stressed that institutions should ensure that risks associated with reported security updates are assessed and classified, and that the consequences of delaying updates are highlighted. The institutions have an independent responsibility to ensure that their service providers have established routines and controls for this work.

3.11. Data and information

3.11.1. Data management

Management of the institution's data (data management) and customer data includes ensuring that the data are protected, available, reliable, used correctly and stored in the correct locations. The institution's data are of high value and require good management.

The institutions' responses to the vulnerability survey show a trend whereby data quality is deteriorating. The institutions recognise that ensuring good data quality is challenging and make clear that measures for improving data quality must be continued.

Several factors can reduce data quality and increase risk in a number of areas, e.g. by credit ratings or anti-money laundering controls being conducted on the basis of inadequate or incorrect data. This may

also result in risk assessments, and measures resulting from risk assessments, being based on inadequate or incorrect information.

Finanstilsynet believes it is important that the institutions continue their efforts to improve the quality of their data.

3.11.2. Securing data (backups)

Ransomware³⁰ is a form of malware that may cause systems and/or data to become unavailable to users. This is done by an attacker locking the systems, stealing data, deleting data or encrypting data, and then demanding money for the return of the systems and data to the institution/users. Even if an institution that finds itself in such a situation chooses to accede to the demands, there is no guarantee that access will be restored.

Finanstilsynet points out that cloud services synchronise files when files change, including when they are encrypted or damaged without authorisation. It is assumed that similar solutions will be used for business applications and customer data uploaded to the cloud.

Concerns were raised in Finanstilsynet's dialogue with the institutions about the increased use of online solutions for backup and the risk this constitutes with respect to the loss of both production data and backup data in the event of an attack. Institutions are also concerned about the potential consequences of a comprehensive attack on a cloud provider, or attacks against mainframe and Unix service providers. The loss of both production data and backup data would naturally have very serious consequences for the affected party.

Finanstilsynet underscores the importance of institutions basing their backup strategies on ensuring that all critical data, cf. classification of information and code, must protect the institution against loss of data through attacks and other adverse incidents. Such measures can include segmentation between systems and the backup solution (offline solutions) or securing of file systems by ensuring that files cannot be overwritten until a backup has been made.

Furthermore, the institution itself must take responsibility for regular testing to verify that restoration from backups functions as intended. This should form an important part of the institution's internal control.

3.12. Transaction monitoring (AML)

In 2019, Finanstilsynet conducted more thematic inspections of governance in relation to the risk of money laundering and terrorist financing than in any previous year. Assessing electronic customer and transaction monitoring was one of the control areas in these inspections. Banks, mortgage companies and finance companies are required to have electronic monitoring systems in place to detect circumstances that are potentially indicative of money laundering and terrorist financing. However,

³⁰ <https://en.wikipedia.org/wiki/Ransomware>

additional supervision is carried out where institutions use electronic systems to meet other statutory obligations.

3.12.1. Quality of customer and transaction controls

In many of the inspections, Finanstilsynet pointed out a lack of references between identified risks and established rules and has questioned whether the rule setting adequately addresses the risks. In many cases, the institutions had not taken full advantage of all the functionality that exists in the AML system to design targeted rules. In several cases, the quality of the institution's electronic customer and transaction monitoring was too low and may have resulted in inadequate ongoing monitoring of customers and transactions. For example, there were deficiencies in the rule setting in the system, including a lack of industry-specific rules, self-produced rules, established thresholds for customers subject to enhanced control, and customer-specific rules. Finanstilsynet also pointed out that institutions had too few dedicated rules in the individual business areas. Finanstilsynet has noted that banks have increased their analytical resources in this area and are testing the use of systems based on machine learning and artificial intelligence to adapt the rules to customers' expected transaction patterns.

It is evident from the institutions' responses to the vulnerability survey that they face challenges with regard to obtaining good, overall data bases, and designing good queries, in order to extract the correct information when it comes to suspicious transactions. Both inadequate systems support and challenges have been reported in relation to the data used as a basis for the analyses.

3.12.2. Quality assurance and follow-up of the rules

Finanstilsynet also pointed out the importance of testing the rules and regularly evaluating the effects of the rules. Finanstilsynet carried out spot checks of the documentation of the implementation of certain rules, and shortcomings were found in their implementation. Furthermore, there are often too many rules with few hits or with very many hits over time, which may indicate that the rules are not very accurate. These factors may result in the rules not identifying the risk they are meant to reveal.

3.12.3. Operation of electronic customer and transaction monitoring systems

Serious deviations related to a lack of monitoring were uncovered in 2019, see 5.2. The greatest risk of inadequate customer and transaction monitoring is that customers and transactions are not included in the data extracted from the source systems and thus are not controlled. Deviations in 2019 arose due to changes in the source systems and failure to make corresponding adjustments to the information extracted from the AML system. Inadequate controls also occurred as a result of errors following changes to the AML system. Shortcomings in customer and transaction monitoring were identified by the internal control in the institution some time after the error occurred. The institutions must improve the acceptance testing of system changes that can affect AML controls so that errors are identified prior to the production phase.

During the inspections, Finanstilsynet also asked questions about the AML systems' access management, pointing out that no more people than necessary should have access to each level of authorisation in the AML system. Finanstilsynet sought controls that would detect or prevent employees deliberately or unconsciously turning off the transaction controls for longer or shorter periods.

3.12.4. Transaction monitoring and customer assessments using artificial intelligence

Assessing customer behaviour based on transaction history and other customer-specific data is challenging for the banks. In many cases, these data are very complicated. Finanstilsynet found that the use of machine learning and artificial intelligence in transaction monitoring is being discussed, and that there is an international trend in banks towards replacing traditional customer assessments and rules for transaction monitoring with systems based on machine learning and artificial intelligence. Finanstilsynet believes that the challenges presented by a high number of false positive hits, as well as the challenges associated with analysing sufficient amounts of data to classify customers according to risk and intercept suspicious activities such as illegal activities or terrorist financing, can be mitigated by the use of artificial intelligence.

3.13. Risk associated with the institution's customers

3.13.1. Login information going astray and fraudulent use of BankID

The increased digitalisation has led to the institutions' customers often having no choice but to use digital identification and authentication systems to gain access to the services. This means that customers with little digital experience are especially vulnerable, see 3.13.6.

Passwords and PIN codes may be difficult for some to remember, and a customer may choose to write this information down. Close relations may have access to each other's digital ID and authorisation codes, and people who are not computer-literate may hand over their digital signature to others to carry out their financial transactions. This results in a risk of the information falling into the hands of unauthorised people and of the customer being defrauded, either by close relations or by others. Fraud in close relationships where funds are used for gambling is a familiar scenario. If unauthorised people gain access to someone else's BankID, this can be misused in many areas, such as entering into loan agreements, purchase contracts, taking out insurance and trading. Fraud statistics for the second half of 2019 show that the figure for fraud involving account transfers where the cause was 'fraudster issues the payment order' was almost NOK 42 million. The highest proportion of this is believed to be fraud where the customer is deceived into handing over their security devices.

3.13.2. Measures for reducing fraud and fraudulent use

Maximum amounts have been set for many of the services by the institutions, partly based on regulations and/or the customer profile, in order to reduce fraud and fraudulent use of payment services, and good monitoring procedures have been established by payment service providers. As far

as other services are concerned, similar measures have been established that may help to reduce fraudulent use.

3.13.3. Social engineering

Fraud statistics for 2019 show that once again social engineering accounted for the highest proportion of losses. Reported figures indicate losses of more than NOK 500 million in 2019, while by comparison, losses due to payment card fraud were around NOK 190 million. Fraudsters are adaptable and develop fraud scenarios based on what they assume will reap the greatest gains at any given time. 2019 saw heavy losses from CEO fraud, invoices with fake payee accounts and investment firms, while losses from love scams were lower than the year before.

The situation is often experienced as very difficult for those who have fallen victim to social engineering and those close to them. Finanstilsynet is aware that banks contact the customer where a suspicion arises that the customer is at risk of social engineering. At the same time, it is difficult for banks in some cases when a customer does not realise, or will not accept, that manipulation and fraud lie behind the cash transfers. Since this type of fraud is steadily increasing, Finanstilsynet urges institutions to continue to work on finding effective measures for the various customer groups.

3.13.4. Customer interface through new service providers

The scope of third-party service providers offering solutions where customers can operate their customer relationships or use financial services is increasing, see 3.7.3. It may be difficult for customers to understand whether the service provider is subject to statutory financial regulations and whether the service being used is properly managed in line with the regulations or agreements entered into between the parties.

When services from third-party service providers are used, customers may not know where to turn if they fall victim to cybercrime or if serious incidents result in a lack of access to their customer relationships or financial services.

Finanstilsynet believes that existing actors, such as banks and insurance undertakings, and the new actors both have a responsibility to provide good customer information and ensure that customers are informed about actual conditions and what these entail.

3.13.5. Communication with customers via email

Finanstilsynet receives enquiries from customers expressing concerns about banks sending information by email that the customer considers sensitive. This could be, for example, information about the customer's cash withdrawals or account information being sent unencrypted via email. Customers are afraid that this type of information will go astray and could be exploited by criminals. Finanstilsynet expects institutions to exercise caution in their communication with customers, and ensure that secure channels are used, such as customer portals, in line with personal data protection rules.

3.13.6. Analogue customers

According to the Norwegian Pensioners' Association there are currently at least 200,000 non-digital senior citizens (analogue customers). The Norwegian Pensioners' Association points out that this group relies on digital help from relatives, neighbours, volunteers and friends, which represents a risk of fraud, see 3.13.1.

Finanstilsynet discussed bank customers in Norway who did not use the banks' digital services in RVA 2017. The reasons for this may include it being difficult and that there is a lack of willingness to facilitate simple digital solutions for senior citizens and others who for various reasons cannot use today's solutions. This could be compounded in an emergency situation, such as the current coronavirus pandemic, where senior citizens are less able to take advantage of traditional payment services such as giro sent by post, over the counter payments or ATM withdrawals. Finanstilsynet believes the institutions have a responsibility to address the needs of these customers, even when they are unable to use analogue banking.

Finanstilsynet believes that technological cooperation between different industries will be able to help to establish simple, integrated digital solutions that can meet the needs of analogue customers. These could be solutions for ordering food, products from pharmacists, banking services and notification services.

3.13.7. Identification controls for analogue customers

In the autumn of 2019, Finanstilsynet received questions from private individuals and the media related to some banks' requests for some customers to re-identify themselves and the publication of a form for re-identification on banks' websites. The requests were made in order to comply with the requirement for ongoing customer monitoring in accordance with section 12 of the Anti-Money Laundering Act. The re-identification requirement concerned bank customers who had not established BankID access but nevertheless had access to online banking, and who would have difficulty meeting up at a bank in person. However, when the banks asked customers to send identification information via a means which is often used by fraudsters, and which banks in other contexts warn customers against using, this caused some uncertainty among customers. Finanstilsynet's view was that such solutions for re-identifying customers should not be used and that secure channels should be used. The relevant banks had to find other solutions for verifying identity for this customer group.

3.13.8. Lack of trust resulting from operational incidents

ICT incidents may result in users being unable to complete their financial services as planned. Serious ICT incidents can also cause disquiet. Finanstilsynet is regularly contacted by customers who are concerned about the security associated with the use of the services and information about their customer relationships, lack confidence in the service provider and are uncertain about the correctness of the information provided. Several of the incidents in 2019, see 5.2, describe cases in which customers have been unable to use the service as planned or have been unable to trust the correctness of the information.

3.13.9. The institutions' integrity as a result of cybercrime

Cybercrime or serious ICT incidents can create uncertainty among users of financial services. Finanstilsynet has been contacted by customers worried about losing their money in the event of such incidents. Finanstilsynet is aware that customers in such situations have made substantial cash withdrawals or have wanted to transfer funds to currencies other than NOK. This is a concern that the institutions need to take seriously.

4. Fraud and fraud statistics

4.1. *New reporting of fraud statistics*

The reporting of losses resulting from payment service fraud was changed from and including the second half of 2019. In the first half of 2019, reports were submitted to Bits AS³¹ in the same format as in previous years. From and including the second half of 2019, reports are submitted to Finanstilsynet in line with the revised Payment Services Directive (PSD 2).³² Therefore, the figures for the second half of the year are not directly comparable with the figures reported for previous periods.

According to section 2 of the Regulations on Systems for Payment Services, banks, financial institutions, e-money institutions, payment institutions and branches of such institutions headquartered in another EEA state must submit fraud statistics to Finanstilsynet at least once a year. Finanstilsynet has decided that the institutions must submit fraud reports semi-annually. This is a continuation of previous practice involving the semi-annual reporting of fraud to Bits AS.

PSD 2's guidelines for reporting fraud include requirements to report fraud statistics from payment service providers to national authorities and to report aggregated data from national authorities to the EBA and ECB. The reporting is more comprehensive than previous reporting and has been challenging for the institutions to implement.

The institutions must report both the total volume of transactions and the volume of fraudulent transactions. This makes it possible to estimate fraud as a proportion of the total transaction volume. Both the value of the transactions and the number of transactions must be reported. The reporting also distinguishes between domestic transactions, cross-border transactions in the EEA and cross-border transactions outside the EEA. Furthermore, fraudulent transactions are classified into three categories based on whether the fraudster issues the payment order, changes or modifies the payment order, or manipulates the payer into issuing the payment order.

4.2. *Losses associated with the fraudulent use of payment cards*

Reported losses from card fraud amounted to just under NOK 95 million in both the first and second half of 2019. This is an overall increase of 28 per cent from 2018. Comparisons with previous years, as well as between the first and second half of the year, are subject to some uncertainty because the reporting was changed from the second half of 2019. The figures show total losses for payment cards for Norwegian customers in recent years, irrespective of whether the loss was covered by the customer, the bank or the payment card company.

³¹ The banking and financial services industry's infrastructure company (Bits AS) www.bits.no

³² Article 96 no. 6, with the associated guidelines on fraud reporting: <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2>

The figures for the first half of 2019 show an increase in losses from the fraudulent use of payment cards compared with previous years. There was a particular increase in the fraudulent use of card details in online transactions, which also accounted for the highest losses in the first half of 2019, see table 4.1. The figures for the first half of 2019 indicate an increase in the number of payment cards subject to fraudulent use, see table 4.2.

Table 4.1 Losses from fraudulent use of payment cards

Type of payment card fraud (amounts in NOK thousands)	2015	2016	2017	2018	First half of 2019
Fraudulent use of card details, Card-Not-Present (CNP) (online transactions, etc.)	98,410	137,015	102,908	114,932	76,546
Stolen card details (including skimming ³³):					
- Fraudulent use with counterfeit cards in Norway	2,670	1,360	483	3,304	1,298
- Fraudulent use with counterfeit cards outside Norway	48,447	41,762	17,452	11,203	2,613
Original card lost or stolen:					
- Fraudulent use with PIN in Norway	18,875	12,857	10,194	9,676	9,146
- Fraudulent use with PIN outside Norway	14,224	10,223	9,663	7,696	3,327
- Fraudulent use without PIN	6,033	3,286	4,891	1,921	1,536
Total	188,659	206,503	145,591	148,732	94,466

Sources: Finanstilsynet and Bits AS

Table 4.2 Number of payment cards subject to fraudulent use

	2015	2016	2017	2018	First half of 2019
Number of cards subject to fraudulent use	44,900	68,162	65,024	60,266	39,918

Sources: Finanstilsynet and Bits AS

Reported losses from card fraud in the second half of 2019 amounted to just under NOK 95 million. This represents 0.02 per cent of the total value of transactions involving payments made by payment cards in this period. The proportion of fraud is highest for remote payments without strong customer authentication (SCA), a category that mainly includes online transactions. In this category, fraud accounted for 0.09 per cent of the value of transactions.

³³ [Wikipedia: Skimming \(fraud\)](#)

Table 4.3 Transactions and fraudulent transactions with payment cards reported by card issuer in the second half of 2019

Transaction value in NOK 1,000	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total transactions
Card payments (issuer)				
Total	414,632,690	103,472,005	12,385,305	530,490,001
Of which fraud	7,091	67,236	20,354	94,681
Of which initiated electronically:				
Fraudster issues the payment order, of which	8,447	48,593	15,855	72,896
- Lost or stolen card	2,091	3,831	915	6,837
- Card not received	1,122	961	327	2,410
- Counterfeit card	69	451	1,034	1,554
- Theft of card details	2,411	36,383	12,127	50,921
- Other	2,650	6,953	1,453	11,056
Fraudster changes or modifies the payment order	22	549	1,668	2,239
Fraudster manipulates the payer into making a card payment	49	6,886	393	7,328
Remote payment without strong customer authentication (SCA)				
Total	23,266,936	28,853,569	3,275,446	55,395,951
Of which fraud	2,500	34,749	12,033	49,282

Source: Finanstilsynet

Around 40,000 cards were reported as having been subject to fraudulent use in the first half of the year and around 110,000 fraudulent transactions with cards were reported in the second half of 2019. The ‘increase’ must be viewed in the context of the fact that according to the guidelines the number of fraudulent transactions must now be reported and not just the number of cards subject to fraudulent use.

0.007 per cent of the total number of transactions with payment cards in the second half of 2019 were fraudulent. The average value of a fraudulent transaction with a payment card was NOK 856, while the average value of a transaction with a payment card was NOK 327.

Table 4.4 Number of transactions and fraudulent transactions with payment cards reported by card issuers in the second half of 2019

Number of cases	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total	Fraud (%)
Total	1,339,988,557	259,784,056	18,990,578	1,618,763,191	
Fraud	10,796	69,702	30,082	110,580	0.007

Source: Finanstilsynet

4.3. Losses from online banking fraud

Losses related to online banking amounted to NOK 3.6 million in the first half of 2019, which is low compared with previous years. The reported figure for the second half of the year is substantially higher, with losses related to account transfers of more than NOK 300 million.

As previously mentioned, the reported figures for the first and second halves of the year are not directly comparable. This is primarily due to the fact that the figure for the second half of the year includes losses resulting from social engineering, which the banks previously reported as a separate figure. The loss figure for account transfers less losses due to social engineering for the second half of the year is around NOK 46.5 million. While previously only banks reported loss figures, the reporting now encompasses all institutions that provide payment services. The reporting on account transfers also includes online banks, mobile banks and other platforms. The figures show total losses for online banking fraud for Norwegian customers in recent years, irrespective of whether the loss was covered by the customer or the bank.

Table 4.5 Losses related to online banking (amounts in NOK thousands)

Type of fraud – online banking (amounts in NOK 1,000)	2015	2016	2017	2018	First half of 2019
Attacks using malware on customer's PC or security device	3,055	2	727	1,252	201
Lost/stolen security device	963	8,758	1,892	1,959	69
Phishing and false BankID – merchants	5,815	2,428	2,057	16,858	1,435
Other/unknown	2,715	7,444	2,911	6,723	1,932
Total	12,548	18,632	7,587	26,840	3,637

Sources: Finanstilsynet and Bits AS

Table 4.6 Transactions and fraudulent transactions for account transfers (online banking, etc.). Second half of 2019

Account transfers initiated electronically (amounts in NOK 1,000)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total	Fraud (%)
Total	188,219,191,694	25,188,476,543	5,978,582,637	219,386,250,875	
Fraud	41,716	130,886	129,027	301,629	0,00014
Of which different types of fraud:					
- Fraudster issues the payment order	21,297	9,700	10,876	41,873	
- Fraudster changes or modifies the payment order	475	4,069	0	4,544	
- Fraudster manipulates the payer into issuing the payment order	19,944	117,944	118,151	256,039	

Source: Finanstilsynet

4.4. Losses from social engineering fraud

There was a further increase in social engineering fraud in 2019, i.e. where the fraudster manipulates the payer into carrying out a transaction. The reported figures indicate losses of more than NOK 500 million compared with just under NOK 300 million in 2018. It appears that social engineering fraud is a profitable method for criminals. The losses from cross-border transactions in and outside the EEA were approximately the same, but the losses from domestic transactions were significantly lower. Losses due to social engineering primarily involve account transfers (online banking, etc.).

Figures for social engineering fraud are subject to a high degree of uncertainty because payers must bear the losses themselves and many frauds of this type are probably not reported to banks. It is likely that the actual losses are higher than reported. The defrauded customers often contact their bank to ask them to stop transactions and reverse the transfer of funds. Banks also alert customers when, based on their knowledge of a customer, they identify repeated transactions that are abnormal for that customer.

The reporting in line with the guidelines does not distinguish between the different types of social engineering. Finanstilsynet believes that breaking down the manipulation of users into subcategories, as presented in the RVAs for 2017 and 2018, provides information that is important in understanding the fraud picture. Therefore, Finanstilsynet asked major banks and banking groups to report this separately for 2019. The percentage distribution of subcategories of social engineering reported by these institutions is believed to be fairly representative of the distribution for all institutions and is shown in the table below. In 2019, the highest losses were from CEO fraud and fraud involving changing the payee account, while in 2018 the highest losses were from love scams and investments in fake companies.

Table 4.7 Losses from social engineering of payers by subcategory

	2018	2019
Payment for renting an object the payee does not own	0.3%	0.2%
Deposits in response to promises of large payments later	3.1%	2.4%
Love scams	29.7%	8.7%
Investments in fake companies	31.0%	19.8%
Payment for goods not delivered	4.0%	0.8%
Payee account changed	2.9%	22.7%
CEO fraud	11.4%	37.6%
Fraudulent invoices	11.1%	4.1%
Other/new types	6.6%	3.7%

Source: Finanstilsynet

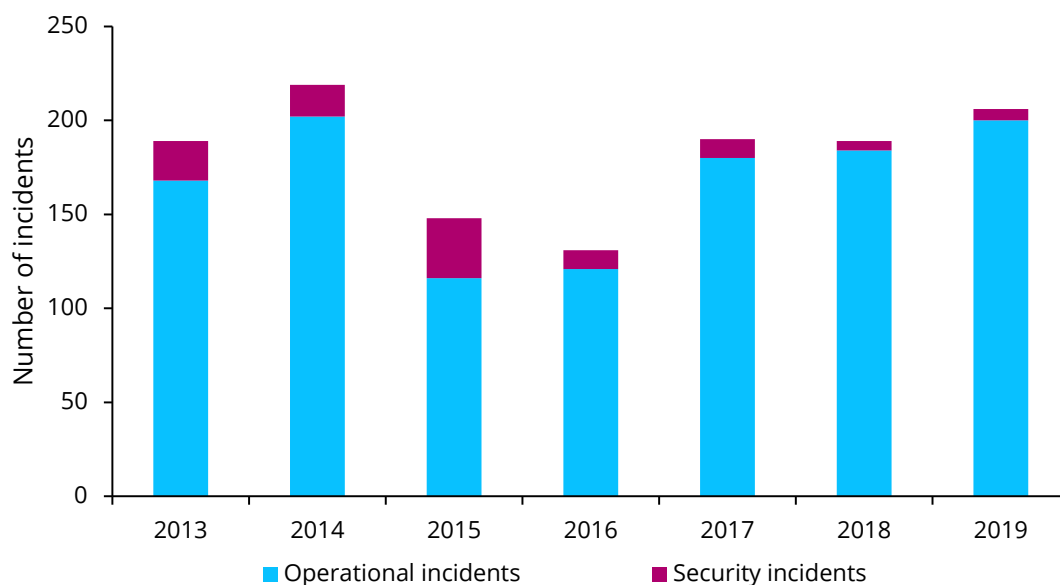
5. Incidents reported in 2019

5.1. Incident statistics

In 2019, financial institutions reported 206 ICT incidents to Finanstilsynet, which was 17 more than the year before. The number of obliged entities increased from 2018 to 2019, and on several occasions Finanstilsynet received reports about the same incident at the institutions' common service providers from multiple investment firms or banks.

There were no protracted incidents in 2019 that impacted the availability of the payment services of many banks simultaneously. In Finanstilsynet's opinion, the availability of payment services and other customer services was somewhat better in 2019 than in 2018.

Figure 5.1 Incidents reported by operational incidents and security incidents



Source: Finanstilsynet

Compared with previous years, Finanstilsynet received more reports of incidents that impacted factors other than availability in 2019. For example, the number of reported incidents and/or irregularities in systems for electronic customer and transaction monitoring increased.

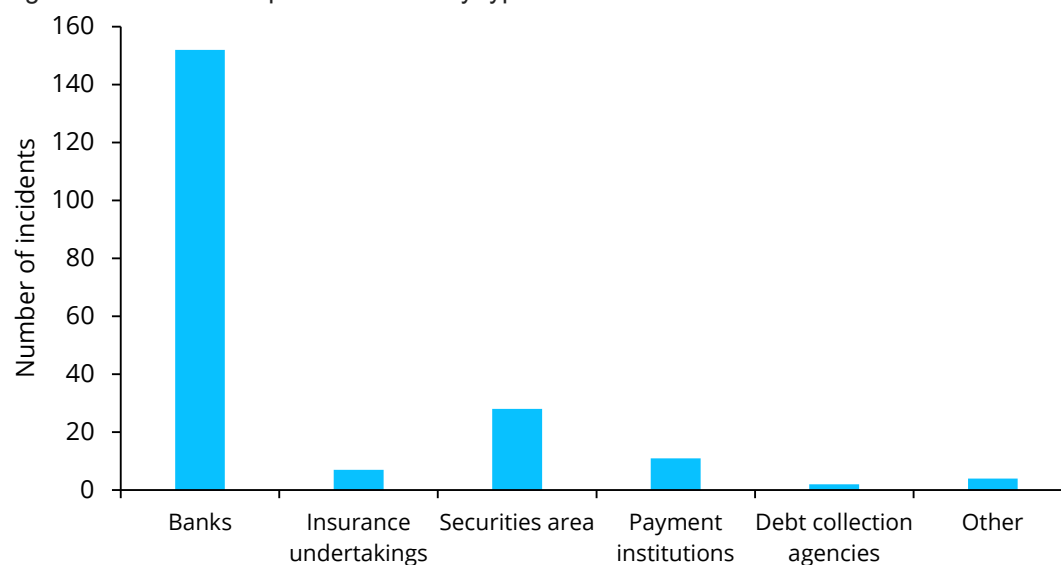
Figure 5.2 shows that the banks accounted for 75 per cent of the incidents reported in 2019.

Table 5.1 Number of incidents reported

Year	Operational incidents	Security incidents	Total number of incidents
2013	168	21	189
2014	202	17	219
2015	116	32	148
2016	121	10	131
2017	180	10	190
2018	184	5	189
2019	200	6	206

Source: Finanstilsynet

Figure 5.2 Incidents reported in 2019 by type of institution



Source: Finanstilsynet

5.2. Incidents with particularly serious consequences

Network problems in Gjensidige Forsikring AS

Gjensidige was struck by serious network problems on Friday, 8 March and Saturday, 9 March 2019. From Friday morning at 07:00 to 02:30 on Saturday, it was not possible to log in to either the bank's or the insurance company's websites. The intranet was also unavailable. The incident proved to be due to the upgrading of a security solution but did not have consequences before a number of days after the upgrading itself.

Vipps 17 May

In the middle of the busiest period of 17 May, Norway's national day, Vipps stopped working for payments from people to companies, meaning that users were unable to pay for soft drinks, hotdogs

and ice cream. The problem lasted for around an hour. Vipps had increased capacity in order to meet the expected increase in demand on 17 May. However, the capacity of one component that Vipps did not know was of importance for the capacity of the payment solution was not increased.

Double charges – VISA

On 22 and 23 May 2019, DNB experienced problems with VISA card reservations. The reservations were not deleted once the capital transactions had been posted. The affected customers saw amounts being charged twice and some customers' account balances dropped below zero. The bank spent longer than expected sorting things out and deleting the reservations. It was not until the afternoon of 23 May that it could verify that all accounts had been updated with the correct balance. The error revealed weaknesses in the bank's change management and testing.

Incorrect implementation of eInvoice service

In July 2019, Finanstilsynet received an incident report from Vipps and enquiries from end users about eInvoices being shared with people other than the person named as the recipient on the invoice and about the correct eInvoice recipient not receiving the invoice. The problem associated with the banks' 'Yes Thank You to All eInvoices' service became especially visible when Vipps introduced its 'invoice payment' feature in the Vipps application with the simultaneous option for 'Always Vipps eInvoice'.

It is supposed to be possible to enter into an eInvoice agreement on behalf of someone else for bills from a specific issuer, so-called 'Yes Thank You to Specific eInvoices', but the option should not be possible with the 'Yes Thank You to All eInvoices' option turned on. However, some banks had implemented 'Yes Thank You to All eInvoices' incorrectly. This resulted in customers who had paid a single paper bill on behalf of someone else also receiving subsequent bills from this issuer, who billed them rather than sending the bill to the addressee on the bill. The banks' common rules for eInvoices are set by Bits AS. Finanstilsynet has followed up Bits AS, which has implemented measures and monitoring with respect to both the banks and bill issuers.

Incidents related to the banks' electronic customer and transaction monitoring systems for detecting money laundering and terrorist financing (AML systems)

More incidents related to discrepancies in the banks' AML systems were reported in 2019 than in any previous year. This may be due in part to the fact that the attention paid to this area has increased in recent years. The incidents reported in 2019 concerned errors in the data retrieved from the banks' source systems for the AML system, errors following changes in the AML system itself and operational errors. The consequences were inadequate AML controls of customers and transactions. Some of the reported incidents were due to errors that had existed for several years and that have resulted in serious discrepancies in customer and transaction controls.

BankID incidents

Finanstilsynet again received many reports in 2019 about various problems with BankID. The problems especially arise when many people are using BankID at the same time, for example on the

dates when tax settlements and tax refunds are published. BankID is a complex service. Finanstilsynet notes that the incidents where all or part of the BankID service does not work are caused by many different factors. Of the incidents reported in 2019, the disruption seen on the date tax settlements were published, 20 June, was the most serious.

Security incidents

Finanstilsynet notes that the institutions have strengthened their defences, meaning that ever more attacks are prevented before they have consequences. Only six of the reported incidents in 2019 were security incidents. The security incidents involved attacks with cryptoviruses that encrypted files and made parts of the institution's IT systems unavailable, phishing attempts to extract information, unauthorised retrieval of corporate information from inside the institution and attacks aimed at preventing access to services (DDoS attacks).

Reported vulnerabilities

Finanstilsynet learns about vulnerabilities identified by the institutions through incident reports and its supervisory activities, without the vulnerabilities necessarily having been exploited. Reports received by Finanstilsynet underscore the importance of the institutions further developing tool support and procedures for quickly detecting, notifying and managing newly identified critical vulnerabilities and regularly reviewing and checking the status of security updates to identify missing updates. The measures apply to all platforms and to exposure to both internal networks and the internet. Strict control of administrator rights reduces the risk of unauthorised updates.

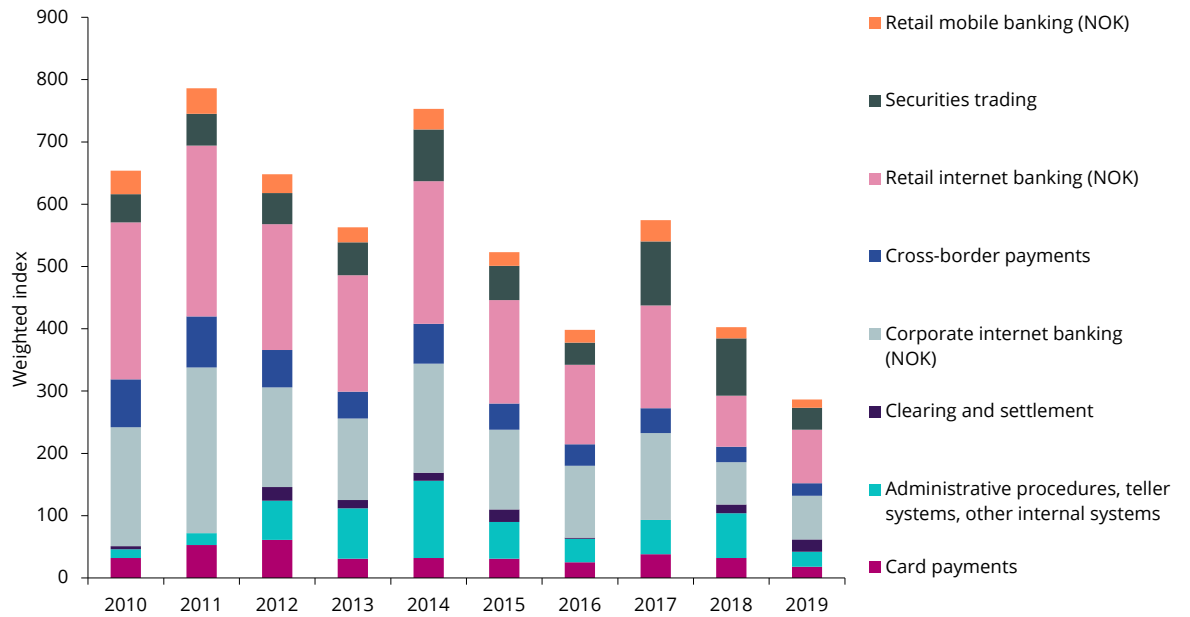
5.3. Analysis of incidents as a measure of availability

The reported incidents were of differing degrees of severity. For incidents that caused reduced availability, Finanstilsynet has considered the duration of the disruption, the number of institutions affected, the number of customers affected and whether there are alternative services that can meet customer needs (such as when the mobile banking service is unavailable, but the online bank is available). The incidents are weighted on the basis of the number of affected users, incident duration, time and access to replacement services. The findings are collated in a time series so that Finanstilsynet can monitor development over time.

Figure 5.3 shows that payment systems and other customer services were more available to customers in 2019 than in 2018 and previous years. The scale on the y-axis is an index based on the weighting of each incident. A lower index value indicates fewer business disruptions with consequences for users.

Figure 5.3 'Service not available' incidents weighted by impact

The following has been assessed: number of affected users, duration of the incident, any harm inflicted on customers as a consequence of the incident and alternative ways of accessing the service.



Source: Finanstilsynet

6. Notifications from the institutions

6.1. Notifications of outsourcing

Finanstilsynet received 135 notifications of outsourcing of ICT operations in 2019. Finanstilsynet also assessed outsourcing agreements for ICT operations when considering licence applications. As in 2018, there was a continued trend in 2019 towards the increased use of cloud services for both application and infrastructure services.

Over time, notifications of outsourcing have become more comprehensive and the complexity of outsourcing agreements has increased. However, Finanstilsynet has noted an improvement in the institutions' management of outsourcing agreements. This applies to the content of the institutions' risk analyses for outsourced operations, board consideration of outsourcing agreements and the institutions' risk assessments, as well as the quality of the agreements with the institutions' ICT service providers.

The institutions have a responsibility to ensure that ICT operations, including outsourced services, satisfy all of the requirements set out in the ICT Regulations, cf. section 12 of the Regulations. Other sector legislation may also contain detailed rules on outsourcing. The institutions must establish service provider agreements that comply with laws and regulations and ensure that the service provider and any subcontractors provide ICT services in line with these requirements. Finanstilsynet can gain insight into the institutions' outsourcing agreements when considering notifications of outsourcing, cf. section 4(c) of the Financial Institutions Act, and processing licence applications, and as part of its supervisory activities.

6.2. Notifications regarding payment service systems

In 2019, Finanstilsynet considered 21 notifications from institutions subject to supervision concerning new or changed payment services. Key points that are considered include whether risk assessments have been carried out, whether a description of security mechanisms exists, whether stress and end-to-end tests have been carried out and whether emergency preparedness and a recovery plan have been established. Some of the notifications were followed up. Cooperation between banks on payment solutions and new mobile payment solutions were recurrent themes.

The Act on Payment Systems requires Finanstilsynet to be notified of the establishment and operation of payment services without undue delay. The duty of notification applies to both existing and new licensed institutions and covers banks, e-money institutions, payment institutions and other providers in cases where the institution will provide payment services. The duty of notification is triggered upon the introduction of a new payment service system, a new version that significantly impacts other affected parties included in the payment service, and a new version with modified or new functionality of material importance for the payment service system.

6.3. Reauthorisation and licence to provide payment services

The public law part of the EU's revised Payment Services Directive (PSD 2) was introduced in Norway on 1 April 2019. The new statutory provisions make licences mandatory for two new payment services described as so-called 'initiation services': payment initiation services and account information services, respectively.

The Regulations on Amendments to the Financial Institutions Regulations, point IV, set out transitional provisions (requirement for reauthorisation) for e-money institutions, payment institutions with an ordinary licence, payment institutions with a limited licence and institutions that are able to document that they offered payment initiation services and/or account information services prior to the Regulations coming into force.

The new Regulations (section 3-2 of the Financial Institutions Regulations) stipulate a strict requirement that the institutions must have well-documented procedures in areas related to ICT and payment services. Institutions that as of 1 April 2019 had a licence as a payment institution and/or e-money institution had to document that they satisfied the new requirements by 1 September 2019. Finanstilsynet received 20 applications for reauthorisation. Finanstilsynet also received ten applications for a licence to provide payment services. The applications showed that many of the institutions had good procedures in place for ICT and payment services, but also that several institutions had an inadequate understanding of the regulations and the need to significantly improve their procedures. The findings showed the importance of the requirements in helping to mitigate the risk associated with payment service providers.

On 14 September 2019, rules in line with Commission Delegated Regulation (EU) 2018/389 also came into force. The rules include requiring account servicing payment service providers (banks) to give payment institutions providing payment initiation services and/or account information services access to the same account information the account holder has access to via the bank's customer interface. Banks are obliged to make at least one interface for accessing payment account information available to these institutions. In line with the Commission Regulation, banks that have chosen to develop dedicated interfaces for access to payment account information can, on certain conditions, apply for an exemption from the requirement to have a backup solution. Finanstilsynet received 111 applications from banks for exemptions from the requirement for a backup solution. At the end of April 2020, a number of banks still did not meet the conditions for exemption.

PSD 2 defines security requirements to protect customer data, verify user identity and reduce the risk of fraud, so-called strong customer authentication (SCA). These rules were introduced in Norway both through the Regulations on Systems for Payment Services and through the rules that implement Commission Delegated Regulation (EU) 2018/389 in Norway. The requirement for strong customer authentication (SCA) entered into force in the EEA on 14 September 2019.

Based on a number of enquiries to the European Banking Authority (EBA) and national supervisory authorities about which authentication methods were considered to be in compliance with the rules of

SCA, this was clarified in June 2019 in a statement issued by the EBA. In order to avoid negative consequences for users who pay by card when shopping online, national supervisory authorities were allowed to defer the deadline by which card issuers and processors and e-commerce companies were meant to establish SCA for the use of payment cards for online purchases. Almost all banks and payment institutions have applied to Finanstilsynet to defer the deadline. In October 2019, the EBA decided that all card issuers and processors and e-commerce companies must have completed, tested and implemented SCA by 31 December 2020. Finanstilsynet will monitor progress in the institutions.

6.4. Risk reporting for payment service providers

Section 2 of the new Regulations on Systems for Payment Services, which came into force on 1 April 2019, requires payment service providers³⁴ to report to Finanstilsynet, at least once a year, on the operational and security risks associated with the provider's payment services and on an assessment of whether the measures taken by the provider are adequate.

Finanstilsynet is developing a separate form for such reporting, which will be based on the form Finanstilsynet uses in connection with the annual vulnerability survey, see Appendix 1. A proposed form, together with an overview showing the relationship between the questions on the form and the control objectives in COBIT, has been published³⁵ on Finanstilsynet's website.

The deadline for submitting the first reports was set as 30 June 2020. Finanstilsynet has postponed this deadline because of challenges the institutions have to deal with due to the coronavirus crisis.

³⁴Banks, credit institutions, e-money institutions, payment institutions, account information service providers and branches of such institutions headquartered in another EEA state. Payment institutions with limited authorisation, ref. section 2-10(4) of the Financial Institutions Act are specifically exempted from the scope of the Regulation.

³⁵[PSD 2 – Annual reporting of risk assessments of the institutions' payment services](#)

Appendices

1 – Institutions’ response to the questionnaire on vulnerability

In December 2019, Finanstilsynet conducted its annual questionnaire survey on vulnerability. Finanstilsynet asked the institutions to rate their vulnerability to threats. A total of 16 institutions responded to the survey. The results appear in the tables below.

The institutions’ responses are indicated by colour codes. Green expresses low vulnerability, yellow medium vulnerability and red high vulnerability. No colour indicates that the institution did not reply.

The institutions were also asked to rate their vulnerabilities in the period ahead, i.e. as increasing, stable or decreasing. The trend is expressed in the far right column of the tables and represents the average of the institutions’ assessments. A horizontal arrow (where the interval is -0.2 to +0.2) indicates a stable trend. Arrows that point up indicate that vulnerability is considered to be increasing (the interval +0.2 to +1), and arrows that point down indicate that vulnerability is considered to be decreasing (the interval -0.2 to -1). For each question, an arithmetic mean of the institutions' responses is calculated.

Management and control

Vulnerability		The institutions' responses	Trend 2018	Trend 2019
1	We comply with the principle of three lines of defence.		N/A	→
2	We have a well-established risk analysis process. Employees are familiar with the process and make active and ongoing contributions.		N/A	→
3	Information forming the basis for risk assessments is collected systematically on an ongoing basis. The information may be analyses of deviations and incidents, information from external sources, results of penetration testing and observations from customers and employees		N/A	↗
4	We perform tests to test the security of our services. (E.g. penetration testing, testing according to the TIBER standard, vulnerability scanning).		N/A	→
5	Security testing is performed by persons who have not been involved in the development of the service being tested.		N/A	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

The institutions report an ever-increasing complexity of their system portfolios. This makes the work on risk analyses more extensive and challenging.

IT systems do not function satisfactorily as support for decisions, customer services or case processing

Vulnerability		The institutions' responses	Trend 2018	Trend 2019
1	The ability of systems to retrieve relevant information from external and internal sources and compile and synchronise the information into a picture of the institution's risk for the purpose of management and reporting to the authorities.		→	↗
2	The ability of systems to automatically provide an overall risk picture, so that if a cornerstone enterprise goes bankrupt, for example, the system automatically issues an alert about loans to the enterprise's employees and suppliers, so that we can consider writing these off as losses.		→	→
3	The ability of the systems to reflect customers' debt servicing capacity		→	↗
4	The quality of data in our systems and registers		↘	↗
5	Integration and synchronisation of systems		→	→
6	When new IT systems are to be developed, do we take into account the needs and systems of all relevant departments? We do this to avoid the challenges associated with "silo solutions", such as extensive software maintenance, complicated operations and challenges associated with data synchronisation.		→	→
7	The scope of and faults and deficiencies in systems		→	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

The institutions seem to assume that the data from the IT systems will be attended by greater uncertainty in the period ahead when used as a basis for decisions. For example, data quality is considered to be poorer than in 2018, and the institutions believe that this could represent an increasing problem in the future. It may appear that the IT systems to a lesser extent than in the past provide adequate and necessary business support, partly due to new requirements. This concerns the systems' ability to provide an overall picture of the institution's exposure to various industries and customers.

Operations

Vulnerability		The institutions' responses	Trend 2018	Trend 2019
1	Organisation, procedures, job description, reporting and controls		→	→
2	Agreements with service providers give us the right to scrutinise all aspects of the delivery.		→	→
3	The test systems are "production-like", i.e. test data, applications, software, control systems and hardware are the same for testing as for production.		→	→
4	We make changes in the infrastructure ("non-functional" changes) during periods with little traffic and can quickly reverse the change and roll back if necessary.		→	→
5	Complexity of IT systems		↗	↘
6	Intrusion detection and intrusion prevention, firewall, antivirus, control of web traffic, securing of e-mail and other measures to ensure stable operations		→	→
7	Logs and our ability to react to the contents of the logs		→	→
8	Our ability to identify "ticking bombs", i.e. components that gradually wear out, or assets that gradually reach levels requiring intervention, such as memory leakage, expired certificate dates, worn out electronic components, an energy supply that is running down (batteries, fuel for emergency generator etc.)		→	→
9	Our ability to detect irregularities (abnormal load, abnormal ports/protocols, irregular response times) in data traffic and take action before damage occurs		→	→
10	Our protection against data attacks (advanced persistence threat, Trojans, ransomware, DDoS)		→	→
11	The quality of our business continuity and disaster recovery systems; see section 11 of the ICT regulations		→	→
12	Procedures for cooperation with service providers		→	→
13	The pressure to deliver we are exposed to in the market means that the quality of solutions is not always good enough.		↗	→
14	Access to expertise, including the expertise to stipulate requirements for service providers and to monitor deliveries		→	↘
15	The scope of changes		↗	→
16	New regulatory requirements that make it necessary to change our systems		↗	↘
17	Our knowledge of where data transmission lines go and line redundancy		→	→
18	Access management, access control and dual control		→	→
19	Employee alertness to threats and attacks Training		→	↗

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

As in 2018, the pressure to deliver is considered to pose a risk, but the institutions expect this risk to level off. Among other things, the trend for the extent of changes (point 15) was stable in 2019. Although the institutions report an ever-increasing complexity of their IT systems, the risk associated with this complexity (point 5) seems to have declined in 2019, and the trend appears to have shifted from increasing to decreasing risk.

The risks associated with attacks appears to have increased from 2018 to 2019, see points 6 and 10. The risk related to system changes remains high, reflecting new regulatory requirements, but the institutions expect this risk to subside. This may be due to the fact that a number of regulatory changes have now been implemented, cf. PSD 2, MiFID II and GDPR.

The risk associated with employees' lack of security awareness has risen slightly, which may be due to the increasing sophistication of the attacks. Also, a more complex service provider situation, involving a large number and often new external employees, may be a contributing factor. There is still risk associated with access to expertise, but this risk is on the decline. This may reflect expectations that the pressure to deliver and regulatory requirements will be reduced in the period ahead.

Data protection

	Vulnerability	The institutions' responses	Trend 2018	Trend 2019
1	Our guidelines for classification of structured (databases) and unstructured (text documents, e-mails) data and protection of the data		→	→
2	Access controls – employees, consultants, suppliers, application accesses, software accesses		→	↗
3	Our logging systems and our ability to react to log contents		→	→
4	Network segmenting, perimeter protection, encryption		→	→
5	Protection of data on portable devices		→	→
6	On termination of data storage agreements, must the supplier document that data have been completely deleted?		→	→
7	Unstructured data (i.e. data that users themselves find it necessary to protect) such as e-mails, presentations, text documents, are reviewed regularly with a view to protection or alternatively deletion.		↘	↗

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

The risk associated with access controls shows a rising trend, which may be due to the fact that a number of external staff are involved in connection with outsourcing or the purchase of services. Unstructured data are reported to pose a greater risk in 2019.

ID theft

Vulnerability		The institutions' responses	Trend 2018	Trend 2019
1	An attacker takes over a user ID in the institution and uses it fraudulently.		→	→
2	Controls on the issue, use and deletion of login IDs and passwords to customers		→	→
3	Controls that prevent skimming and card-not-present fraud		→	→
4	We require strong customer authentication in connection with payments for online transactions.		N/A	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

The risk associated with 'Card not present' is reported to be higher in 2019 than in 2018, but the trend is unchanged. The risk is assessed to be about the same as in 2018.

Internal fraud

Vulnerability		The institutions' responses	Trend 2018	Trend 2019
1	Our policy on dual control		→	→
2	Logging and alerts		→	→
3	Analysis of "suspicious" transactions such as backdating, movements in internal accounts, transfers from customer to employee and back		→	→
4	Monitoring of employees' own-account trading		→	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

The risks associated with inadequate logging and notification appears to be greater in 2019 than in 2018. The general picture is about the same in 2019 as in 2018.

Money laundering

Vulnerability		The institutions' responses	Trend 2018	Trend 2019
1	Market surveillance		↘	→
2	The ability of the IT systems to compile information about customers, customer relations and customer behaviour (KYC – Know Your Customer)		→	→
3	Electronic surveillance of transactions and transaction patterns – precision in flagging suspicious transactions		→	↗

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: Not assessed.

The institutions report heightened risk associated with the IT systems' ability to collect information about customers, customer relations and customer behaviour. The risk associated with inaccurate disclosure of suspicious transactions is expected to increase.

2 – Basis for the risk matrix

Finanstilsynet's assessment of risk in the different areas, classified according to probability and the seriousness of the consequences, is discussed in this appendix. Along with the observations and assessments in chapters 3 to 6, this forms the basis for the risk matrix in chapter 1.

The following definitions are used:

Vulnerability – weakness in technical infrastructure, functions and processes that may result in undesirable incidents.

Threat – factor with the potential to cause an undesirable incident.

Risk – the risk of an undesirable incident occurring as a consequence of inadequate internal processes or systems or failure thereof, human error or external incidents.

Consequence – possible result of an undesirable incident.

Risk assessment – involves identification, analysis and evaluation of a risk. A risk assessment lays the foundation for an institution's risk-reducing measures and the priority given to them.

Governance model and internal control

Finanstilsynet assesses the overall risk associated with vulnerabilities in the **institution's governance model** and **internal control** as **medium**. The probability of the three lines of defence not revealing serious weaknesses in the institution's internal control through their activities is assessed as *low* to *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of failure to comply with laws and regulations not being detected as a result of inadequate supervision by an institution's operational management is assessed as *low* and the consequences as *serious*.
- The probability of important requirements in governing documents not being implemented and operationalised, including controls, is assessed as *medium* and the consequences as *moderate*.
- The probability of the compliance function not detecting serious weaknesses in operational units' control is assessed as *medium* and the consequences as *moderate*.
- The probability of the institution's board and executive management not possessing information that confirms or disproves compliance with internal and external requirements is assessed as *medium* and the consequences as *moderate*.
- The probability of the institution's board and executive management *not* having sufficient expertise and insight to help to ensure that IT investments support the institution's strategy and needs, and the necessary understanding of the risk picture in the ICT area to ensure stable and secure ICT operations is assessed as *medium* and the consequences as *moderate*.

- The probability of unclear roles in the institution's first and second lines of defence leading to serious weaknesses in the surveillance and control of the institution's governance is assessed as *low* and the consequences as *limited*.
- The probability of serious vulnerabilities not being detected as a result of deficient risk management between the operational unit and the risk management function in the second line of defence is assessed as *low to medium* and the consequences as *moderate*.
- The probability of serious weaknesses in internal control not being detected by the internal audit as a result of inadequate competencies and understanding of risk on the part of the institution's internal audit is assessed as *low* and the consequences as *moderate*.
- The probability of serious organisational challenges as a result of weak change management is assessed as *medium* and the consequences as *moderate*.

Skills and skills management

At present, Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with **skills and skills management** as **medium**. The probability of adverse incidents occurring or not being adequately managed as a consequence of a lack of skills in Norway is assessed as *medium* and the consequences as *limited to moderate*. This is based on the following assessments:

- The probability of the board and the executive management not maintaining a sufficient overview of employee skills and current and future needs as a result of inadequate skills management is assessed as *low to medium* and the consequences as *limited*.
- The probability of inadequate skills management in institutions resulting in the loss of and/or an inadequate supply of the skills necessary for sound operations is assessed as *medium* and the consequences as *moderate*.
- The probability of business disruptions and unavailable services as a result of insufficient skills is assessed as *low* and the consequences as *moderate*.
- The probability of breaches of information security as a result of inadequate access to security skills is assessed as *medium* and the consequences as *moderate*.
- The probability of institutions' inadequate competence in services developed and operated by service providers resulting in breaches of laws and regulations is assessed as *low to medium* and the consequences as *limited*.
- The probability of increased dependence on foreign service providers as a result of lack of resources and rising needs in Norway is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate understanding of the risks attending the use of cloud services resulting in adverse incidents is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate competence in new technology, such as RPA, AI and blockchain, resulting in failure to identify significant operational risks when using such technology is assessed as *medium* and the consequences as *moderate*.

Vendor management

Finanstilsynet assesses the overall risk associated with vulnerabilities in **vendor management** as **medium**. The probability of adverse incidents is assessed as *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of major irregularities in the service provider's internal control not being discovered by the institution is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of security breaches occurring as a result of inadequate supervision and commitment to the security requirements by the service provider is assessed as *medium* and the consequences as *moderate*.
- The probability of an unacceptably long restoration time in the case of serious business disruptions due to unclear roles and responsibilities in the cooperation with the service provider and between service providers is assessed as *medium* and the consequences as *serious*.
- The probability of service unavailability as a result of inadequate monitoring of service quality is assessed as *low* and the consequences as *moderate*.
- The probability of undesirable dependence on service providers as a result of inadequate regulations (e.g. exit rules) in the agreement is assessed as *medium* and the consequences as *moderate*.
- The probability of undesirable dependence on service providers as a result of inadequate expertise on the part of the institution concerning the outsourced services is assessed as *medium* and the consequences as *limited*.
- The probability of inadequate (regular) risk assessments failing to detect weak sustainability on the part of service providers as a consequence of a difficult liquidity situation (bankruptcy risk), a challenging resource situation or other factors that may threaten the service provider's ability to deliver, is assessed as *low* and the consequences as *moderate*.
- The probability of serious weaknesses in a service provider's internal control not being detected through the work of a service provider's chosen auditor on an independent audit report is assessed as *medium* and the consequences as *moderate*.

Digital crime

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of **digital crime** as **high**. The probability of adverse incidents is assessed as *medium to high* and the consequences as *serious*. This is based on the following assessments:

- The probability of serious weaknesses in an institution's defences not being uncovered as a result of non-existent or deficient security testing is assessed as *high* and the consequences as *serious*.
- The probability of an institution having serious faults in its security configuration of critical systems as a result of failure to classify its systems is assessed as *medium* and the consequences as *serious*.

- The probability of an institution having serious faults in its security configuration of cloud services is assessed as *medium* and the consequences as *serious*.
- The probability of criminals succeeding in exploiting vulnerabilities in hardware (CPU) or firmware (UEFI) to attack an institution is assessed as *low* and the consequences as *moderate*.
- The probability of institutions being hit by a ransom virus with loss of critical business data as a result of malware (encryption) is assessed as *moderate* and the consequences as *critical*.
- The probability of an institution not detecting criminals who have established a digital foothold inside the network before damage is averted is assessed as *medium* and the consequences as *critical*.
- The probability of serious security flaws not being patched in time as a consequence of inadequate security updates (patch management) is assessed as *medium* and the consequences as *serious*.
- The probability of new applications or changes in existing applications being released into production with serious security flaws is assessed as *medium* and the consequences as *serious*.
- The probability of third-party applications integrated by a third party between the institution's systems and its customers resulting in adverse security incidents is assessed as *medium* and the consequences as *moderate*.
- The probability of employees or service provider personnel representing a significant vulnerability as a result of negligence and inadequate competence in secure use of the institution's systems is assessed as *high* and the consequences as *serious*.
- The probability of criminals or foreign intelligence services attempting to recruit employees or service provider personnel to gain access to information about vulnerabilities in the digital infrastructure or other information about the institution is assessed as *medium* and the consequences as *serious*.
- The probability of employees being used involuntarily, through social engineering, as a medium for a cyber attack is assessed as *high* and the consequences as *serious*.
- The probability of criminals succeeding in entering the institution's premises as a result of inadequate visitor control procedures is assessed as *low* and the consequences as *limited*.
- The probability of criminals succeeding in forcibly entering the institution's premises is assessed as *high* and the consequences as *serious*.
- The probability of employees being used involuntarily, through threats, as an instrument for a cyber attack is assessed as *low* and the consequences as *moderate*.
- The probability of service provider personnel being used involuntarily, through threats, as an instrument for a cyber attack is assessed as *low* and the consequences as *moderate*.
- The probability of disloyal employees in the institution or personnel at service providers' development units planting malicious code in critical business applications is assessed as *low* and the consequences as *moderate*.
- The probability of employees or service provider personnel helping criminals to channel criminal transactions through an institution's systems is assessed as *medium* and the consequences as *serious*.
- The probability of personal data, including information about an institution's employees and service provider personnel who have roles that may be of interest to and exploited by

criminals, falling into the hands of criminals is assessed as *medium to high* and the consequences as *serious*.

Information leaks

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of **information leaks** as **high**. The probability of adverse incidents is assessed as *high* and the consequences as *moderate*. This is based on the following assessments:

- The probability of classified documentation being sent from the institution in an unauthorised manner as a result of lack of classification and control is assessed as *high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control outgoing emails is assessed as *very high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control the use of USB storage media is assessed as *very high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control service provider personnel is assessed as *moderate* and the consequences as *serious*.
- The probability of sensitive information that may be used to harm the institution intentionally or unintentionally being sent to or shared with external sources in an unauthorised manner and this *not* being detected is assessed as *high* and the consequences as *moderate*.
- The probability of employees or service provider personnel operating as insiders and handing over or sending sensitive information, such as lists of email addresses and login information, to criminals, is assessed as *medium* and the consequences as *moderate*.

ICT operations

Finanstilsynet assesses the overall risk associated with vulnerabilities in **ICT operations** as **high**. The probability of adverse incidents is assessed as *medium to high* and the consequences as *moderate to high*. This is based on the following assessments:

- The probability of unstable and/or unavailable services as a result of increased integration among different service providers is assessed as *medium to high* and the consequences as *serious*.
- The probability of operational problems that impact shared operational infrastructure is assessed as *medium* and the consequences as *serious*.
- The probability of operational problems as a result of a lack of comprehensive understanding and overview of the institution's architecture and digital business processes is assessed as *medium to high* and the consequences as *moderate*.
- The probability of impaired data quality as a consequence of complex integration among service providers is assessed as *medium* and the consequences as *moderate*.
- The probability of operational problems as a result of inadequate configuration management (hardware applications, databases, operating systems etc.), is assessed as *medium* and the consequences as *moderate*.

- The probability of the agreed time for correcting critical errors not being adhered to as a result of the complexity of the system portfolio, entailing integration between new and old systems is assessed as *medium* and the consequences as *serious*.
- The probability of service unavailability as a result of deficient capacity management is assessed as *medium to high* and the consequences as *serious*.
- The probability of components in redundant systems failing as a result of deficient surveillance and testing is assessed as *low* and the consequences as *serious*.
- The probability of operational problems (networks and services) as a result of invalid digital certificates or invalid licences is assessed as *low* and the consequences as *moderate*.
- The probability of operational problems in the process of phasing out outdated and critical systems is assessed as *high* and the consequences as *moderate to serious*.
- The probability of operational problems as a result of lack of access to expertise in operating support for mainframes is assessed as *medium* and the consequences as *moderate*.

Business continuity management and disaster management

Finanstilsynet assesses the overall risk associated with vulnerabilities in **business continuity management and disaster management** as **medium to high**. The probability of adverse incidents resulting in the activation of disaster recovery systems for critical business processes is assessed as *very low to low* and the consequences as *critical* if the system does not function as intended. This is based on the following assessments:

- The probability of the institution's disaster recovery system not being established in accordance with its needs as a consequence of the absence of or inadequate business impact analyses and requirements is assessed as *medium* and the consequences as *critical* if the system has to be activated.
- The probability of institutions not being adequately prepared to respond to a serious situation as a result of deficient training and exercises is assessed as *high* and the consequences as *serious*.
- The probability of the emergency response management of an institution and its service provider being inadequately coordinated in the event of a serious incident is assessed as *medium* and the consequences as *critical*.
- The probability of institutions failing to handle a serious incident effectively as a consequence of unclear roles and responsibilities internally and between the institution and the service provider is assessed as *low to medium* and the consequences as *serious*.
- The probability of the disaster recovery system not functioning as intended owing to deficient technical tests and deficient evaluation of these tests is assessed as *low to medium* and the consequences as *critical*.
- The probability of inadequate security updates of the disaster recovery system is assessed as *low to medium* and the consequences as *serious*.
- The probability of an institution affected by a serious digital attack not being capable of handling the situation effectively as a consequence of the lack of a business continuity plan to

handle cyber attacks and inadequate training and exercises is assessed as *medium to high* and the consequences as *critical*.

Geopolitical factors

Finanstilsynet assesses the risk associated with vulnerabilities in relation to foreign operators that deliver critical ICT services to Norwegian institutions as **medium to high**. The probability of adverse incidents when foreign service providers are cut off from delivering their services is assessed as *low* and the consequences as *serious*. This is based on the following assessments:

- The probability of an institution's disaster recovery personnel *not* being able to maintain secure and stable operations in situations where foreign service providers are unavailable, is assessed as *low* and the consequences as *serious*.
- The probability of an institution's disaster recovery personnel *not* being able to maintain secure and stable operations in the event of serious ICT incidents where foreign service providers are unavailable, is assessed as *medium* and the consequences as *serious*.
- The probability of a breakdown in communication with foreign operators, whereby the foreign provider will be cut off from performing critical ICT services, is assessed as *low* and the consequences as *serious*.

Change management

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with **change management** as **medium**. The probability of adverse incidents is assessed as *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of service unavailability as a result of non-functional changes (changes in the configuration of operating components) is assessed as *medium* and the consequences as *moderate*.
- The probability of functional changes (software) introducing vulnerabilities into institutions' defences is assessed as *low* and the consequences as *moderate*.
- The probability of failure to establish adequate controls for identifying functional and non-functional changes that have been released into production without monitoring the change process, so-called unauthorised changes, is assessed as *high* and the consequences as *serious*.
- The probability of the high rate of change leading to new services without the necessary quality being released into production is assessed as *high* and the consequences as *moderate*.

Access management

Finanstilsynet assesses the overall risk associated with vulnerabilities in **access management** as **medium to high**. The probability of adverse incidents is assessed as *medium to high* and the consequences as *moderate*. This is based on the following assessments:

- The probability of employees with extended access rights performing illegal actions is assessed as *low* and the consequences as *moderate*.

- The probability of service provider personnel with extended access rights performing illegal actions is assessed as *low* and the consequences as *serious*.
- The probability of employees or service provider personnel having administrative rights without the executive management being aware of it is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of inadequate access management and control of employees' accesses is assessed as *high* and the consequences as *moderate*.
- The probability of confidential and/or classified information going astray as a result of a service provider's security breaches is assessed as *medium to high* and the consequences as *moderate*.
- The probability of service provider personnel, or a service provider's vendor's personnel, breaking rules while performing operating tasks is assessed as *medium* and the consequences as *serious*.

Data quality

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with **data quality** as **medium**. The probability of adverse incidents is assessed as *medium* and the consequences as *limited*. This is based on the following assessments:

- The probability of decisions being based on the wrong premises as a result of poor data quality or lack of data is assessed as *medium to high* and the consequences as *moderate*.
- The probability of weaknesses in anti-money laundering controls as a result of poor data quality or lack of data is assessed as *medium* and the consequences as *limited to moderate*.
- The probability of failure to identify risks as a result of poor data quality or lack of data is assessed as *medium* and the consequences as *limited*.
- The probability of the monitoring of operations failing to identify irregularities as a result of poor data quality or lack of data is assessed as *medium* and the consequences as *limited to moderate*.

3 – Finanstilsynet’s monitoring activities

Key areas for Finanstilsynet’s ICT supervision

Supervisory activities are risk-based, and Finanstilsynet gives priority to institutions that have the greatest influence on financial stability and well-functioning markets. ICT risk is assessed, and the institutions’ own annual assessments of ICT risk are reviewed. Emphasis is placed on monitoring the organisation of ICT/cyber security work, the security of institutions’ ICT systems and the organisation of surveillance activities. Inspections include institutions’ control of access to systems, particularly those containing sensitive information, and the institutions’ testing of penetration of their systems.

Other prioritised topics for supervision will be overall governance of ICT activities, the institutions’ emergency response work in connection with business continuity and disaster recovery systems and the testing thereof, outsourcing, the institutions’ payment services and ICT systems for detecting money laundering and the financing of terrorism. Finanstilsynet places emphasis on the institutions having procedures in place for ensuring complete data extracts to anti-money-laundering systems.

The use of new technology and major changes in the ICT area are also topical subjects.

Supervisory activities extend to the institutions’ evaluations of the risk associated with outsourcing of ICT and the quality and monitoring of agreements between institutions and service providers.

Work with payment systems

The EU’s revised Payment Services Directive (PSD 2) has been transposed into Norwegian legislation and will form the basis for the supervision of institutions’ payment services. Institutions will be monitored with respect to their compliance with the new regulations relating to payment service systems³⁶, risk related to payment services and compliance with the duty to report new or changes to existing payment services. Account servicing payment service providers’ interfaces (APIs) for account access will also be followed up. When processing concessions, care will be taken to ensure that the institutions have well-documented procedures in areas relating to ICT and payment services.

The cooperation with Norges Bank on the payment system and financial infrastructure will continue.

Follow-up of incidents

Following up ICT incidents is a prioritised part of supervisory activities. Finanstilsynet will continue to closely monitor developments in 2020. When incidents occur, emphasis will be placed on whether the institution identifies causes and takes steps to prevent recurrence. Incidents involving serious irregularities will be monitored throughout the life of the incident. Special measures will be considered.

³⁶ [Lovdata: Regulations on payment services systems \(Norwegian text\)](#)

Finanstilsynet will continue to make an annual review of incident reporting with the largest institutions.

Outsourcing of ICT activities

Finanstilsynet will continue to monitor institutions' outsourcing of ICT activities and ensure that the institutions, when entering into a new or changing an existing outsourcing agreement, reports this to Finanstilsynet, as required by Section 4c of the Financial Supervision Act.

Finanstilsynet monitors that the institutions make a prudent assessment of the outsourcing relationship, that the agreements are in line with regulations and that the outsourcing is handled in a proper manner by the institution, cf. Section 2 of the ICT Regulations.

Contingency preparedness

The work of the Financial Infrastructure Crisis Preparedness Committee (BFI) will continue. BFI reviews incident scenarios and determines whether the responsibilities associated with crisis situations are sufficiently clear. Emergency response exercises are planned for 2020 as well, and measures linked to findings from previous exercises will be followed up.

Special incidents, such as the corona crisis and the institutions' organisation of their ICT activities, will be closely monitored, particularly at key operators in the financial infrastructure.

Finanstilsynet participates in relevant contingency preparedness work initiated by other sectors and cooperation within the national regulatory framework for managing ICT security incidents, partly through the National Cyber Security Centre (NCSC), established by the Norwegian National Security Authority (NSM).

Finanstilsynet will align its contingency work and handling of ICT security incidents with NSM's framework for handling ICT security incidents³⁷. In 2019, the Ministry of Finance appointed Finanstilsynet as sectoral response group (SRM) in the financial market area. Finanstilsynet will exercise its role in collaboration with Nordic Financial CERT according to agreed information exchange rules. The NSM framework forms the basis for the interaction between Finanstilsynet and Nordic Financial CERT.

Monitoring of the cybercrime threat picture

Finanstilsynet will remain constantly informed of institutions' use of ICT and developments in payment services, including special developments relating to:

- the cybercrime threat picture
- contingency preparedness work targeting digital vulnerability and security
- institutions' organisation and follow-up of security work

³⁷ [NSM: Rammeverk for håndtering av IKT-hendelser \(in Norwegian only\)](#)

- changes in payment services due to the use of new technology (FinTech)
- cross-border activities

In cooperation with Norges Bank, Finanstilsynet will assess and possibly implement a nationally adapted cybersecurity testing framework (the TIBER framework).

Consumer protection

Finanstilsynet stresses the importance of institutions safeguarding their customers' security. It will also monitor that institutions do not share customer data without consent, and that data do not fall into the hands of unauthorised third parties.

Finanstilsynet will check that institutions establish digital solutions in compliance with the regulations, and that the solutions launched have built-in security and functionality in line with consumer expectations.

Payment service systems will be checked to ensure that they do not require users to accept additional functionality in order to be able to use the service, and that users are given the opportunity to protect themselves against adverse incidents, such as the ability to block their cards against online use.

Based on new requirements for reporting fraud relating to the use of payment services, cf. Section 2 of the regulations on payment services systems, Finanstilsynet will examine the total extent of fraud and, when needed, also individual operators.

If incidents occur, Finanstilsynet will check that the institutions provide customers with information on how they become affected and how the institution or customers themselves can mitigate the situation.

Finanstilsynet will continue to check that banks discharge their responsibilities with respect to compliance with the provisions of the Financial Institutions Act³⁸ regarding the provision of cash. Special attention will be given to new cash in-store solutions. Finanstilsynet will also check that banks have established solutions in line with the provisions of the Financial Institutions Regulations³⁹ regarding solutions to meet increased demand for cash in a crisis situation.

³⁸ [Act on financial institutions and financial groups \(Financial Institutions Act\)](#)

³⁹ [Regulations on financial institutions and financial groups \(Financial Institutions Regulations\)](#)

4 – Internal control functions

High quality in an institution's three lines of defence (operational management, risk management and compliance) and internal audit is crucial for effective governance. Weaknesses in the lines of defence increase the risk of serious vulnerabilities not being detected. To ensure that the three lines of defence function as intended, the functions must be independent of the areas and units they control. The defence lines must report directly to the executive management and/or the board. In all three defence lines, appropriate internal control procedures, mechanisms and processes must be designed, developed, maintained and evaluated.

First line of defence (operational management)

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

Second line of defence (risk management and compliance)

The second line of defence consists of risk management and compliance functions that oversee and follow up the operational management's governance.

The responsibility of the risk management function is to facilitate the implementation of the institution's risk management framework. The risk management function is also responsible for assisting the first line in implementing risk management and ensuring that processes and controls established in the first line are effective and correctly designed. The function is also responsible for identifying, overseeing, analysing and reporting risks indicated by first-line risk reporting and using these to provide a comprehensive picture of the institution's risk situation.

The responsibility of the compliance function is to oversee compliance with legal and regulatory requirements and the institution's internal requirements. It is also responsible for advising the executive management and other stakeholders on compliance with these requirements, for establishing guidelines and processes for managing compliance risk and for ensuring compliance.

The second line of defence may also consist of other non-operational functions, for example within data security.

Third line of defence (internal audit)

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

It is not usual for small institutions to have their own dedicated resources in the three lines of defence. The second-line role of compliance does not normally have the necessary ICT expertise to oversee the institution's compliance with the ICT regulations, and the third line of defence in the form of an internal audit is usually outsourced.

Institutions that are not required to have their own internal audit, or do not possess ICT expertise in their risk management and compliance function, should consider using external resources to assess whether the institution's framework, including policies and guidelines, is in line with good practices and vendor management requirements. Other elements that should be considered are whether the compliance function's monitoring is consistent with the board of directors' and executive management's need for confirmation that the requirements stipulated in laws and regulations are complied with, and whether independent reviews of controls carried out within the institution and at service providers are of the expected quality.

Knowledge of the institution's risk picture and threat situation are key to identifying areas to be prioritised for internal audit. The rapid changes taking place through innovation, the use of new technology, new regulatory requirements and changes in the threat picture also place demands on the internal audit unit's ability to adjust and build competencies. In recent years, technological development has been linked to a far greater extent than previously to institutions' business processes, which means that the auditors must also have a certain insight into the business in addition to IT expertise.

It is important that an institution's internal audit has adequate expertise and understanding of risk, and that the board fulfils its responsibility for ensuring that the internal audit has the necessary expertise and resources to perform its duties in accordance with the risk picture and changes therein.

Finanstilsynet will assess the ICT governance of institutions through its supervisory work, and in so doing seek to detect vulnerabilities that may constitute a risk. Finanstilsynet may also point out areas where improvements might reduce an institution's risk. An open dialogue and good cooperation are important to enable Finanstilsynet to form a correct picture of institutions' risk and control situation. Finanstilsynet also refers to the EBA's 'Guidelines on Internal Governance'⁴⁰.

⁴⁰ [Guidelines on internal governance under Directive 2013/36/EU EBA](#)

5 - International frameworks relating to ICT security

This appendix describes:

- Guidelines on outsourcing arrangements from the European Banking Authority (EBA)
- Guidelines on ICT and security risk management from the EBA
- Information security frameworks (CSA, CIS, NIST, ISO 27001, OWASP, COBIT)
- Security testing framework (TIBER)

EBA guidelines on outsourcing arrangements

The European Banking Authority (EBA) published 'Guidelines on outsourcing arrangements' on 25 February 2019. The guidelines entered into force on 30 September 2019.

The new guidelines replace the 'Guidelines on outsourcing' established in 2006 by the EBA's predecessor CEBS and the EBA's 'Recommendations on outsourcing to cloud service providers' from 2017. The guidelines target banks, mortgage companies, investment firms, payment institutions and electronic money institutions and include detailed requirements to ensure that institutions have adequate management and control of outsourcing arrangements. The guidelines also include criteria to determine whether an agreement with a third party should be considered as outsourcing.

Finanstilsynet has confirmed that the guidelines are complied with in Norway. However, Finanstilsynet has noted that institutions' duty to notify outsourcing arrangements is more stringent under Norwegian rules than under the EBA guidelines. The EBA guidelines do not set explicit notification requirements, but state that the supervisory authorities shall monitor outsourcing arrangements. Pursuant to Section 4 of the Financial Supervision Act, institutions shall notify Finanstilsynet when entering into outsourcing agreements. The notification requirement for supervised institutions pursuant to Section 4c applies regardless of the nature, scope or duration of the agreement and includes outsourcing within a group. The notification shall be given at least 60 days prior to the entry into force of the agreement, changes to the agreement or change of contractor. However, some exemptions from the notification requirements have been made in separate regulations. For example, investment firms are exempted from the notification requirement.

The right to enter into outsourcing arrangements is more comprehensive in the EBA guidelines than under Norwegian law. According to the guidelines, so-called 'critical or important functions' may be outsourced. Banking and payment services can also be outsourced, but only to institutions with a licence or permission to engage in such business. Pursuant to Section 13-4 of the Financial Institutions Act, institutions may not outsource core tasks, nor outsource tasks on a scale or in a manner that cannot be deemed prudent or makes the supervision of the outsourced business or of the institution's overall business more difficult. There is no corresponding restriction on the outsourcing of core tasks in investment firms, but investment services can only be outsourced to institutions that are licensed to provide the relevant service.

Guidelines on ICT and security risk management from the EBA

The EBA has prepared guidelines on ICT security and risks and published ‘Guidelines on ICT and security risk management’ on 28 November 2019. The guidelines are based on the requirements of the revised Payment Services Directive’s ‘Guidelines on security measures for operational and security risks of payment services’, effective as of 30 June 2020.

The guidelines target banks, payment institutions and electronic money institutions and include detailed requirements regarding how institutions may protect themselves against the ICT security risk to which they are exposed. At the overarching level, the Norwegian ICT regulations have regulated the same areas as those covered by the guidelines since 2002. One of the main objectives of the guidelines is to give the institutions a better understanding of the supervisory authorities’ expectations as to how ICT security risks should be managed. Finanstilsynet will update its supervisory practices in line with the new guidelines.

Finanstilsynet has confirmed that the guidelines will be complied with in Norway.

Information security frameworks

A number of frameworks and guidelines have been prepared that may be of good use to institutions without expertise and detailed knowledge of what is in line with good practices, such as the Centre for Internet Security (CIS), the Cloud Security Alliance’s (CSA) framework for cloud services security, the NIST cyber security framework, the ISO standards ISO27001/27002 for information security, OWASP for security in web applications, and ISACA’s COBIT framework.

Security testing framework (TIBER)

The purpose of threat-based security tests is to improve and assure the quality of institutions’ cyber resilience. Such tests use military terms and methods, such as ‘red teaming’. The implementation of such security testing is based on methods that are optimised to identify weaknesses as effectively as possible while mitigating the risks to which the institution being tested is exposed. An important aspect of the methodology is that the testing experience is also communicated to the institution for follow-up. The European Central Bank (ECB) has drawn up the TIBER framework – Threat Intelligence-based Ethical Red Teaming and recommends involving the authorities in the testing in order to ensure high-quality tests. Furthermore, it is desirable that the national supervisory authorities in the EU/EEA area oversee that financial institutions of critical importance to society make sure that they have effective cyber resilience capabilities.

The countries that have implemented such testing frameworks have established a national ‘TIBER unit’ that, among other things, is involved in designing testing regulations, monitoring how the tests are performed and summarising the TIBER test results in the individual countries. The purpose is to build strong experience bases that can be used for subsequent testing. Security testing regulations may cover large parts of an institution’s ICT security area. Experience from tests that have been conducted have shown that they uncover more serious and a far larger number of weaknesses than traditional quality management and auditing procedures.

Experience from other Nordic countries shows that access to service providers who are skilled and experienced in methodical threat-based 'red teaming' is a prerequisite for succeeding with TIBER tests. Lack of such expertise has proven to cause slower execution of tests, have a negative effect on quality and raise costs.

Initial implementation of a TIBER test must be expected to cause increased costs for institutions involved in the test. However, costs are expected to be significantly reduced in connection with subsequent tests. Experience from tests conducted in other countries suggests that the tests are nevertheless profitable for the institutions and may contribute to improving the cyber resilience of institutions maintaining critical functions in society.

Finanstilsynet expects institutions, independent of their participation in security testing under a testing framework such as TIBER, to systematically use similar threat-based 'red teaming' methods to secure their IT systems against cyber crime.

FINANSTILSYNET

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

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

