FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Financial institutions' use of information
and communications technology (ICT)

RISK AND VULNERABILITY ANALYSIS
2018

Risk and Vulnerability Analysis 2018

Financial institutions' use of information and communications technology (ICT)

Finanstilsynet, 8 May 2019
English translation as of June 2019

Contents

1 Introduction

The Financial Supervisory Authority of Norway (Finanstilsynet) performs an annual risk and vulnerability (RAV) analysis of the financial sector's use of ICT.

The purpose of the report is to describe risks and vulnerability relating to financial stability, individual institutions and the institutions' customers. By monitoring reported incidents, findings from inspections and other contact with the financial sector, Finanstilsynet obtains good insight into financial institutions' use of ICT, payment services and relevant areas of risk.

Chapter 2 summarises the report.

Chapter 3 presents Finanstilsynet's findings, observations and lessons learned in its supervisory activities in 2018, including incident reports received and notifications of new payment services and changes in existing services. The chapter also covers ICT security, cyber threats and changes in the threat picture, as well as ways in which institutions should protect themselves against cyber threats. Technology trends considered to be of potential significance for financial institutions' use of ICT are described. The monitoring of outsourcing contracts is also described. Relevant regulatory frameworks and trends deemed to be of potential significance in the long term for financial institutions' use of ICT, and which may result in changes in the risk and vulnerability situation of both institutions and their customers, are also presented.

Chapter 4 cites financial institutions' own assessments of the most prominent threats, based on information obtained from questionnaires and interviews. Furthermore, a number of key service providers have been interviewed, and threat and risk assessments issued by national security services and authorities with particular focus on the financial sector are cited.

Chapter 5 presents Finanstilsynet's overall assessment of the risk picture in 2018 based on findings, observations and trends. The assessment describes the most important threats to and vulnerabilities of financial institutions' ICT systems and the financial infrastructure that could have a significant impact on financial stability and smoothly functioning markets. Vulnerabilities and threats targeting institutions' customers are also described.

Chapter 6 describes the areas on which Finanstilsynet will focus particular attention in the future.

A glossary explaining key terms and acronyms used in the report is attached.

2 Summary

2.1 General assessment

The Norwegian financial infrastructure is robust. There were no ICT incidents that had consequences for financial stability in 2018. Financial institutions' customers experienced approximately the same number of serious incidents as in 2017, but overall availability of services was better than in 2017.

In 2018, Finanstilsynet again identified vulnerabilities that could lead to serious incidents. Consequently, Finanstilsynet is still of the opinion that institutions should strengthen their efforts to improve ICT security and take steps to reduce the risk of serious incidents occurring.

The technical infrastructure is increasingly complex, due to the larger number of operators, new technology and use of technology in new areas. This increases the risk of incidents. The high pace of change and complex value chains, involving a steadily growing number of operators, pose a challenge to institutions' efforts to maintain good governance and ensure adequate security.

2.2 Finanstilsynet's findings and observations

2.2.1 Areas of supervision

Payment services

Finanstilsynet observed few serious incidents, in terms of either scope or duration, in payment services in 2018.

The payment service area continued to undergo major changes in 2018, including the merger of Vipps AS, BankAxept AS and BankID AS. Several banks established payment service agreements with global financial institutions. The banks also prepared for the implementation of new rules under the revised Payment Services Directive (PSD 2), which entered into force in Norway on 1 April 2019.

Payment card fraud continued to decline in 2018. The number of fraudulently used cards fell by around 46 per cent compared with 2017, while losses measured in NOK declined by 36 per cent. Since 2016, losses have been reduced by 55 per cent, from NOK 207 million to NOK 97 million. Actions taken, including monitoring by banks to prevent fraudulent use of cards and payment card issuers' introduction of more stringent security requirements, appear to have had a significant effect. Losses due to online banking fraud are low, although they increased slightly in 2018, to NOK 20 million.

PSD 2 imposes expanded requirements on institutions regarding governance of risk and vulnerability in payment systems. Supervisory activities in 2018 identified inadequate functionality in payment services and a need for better information on service functionalities.

Banks

Through its supervisory activities, Finanstilsynet has found deficiencies in financial institutions' ICT governance related, for instance, to the way management and control functions are organised, availability of expertise and resources and subcontractors' access management. Deficiencies were also detected in business continuity and disaster recovery systems.

Service providers are often authorised to register users in a bank's systems, potentially enabling them to access the bank's data. In Finanstilsynet's opinion, financial institutions must improve their procedures for monitoring service providers' management of access rights.

Finanstilsynet has seen a number of examples where customers and payment transactions have not been checked because data were not included in extracts from source systems to the anti-money laundering system.

Securities

Through its supervisory activities, Finanstilsynet has detected weaknesses in institutions' disaster recovery systems, where systems designed for use in a crisis have not had sufficient capacity to take over relevant workloads.

Financial institutions still need to improve their documentation of guidelines, procedures and plans for performing security tests.

Insurance

Incidents reported show weaknesses in insurance undertakings' own testing regimes, which have resulted in confidentiality breaches in connection with system commissioning.

Through its supervisory activities, Finanstilsynet has discovered that undertakings do not adequately monitor the access rights of their own personnel nor, in some cases, those of service providers.

Accounting and auditing

Finanstilsynet's inspections have revealed that companies have outsourced ICT activities without entering into written agreements that adequately ensure that the companies have insight into and governance of the outsourced activities.

They also revealed a lack of guidelines for testing defences against cybercrime, including attacks targeting the company's systems.

2.2.2 Incidents

In 2018 a total of 189 ICT-related incidents were reported to Finanstilsynet, which is approximately the same number as in 2017. Five of the incidents were intentional security incidents, i.e. cybercrime. The other 184 reports were notifications of operational incidents.

Customers experienced higher availability of payment services and customer-facing solutions in 2018 than in 2017. Moreover, the incidents that occurred were less serious, in terms of the number of customers affected and the duration of the service disruption.

An incident occurring at a data centre when acoustic effects or pressure changes caused a hard disk drive crash attracted the most attention.

Reports were received of a number of incidents caused by poor governance of customers' user identities, which resulted in serious breaches of confidentiality. One incident was also reported that was caused by use of a robot to generate letters to customers which were then sent to the wrong recipients.

Several institutions reported their detection of security flaws, although these had not necessarily been exploited for malicious purposes.

2.2.3 Outsourcing notifications

A total of 161 notifications of outsourcing were processed in 2018, compared with 86 notifications in 2017.

The notifications show a clear tendency towards increased use of cloud services. Finanstilsynet has the impression that, on the whole, institutions that use cloud services perform the necessary risk assessments, make an effort to meet security requirements, and pay sufficient attention to monitoring of operations and security in the outsourced activity.

Through their service provider management procedures, financial institutions must ensure the necessary governance of outsourced activities. Institutions must therefore have the necessary capability and expertise to meet this requirement.

2.2.4 ICT and information security

Financial institutions have observed a significant increase in undesirable activity (cybercrime) targeting their technical infrastructure and systems from one year to the next. At the same time, Finanstilsynet sees that institutions are increasingly aware that the threat picture constantly changes. The institutions continuously improve their cyber defences, which include surveillance of technical infrastructure and systems. Establishing adequate cyber defences is a challenge.

Cyber attacks are usually averted before the institutions suffer any consequences. To date, there have been no security incidents in the financial sector that have had consequences for financial stability.

Targeted attacks on financial institutions in other countries have primarily been motivated by financial gain. Payer manipulation using a combination of digital manipulation and social engineering has proved most successful, and is therefore proliferating.

Institutions have mainly concentrated on protecting their networks from external attack. However, institutions must also focus attention on their ability to detect and eliminate malicious operators within their networks.

Failure to classify information entails a risk that the information is not covered by protective measures, and confidential information can therefore fall into the wrong hands.

Cyber attacks can undermine confidence in financial institutions and financial stability, and is a steadily growing threat. The goal of the EU Commission and the European supervisory authorities EBA, ESMA and EIOPA is to harmonise and establish minimum requirements for ICT security for the financial sector. These institutions also point to the need to coordinate regulatory and security testing frameworks so as to test the robustness of institutions' cyber defences. This is an area on which supervisory authorities will continue to focus attention.

2.2.5 Financial technology trends

Developments in financial technology are driven by both new and existing financial institutions. Institutions continuously seek to simplify and improve their ICT solutions. At the same time, the complexity and vulnerability of the overall technical infrastructure are increasing as a result of the larger number of operators, new technology, more services, and the generally high pace of change.

Institutions that use artificial intelligence (AI) should design a management model which establishes necessary principles for its use, and which is supported and approved by the institution's executive management and board of directors.

2.2.6 Governance of ICT activities

Financial institutions must establish a functional governance model for ICT activities based on the principle of three lines of defence: operational management, risk management and compliance, and internal audits. Institutions must also establish effective ICT risk management procedures, with broad-based involvement of the institution's personnel and a good understanding of risk.

Ensuring adequate ICT expertise is a challenge for institutions. There is a risk that the financial sector will be unable to meet its future needs for skills and knowledge in Norway in critical areas of expertise. This could further increase their dependence on foreign operators in the years to come, and give rise to new vulnerabilities and higher risk. Finanstilsynet stresses the importance of institutions

that outsource services to other countries establishing contingency measures whereby critical ICT services can be taken over and performed by personnel in Norway or in other countries if service providers outside Norway should be unable to perform these services due to geopolitical conditions.

2.3 Financial institutions' assessments

Financial institutions consider the following threats to be the most important:

- social engineering whereby the attacker can obtain unauthorised accesses and use them fraudulently
- fraud committed by family members, such as by misusing BankID
- pressure to deliver, due to both the many new regulations and customer demands
- increased complexity of system portfolios
- multiple service providers involved in service delivery
- change in and relocation of operating sites
- cyber attacks
- lack of expertise in key ICT fields

According to the financial institutions, risk related to poor data quality and inadequate protection of unstructured data is declining. This may be a result of the work the institutions have done in connection with implementation of the EU's General Data Protection Regulation (GDPR).

Financial institutions see the growing number of service providers, and subcontractors, in value chains as a risk, due to the increased complexity of infrastructure and interaction. The scope of changes and new regulatory requirements may reduce institutions' ability to deliver on time and with the requisite quality. The tendency towards diminishing risk associated with organisational deficiencies, job descriptions, reporting and control, has come to a standstill.

The financial institutions' assessment of risk related to protection of sensitive data shows that the picture is approximately the same as in 2017.

Finanstilsynet considers that financial institutions have gained better control of disclosure of user identities and passwords to customers and employees. The risk of an attacker stealing a user identity and making fraudulent use of it is therefore deemed to have decreased somewhat.

The risk of money laundering has been reduced by improvements in IT systems' ability to collect relevant information on customers, customer relations and customer behaviour as a basis for controls.

Overall, financial institutions seem to assess risk as having increased slightly in 2018, as it did in 2017 and 2016.

2.4 Current areas of risk

Financial infrastructure

Finanstilsynet considers Norway's financial infrastructure to be robust. There were no ICT incidents that impacted on financial stability in 2018, although one critical incident occurred in central infrastructure in the payment service and some incidents rendered payment solutions unavailable for periods of time. On the whole, stability in 2018 was better than in 2017, and on a par with 2016.

Financial institutions

Finanstilsynet considers vulnerabilities in financial institutions' operating systems, access management, business continuity management and disaster recovery systems, handling of confidential information and cybercrime defences to be the primary threats related to the institutions' use of ICT. All of these are assessed as being medium to high-risk threats.

Vulnerabilities in financial institutions' service provider management, change management, governance model and lines of defence for ICT activities, and vulnerabilities related to geopolitical conditions and ICT expertise in Norway, also constitute threats to the institutions' use of ICT. These are considered to be medium-risk threats.

Financial institutions' customers

Due to increased digitalisation, institutions' customers have had to use digital identification and authorisation systems that often consist of a password or a code that must be remembered. Many people find this a challenge, and often write down their passwords. Passwords and codes that are shared or stolen pose a considerable risk of fraudulent use, at the worst with substantial financial consequences for the victim.

Fraud targeting bank customers, such as love scams, investment fraud, fake invoices and customers who are misled into divulging sensitive information poses a significantly greater risk to individual customers than cybercrime targeting financial institutions or use of the institutions' systems.

3 Finanstilsynet's findings and assessments

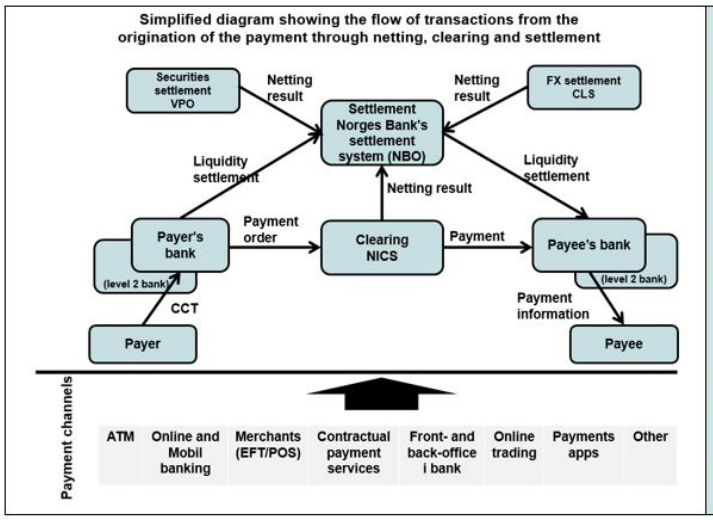
3.1 Payment services

3.1.1 General comments regarding payment services

Effective, robust and stable payment services are a fundamental prerequisite for financial stability and well-functioning markets. The Norwegian payment system infrastructure is among the most efficient and reasonably priced[1] in the world.

In Norway, payment systems and services are governed by laws and regulations and through the financial industry's self-regulatory system, which is administered by Finance Norway (FNO) and Bits. Partly as a result of the revised Payment Services Directive (PSD 2), a number of regulatory amendments have been adopted with effect from 1 April 2019 that will affect payment services. The most pivotal changes concern the Act relating to Payment Services, Regulations on Payment Service Systems and Regulations on Payment Services.

Figure 1: Flow of transactions in the Norwegian payment service



A payment system is defined as a system based on common rules for clearing, settling and transferring payments between two parties to a financial transaction. A legal distinction is made between interbank systems, which process transactions between banks, and payment services, which handle transactions between customers and banks.

Figure 1 shows the flow of transactions in the Norwegian payments system. The lower portion of the figure shows the various payment channels used by customers.

Source: Finanstilsynet

[1] Financial Infrastructure 2018. Report from Norges Bank.
Bits: Joint evaluation of possible participation in the P27 initiative concluded in Norway

3.1.2 Governance of risk and vulnerabilities in payment services

Good governance on the part of financial institutions is crucial to ensuring robust, stable payment services.

The regulatory framework sets a number of requirements for the governance of payment services[2], including the management and control of operational and security risk. These requirements will apply to both institutions that currently provide payment services and new payment service providers.

Payment service providers must carry out risk and vulnerability assessments prior to launching a new payment service and in the event of incidents or changes of significance for the level of security. Measures based on the results of risk and vulnerability assessments must be established to ensure the necessary confidentiality, integrity and availability. Financial institutions must make sure that their systems are in compliance with regulatory frameworks, agreements and internal procedures, and are responsible for ensuring that each system is protected in its entirety (end-to-end) by logical and physical security measures.

Data traffic in electronic payment services must be monitored to ensure an adequate level of security and it must be possible to detect and prevent unauthorised use of the service. Payment service providers must report payment service fraud statistics at least once a year to Finanstilsynet.

Payment service providers must have systems and control mechanisms for operational and security risk related to service performance, as well as effective procedures for dealing with incidents, including serious operational incidents and security incidents. At least once a year, payment service providers must submit to Finanstilsynet an overall assessment of operational risk and security risk related to the services, and an assessment of their own measures.

Finanstilsynet notes the high pace of change, which in itself creates higher risk. These changes must be seen in the light of increased competition as a consequence of technological advances, regulatory amendments and customer expectations. New operators enter the value chain, and payment services are integrated into other services. A number of financial institutions have already established application programming interfaces (APIs) that enable third-party operators to offer new services. Account servicing payment service providers (ASPSPs) are expected to make extensive efforts to ensure that the quality of their new APIs eliminates the need to keep existing customer interfaces available as a fallback solution. Finanstilsynet is aware that financial technology enterprises have shown great interest in exploiting the new opportunities that PSD 2 offers with regard to access to payment accounts.

In Finanstilsynet's experience, financial institutions invest extensive effort in their disaster recovery systems, also called backup or contingency systems, in order to reduce their vulnerability to operational irregularities in payment services. The number of incidents in 2018 was at the same level

[2] See the Regulations on Payment Service Systems

as in 2017, but the availability of financial institutions' payment services was better, on the whole, in 2018 than the year before. However, the incidents show that institutions must continue to focus on improving the quality of their change processes and the disaster recovery systems of payment services, both to reduce the number of incidents and to mitigate the negative consequences of an incident.

When incidents occur, it is important to provide customers with comprehensive information. If an incident affects or could affect customers' financial interests, the service provider must notify the customers without undue delay. The notification must contain information on actions that can be taken by the customers themselves.

Finanstilsynet underscores the responsibility of the board of directors and executive management to ensure that the institution has procedures and systems to provide stable operating systems and effective disaster recovery systems. This responsibility also applies to any parts of services that are outsourced.

3.1.3 Notification regarding payment service systems

The Payment Services Act requires that Finanstilsynet be notified without undue delay of the establishment and operation of payment services. The duty of notification applies to both existing and new licensed institutions, and covers banks, e-money institutions, payment institutions and other operators in cases where the institution is to provide payment services. Finanstilsynet will monitor institutions' compliance with the duty of notification.

The following are subject to notification (specified in Finanstilsynet's circular 17/2004):

- introduction of a new payment service system
- a new version that materially affects other parties involved in the payment service
- a new version with a modified or new functionality of material importance for the payment service system.

In 2018, Finanstilsynet received 12 notifications of new or modified payment service systems. The notifications mainly concern changes in online banks, payment card systems, PSD 2 interfaces (APIs) and Vipps services.

3.1.4 Developments in payment services and mobile payment services

Trends

Developments in payment services take the form of new operators entering the market, current operators' offers of new services based on existing systems, new partnership constellations between banks or between banks and other operators, and collaboration between payment service users.

At the start of 2018, a majority of the banks operating in the Norwegian market were participating in the Vipps partnership. Vipps is the primary mobile payment service in Norway, but can only be used for payment in physical stores to a limited extent. Through Vipps, account-to-account payments may be made (for the time being only for person-to-person payments) by using the instant payment infrastructure[3], or MasterCard and Visa's payment card systems. In 2018, Vipps launched the possibility of payment of e-invoices.

To strengthen their competitiveness in relation to global operators, Vipps AS, BankAxept AS and BankID AS merged in 2018. The new company has kept the name Vipps AS.

Many merchants have previously chosen not to permit contactless payments since this technology was only available through Visa and MasterCard's international payment services. In 2017, BankAxept AS established support for contactless payment using physical cards, and in the course of 2018 the banks rolled out a multitude of payment cards that support contactless payments, also for BankAxept. The number of merchants who accept contactless payments has increased substantially and customer behaviour patterns are gradually changing.

In 2018, Aera Payment & Identification AS (Aera) continued its efforts to establish an open payment platform capable of accepting all types[4] of cross-channel payments (e-commerce, mobile commerce and in-store)[5] and to be integrated with the retail grocery sector's store systems and loyalty programmes.

The use of biometrics in connection with authentication and payment is on the rise, and several financial institutions now use both fingerprint touch and facial recognition systems to log onto mobile devices.

Several Norwegian banks have established bilateral agreements enabling them to provide services equivalent to PSD 2's payment authorisation services and account information services for payment accounts in the banks that are party to the agreements. There are also banks that have established bilateral agreements that offer additional payment services to those under PSD 2, usually called "Open Banking". See also 3.15.2.

In 2018, a number of banks entered into partnership with Apple so that their payment cards could be used on Apple Pay[6]. Some banks also signed an agreement with Google to enable their payment cards

[3] Https://www.bits.no/bank/straksbetalinger
[4] BankAxept, Visa/Visa, Electron, MasterCard/Maestro, Diners, American Express, JCB, China Union Pay, Apple Pay, Samsung Pay and Android Pay, Vipps, Alipay
[5] https://aera.id/betaling/
[6] https://www.tek.no/artikler/nordea-melder-om-ekstrem-interesse-for-apple-pay/440510

to be used on Google Pay[7]. Several banks also established agreements in 2018 that make it possible to make watch-based payments (Garmin Pay and Fitbit Pay).[8]

In autumn 2017, it became possible for Chinese tourists in Norway to pay using Alipay. In 2018, Alipay entered into collaboration with Nets, enabling Norwegian stores to accept Alipay payments in the same way as Visa or MasterCard payments. The technology is based on QR codes. Alipay has also entered into an agreement with Vipps to facilitate Alipay payments.

PSD 2 sets strict requirements regarding customer authentication and certificate solutions. Buypass[9] will offer electronic certificate solutions that are PSD 2-compliant.

For e-commerce purposes, several different means of payment are currently available, such as payment cards, invoice-based payment through a variety of payment service providers or invoice collection agencies, or cash-on-delivery payment. Several service providers offer "checkout" solutions, i.e. they are full-range providers of all types of payment. Under PSD 2, payment service providers may also offer account-to-account payment.

Rules equivalent to PSD 2 entered into force on 1 April 2019

Under PSD 2, licensed financial institutions may access account information and are authorised to make payments on behalf of customers. The rules governing access to payment accounts in order to perform payment authorisation services and account information services are set out in regulations on payment service systems, as well as in rules in accordance with the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, which are to apply from 14 September 2019, also in Norway.

Account servicing payment service providers (ASPSPs) are working to establish APIs that enable third-party operators to offer new services based on access to payment accounts. By 14 September 2019, all ASPSPs in Norway are expected to have established dedicated interfaces and applied for approval of exemption from the requirement of fallback solutions.

Through an open payment market, and the establishment of public APIs for the infrastructure of financial institutions, new and existing licensed operators will be able to offer the new payment services, i.e. payment initiation services[10] and account information services[11]. A number of ICT service providers have established an interconnectivity platform for PSD 2, to form an access hub for

[7] https://www.dinside.no/mobil/na-kommer-google-pay-til-norge/70394529
[8] https://www.dinside.no/mobil/na-kan-dnb-kunder-betale-med-klokka---men-kanskje-ikke-den-du-onsker/70537330
[9] https://www.tu.no/filer/EVENT/Digital2017_presentasjoner/Mads_Henriksveen_Buypass.pdf
[10] Payment Initiation Service Providers (PISP). Operators who may initiate payments on behalf of customers
[11] Account Information Service Providers (AISP). Operators who may retrieve information from bank accounts on behalf of customers

financial institutions' APIs to which third party operators wishing to offer payment initiation services and account information services can connect.

Now that PSD 2 has come into force in Norway, Finanstilsynet anticipates a moderate influx of licence applications from new operators, equivalent to the trend observed in EU countries. PSD 2 imposes more requirements on payment institutions applying for licences than PSD 1, but several of the requirements had already been introduced in Norway. This was the case, for instance, for requirements regarding incident reporting, risk assessments related to payment services, security and strong customer authentication. Banks have also been subject to fraud reporting requirements.

As a result of the implementation of PSD 2 in Norwegian law, the obligations of payment service providers regarding reporting of incidents and security incidents are being harmonised with the European Banking Authority's (EBA) incident reporting guidelines. Moreover, payment service providers must report payment service fraud every six months and report their overall assessment of operational risk and security risk annually, in addition to assessing the payment service providers' corrective actions.

Since the rules came into force, foreign operators who submit notification of cross-border activities for new payment services have been authorised to access payment accounts in banks operating in Norway. Finanstilsynet expects more international operators to establish new payment services in the Norwegian market. A number of global operators have already notified Finanstilsynet of cross-border services to Norway, while others have only established services in one or more EU countries for the time being.

3.1.5 Losses arising from payment card fraud

The tables below present statistics for losses arising from payment card and online banking fraud perpetrated against Norwegian customers in the past few years. The figures show total losses, regardless of whether the loss is covered by the customer, the bank or the payment card company.

Losses in Norway related to use of cards

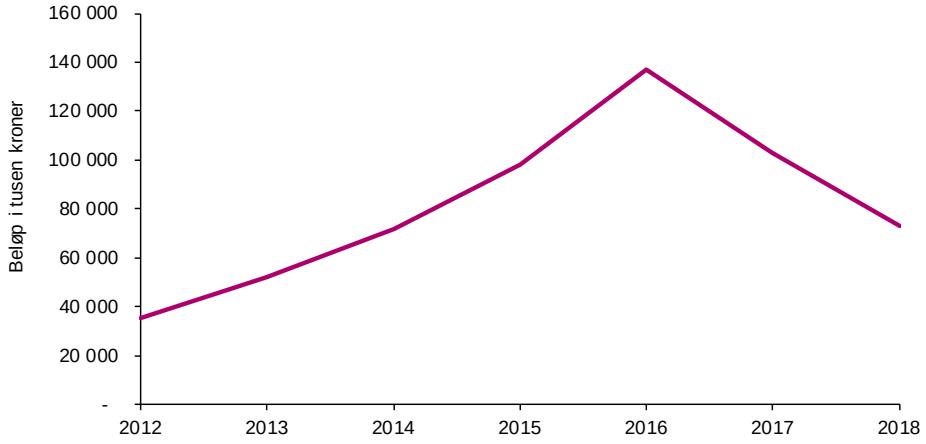
Total losses relating to card payments were reduced by 36 per cent in 2018, and were more than halved compared with 2016. The number of fraudulently used cards was reduced by 46 per cent from 2017 to 2018.

Table 1: Payment card losses (amounts in NOK 1 000)

Type of payment card fraud	2013	2014	2015	2016	2017	2018
Fraudulent use of card data, CardNot-Present (CNP) (online transactions, etc.)	51 954	72 056	98 410	137 015	102 908	72 909
Stolen card data (including. skimming), fraudulently used with counterfeit cards in Norway	762	524	2 670	1 360	483	3 098
Stolen card data (including skimming), fraudulently used with counterfeit cards outside Norway	51 534	51 685	48 447	41 762	17 452	6 308
Original cards lost or stolen, fraudulently used with PIN in Norway	21 274	21 266	18 875	12 857	10 194	4 972
Original cards lost or stolen, fraudulently used with PIN outside Norway	9 570	13 071	14 224	10 223	9 663	4 699
Original cards lost or stolen, fraudulently used without PIN	4 949	5 510	6 033	3 286	4 891	618
Total	**140 043**	**164 113**	**188 660**	**206 503**	**145 591**	**92 604**

Sources: Finanstilsynet and Bits

Figure 2: Fraudulent use of card data, Card-Not-Present (CNP) (amounts in NOK 1 000)



Sources: Finanstilsynet and Bits

Payment card fraud and data theft

The two biggest categories of payment card loss, i.e. e-commerce losses and losses related to the fraudulent use of counterfeit cards outside Norway, have shown the greatest decline. Finanstilsynet believes that the substantial decrease in losses related to payment cards used in e-commerce can be attributed to more stringent regulatory frameworks and the stricter requirements imposed by payment card issuers, payment card acquirers and merchants with regard to strong cardholder authentication, using security protocols such as 3D Secure[12], the preventive measures implemented by financial institutions such as monitoring of card use and the like. The reduction in losses related to the fraudulent use of counterfeit cards outside Norway is due to the fact that fewer and fewer countries use only the magnetic stripe and not a chip. All cards issued in Norway have a chip, which is used to make payments. Fraudsters are unable to copy chips for use in counterfeit cards.

Costs related to payment card fraud

Table 2: Costs related to payment card fraud (amounts in NOK 1 000)

Costs related to payment card fraud	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Number of cards affected by fraud	22 531	38 541	44 900	68 162	65 024	34 999
Total direct losses, see Table 1	140 043	164 113	188 660	206 503	145 591	92 604
Administrative costs for card issuer (NOK 2,250 per card)	50 695	86 717	101 025	153 365	146 304	78 748
Consumer costs (NOK 1,000 per card)	22 531	38 541	44 900	68 162	65 024	34 999
Total estimated costs	**213 269**	**289 371**	**334 585**	**428 030**	**356 919**	**206 351**

Source: Finanstilsynet

Finanstilsynet's estimate of total costs related to stolen payment card data is based on the sum of annual direct payment card losses and the estimated average administrative cost for the card issuer per fraudulently used card, and includes any losses incurred by the merchant, card acquirer, card issuer or card owner. A cost per card has also been estimated, based on the costs incurred by the consumer in connection with stolen card data.

Losses related to online banking

Losses related to online banking rose in 2018. Using the Retefe trojan, fraudsters succeeded in effecting some fraudulent transactions. However, the banks were able to stop most of the attempts to carry out online banking fraud.

[12] The payment card companies' standard for identifying and protecting buyers and sellers when cards are used for online payments.

Table 3: Losses related to online banking (amounts in NOK 1 000)

Type of fraud – online banking	2013	2014	2015	2016	2017	2018
Attacks using malware on customer's PC or security device (Trojans)	1 327	552	3 055	2	727	1 304
Lost/stolen security device	1 285	6 655	963	8 758	1 892	874
Phishing and false BankID – merchants		539	5815	2 428	2 057	16 384
Other/unknown	779	3 474	2 715	7 444	2 911	1 624
Total	**3 391**	**11 220**	**12 548**	**18 632**	**7 587**	20 186

Sources: Finanstilsynet and Bits

Losses related to social engineering fraud

Statistics for 2018 have been compiled from banks' registered losses related to social engineering fraud. The losses have been broken down by type of social engineering. The categorisation is somewhat uncertain, as many banks had not specified losses by type, and in some cases the fraud was a combination of types of fraud. The statistics show that social engineering generates the highest profit for fraudsters. In 2018, losses totalled just under NOK 300 million, almost three times as high as losses related to payment card and online fraud combined. Not all cases of social engineering fraud are reported to the banks, and actual losses are probably significantly higher.

Losses related to social engineering fraud are losses incurred by customers, not by banks. The customers who are defrauded often contact their bank to ask them to stop transactions and reverse the transfer of funds. Finanstilsynet is aware that banks alert customers when the banks, in light of their knowledge of a customer, identify repeated transactions that are abnormal behaviour on the part of that customer.

Victims of social engineering can also be inveigled into performing services for fraudsters. For example, the customer may be talked into letting his account be used for money transfers, thereby helping to conceal transfers of funds deriving from unlawful activity to recipients in other countries.

Table 4: Losses related to social engineering of payers (amounts in NOK 1 000)

Types of fraud in 2018	Number of cases
Payment for renting an object the payee does not own	948
Deposits in response to promises of large payments later	9 091
Love scams	88 191
Investments in fake companies	92 073
Payment for goods not delivered	11 972
Payee account changed	8 606
CEO fraud	33 913
Fraudulent invoices	32 982
Other/new types	19 593
TOTAL	**297 369**

Sources: Finanstilsynet and Bits

3.2 Payment institutions

Finanstilsynet monitors payment institutions in accordance with the requirements in the ICT Regulations, the Regulations on Payment Service Systems, the EBA Guidelines on the security of Internet payments and the anti-money laundering regulatory framework. Through its supervision of payment institutions in 2018, Finanstilsynet identified inadequate provision of information on payment service functions and a lack of options. Customers may have the impression that they are not in control of their own data and payments if they are not given clear information on new functionalities and cannot make their own choices as to whether to use new payment service functionalities.

Finanstilsynet's supervision of payment institutions has also included monitoring of compliance with anti-money laundering rules. Many payment institutions have both merchants and end-users as customers. The risk of money-laundering and the need for stronger measures targeting customers are often greatest where merchants are concerned. Finanstilsynet has identified deficiencies in payment institutions' control of merchant customers.

3.3 Banks

3.3.1 Governance

Finanstilsynet has identified a number of deficiencies in banks' compliance with the ICT Regulations ("Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)"), including with regard to ICT governance. The banking industry's management model is largely based on an approved model consisting of three lines of defence: operational management, risk management and compliance, and internal audits; see 3.11.

Finanstilsynet's findings can chiefly be linked to three areas: deficiencies in the way governance functions are established, poor organisation and unclear lines of reporting, and inadequate efforts to secure sufficient expertise and resources.

Outsourced services, in particular, offer the greatest potential for improvement. It is important to underscore that banks' reporting on governance efforts in their own operations must be based on their own assessments; see 3.8.

In the Risk and Vulnerability Analysis for 2017, Finanstilsynet pointed out that financial institutions must ensure that risks at every level of the value chain are identified, assessed and managed. In addition, banks must have the requisite expertise and capacity to attain the level of security necessary to maintain sound operations. This assessment is still relevant in 2018. See also 3.13.

3.3.2 Information security

Information security is an area to which financial institutions devote considerable attention. In order to adopt a methodical approach to information security, it is important to have established a security policy. The institution's management is responsible for ensuring that the security policy is aligned with the institution's commercial goals and the applicable regulatory requirements.

The security policy must reflect the institution's information security requirements. Finanstilsynet considers it important that it contain a description of how responsibility for information security is defined. The policy must also include a description of how compliance with the policy is to be monitored and of reporting requirements. The institution's executive management is responsible for ensuring that the content of the policy meets the institution's requirements.

3.3.3 Business continuity management, disaster management and disaster recovery systems

Business Continuity Management (BCM) in a financial institution is a vital, central function aimed at ensuring to the greatest possible degree that the institution is prepared for and capable of dealing with a serious situation, often defined as a crisis or disaster (circumstances that result in the institution not being able to maintain its normal activity, in either all or parts of the institution's operations).

Disaster management plays a pivotal role when a crisis or disaster occurs. The difference between business continuity management and disaster management is not always clearly apparent, but the disaster management function is deemed to have overall operational responsibility for leading the institution through a crisis or disaster. The disaster management staff will often be personnel who deal with more serious situations where life and health are at stake. 'Crisis' is an appropriate term for serious ICT incidents. Disasters are largely situations that jeopardise the life and health of employees.

Finanstilsynet recently conducted a comprehensive questionnaire survey on business continuity management and disaster recovery systems, which targeted Norwegian banks and international banks with branches in Norway. The survey provides a picture of the banks' capability of dealing with a serious ICT incident. Finanstilsynet notes that, for the most part, financial institutions have established disaster recovery systems, also called contingency planning systems or backup systems, to be

implemented if normal operating systems are not available. However, a number of deficiencies have been detected that constitute a risk that institutions will face challenges in handling a serious ICT incident. These include deficiencies in governance documents, training, exercises and testing of disaster recovery systems. The survey shows that the institutions should focus more attention on business continuity management and disaster recovery systems, thereby reducing the risk of extensive damage in the event of serious incidents.

3.3.4 Access management

In its inspections, Finanstilsynet has assessed financial institutions' procedures for management and control of employee access to and use of the institutions' systems. In this type of inspection, there is particular focus on institutions' governance of expanded access rights for its own personnel, and for personnel employed by the institution's ICT service providers.

Finanstilsynet is aware that service providers are often authorised to set up users with privileged access rights in the institutions' systems. Such rights constitute a special risk as personnel have access enabling them to change data, retrieve data or affect system operation. The person carrying out the actions can conceal unauthorised actions by deleting log data.

Personnel who are to be given privileged access rights should be subjected to special background checks before such rights are granted. It is also important to maintain close control of persons granted access rights, and to whether these rights are in fact necessary for performance of their tasks. Individual institutions should make it a requirement that privileged access rights be reviewed periodically. Finanstilsynet is aware that financial institutions are strengthening controls by using special access management systems for privileged access rights, a measure that Finanstilsynet considers necessary to achieve effective governance.

With regard to other access rights, Finanstilsynet notes that it is difficult for management staff to understand and interpret detailed overviews showing the access rights and authorisation level of employees. As a result, the quality of the review is impaired, and personnel have access rights that exceed their level of authorisation. System support for role-based access management is intended to ensure that employees are only granted access to the systems and information necessary to enable them to perform their tasks. This is an extremely important risk-mitigating measure.

3.3.5 Systems for detecting money laundering and financing of terrorism

Effective systems for monitoring electronic transactions (anti-money laundering systems) are absolutely essential to enable financial institutions to comply with section 25 'Duty to conduct examinations' and section 26 'Duty to report' of the Anti-Money Laundering Act, and to comply with the requirements in section 38 for such systems. In the past few years, Finanstilsynet has carried out more anti-money laundering inspections than before, and has observed a shift towards the use of more sophisticated scenarios to detect money laundering and financing of terrorism. However, in transaction

monitoring, there is still a high percentage of hits that are not real, i.e. false positive hits, and there are often a number of scenarios for which there are no hits. Finanstilsynet ascribes this to the fact that the work of identifying and developing scenarios, which in turn serve as the basis for monitoring of transactions through the anti-money laundering rules, has not been given the necessary priority by financial institutions' boards and executive management. There is still considerable potential for developing scenarios that assess the customer relationship as a whole, and that can detect deviations from expected customer behaviour.

Through incident reporting, Finanstilsynet has been informed that a number of customers and transactions have not been monitored because they were not included in data extracted from the source system, where the transaction is generated, to the anti-money laundering system. Changes in the source systems, extraction of data to the anti-money laundering system or operations have proved to potentially result in deficiencies in data extraction that have not been detected when testing the changes. In future anti-money laundering inspections, Finanstilsynet will place emphasis on financial institutions having proper procedures for verifying that the data extracted to the anti-money laundering system are complete.

3.3.6 Transaction monitoring

Analyses of transaction patterns in order to detect unauthorised transactions are largely based on rules defined in the surveillance systems. Fraudsters are able to test which rules apply and hence circumvent them. Furthermore, a large percentage of identified irregularities have proved not to be a result of criminal acts. The transaction monitoring process could be substantially improved by using machine learning (ML), whereby each customer transaction will contribute towards developing the algorithm in the system, thus making it "smarter" and producing more accurate results. In light of the multitude of new operators that will presumably emerge as a result of PSD 2, Finanstilsynet considers the use of more advanced monitoring tools to be an important risk-mitigating measure in efforts to combat criminal activity targeting bank customers, as well as money laundering and terrorist financing.

3.3.7 Banks' compliance with the reporting requirements of the Norwegian Banks' Guarantee Fund

In 2018, Finanstilsynet, in collaboration with the Norwegian Banks' Guarantee Fund, again carried out inspections to assess banks' compliance with requirements regarding IT systems for reporting to the Norwegian Banks' Guarantee Fund if the bank is placed under public administration. The data systems have been tested for several years. The conclusion is that the quality of banks' reporting has steadily improved and is approaching a satisfactory level.

If customer deposits become unavailable due to the bank being placed under public administration, the Norwegian Banks' Guarantee Fund will reimburse the guaranteed deposits within seven working days. Details of this scheme may be found on the Norwegian Banks' Guarantee Fund website[13].

[13] https://www.bankenessikringsfond.no/krav-til-datafiler/category891.html

3.4 Securities

3.4.1 Incidents in the securities sector

The securities sector has been impacted by some serious IT incidents in the past few years. For example, data hall failures have affected marketplaces, and IT process malfunctions have resulted in significant erroneous disbursements. The consequences for the financial market are greatest when infrastructure institutions are affected.

The incidents in the securities sector show that institutions carry out effective data recovery procedures, and that active efforts are being made to reduce both the number of errors that occur and their consequences.

Finanstilsynet has carried out a number of on-site inspections with focus on digital security. This has provided greater knowledge of financial institutions' emergency preparedness for cybercrime. After Finanstilsynet's findings were brought to their attention, the institutions have taken steps to improve their defence capability.

3.4.2 Configuration of test systems

Various types of errors that were not detected due to the incorrect configuration of test systems have posed a challenge to the stability and quality of operations in several financial institutions in connection with production release. The problems detected include test systems that are not configured in the same way as the production system and test systems that have access management deficiencies.

3.4.3 Storage system failure

In 2018, incidents occurred in data halls where the hard disk drives (HDD) in storage units failed due to acoustic resonance or an increase in air pressure. Acoustic effects can be caused by alarms or sounds produced by the release of fire extinguishing gas. Pressure changes in data halls can arise due to the rapid release of fire extinguishing gases when automatic fire extinguishing systems are activated, which may affect the HDD's read head and damage the magnetic platters. At the very worst, this could affect all of the institution's HDDs. To eliminate this risk, HDDs can be replaced by solid state drives (SSD), a storage medium with no mechanical parts. However, the costs related to SSDs can be high.

Finanstilsynet recommends that financial institutions consider whether their installations are in the risk category for this type of incident.

3.4.4 Guidelines for use of a third party in security testing

In on-site inspections, Finanstilsynet has noted that third-party operators are often used to test financial institutions' security setups. Risk factors that must be addressed in such testing include the choice of security testing company and personnel, the way the testing is carried out, and the institution's

monitoring and control of test execution. The institution should also have testing frequency guidelines. Reference is also made to 3.10.2.

3.4.5 Dimensioning and testing of disaster recovery systems

In its inspections, Finanstilsynet found that financial institutions' disaster recovery systems were not designed to ensure sufficient capacity to maintain critical services when the systems are activated.

In Finanstilsynet's experience, tests of the recovery system were carried out when the financial institution's normal operating systems were available, with the result that the recovery system was not necessarily adequately tested. This gives rise to uncertainty as to whether the recovery system would function in accordance with the stipulated requirements in an emergency. In this respect, Finanstilsynet emphasises the importance of testing disaster recovery systems in the circumstances and conditions in which the systems are intended to function.

3.4.6 Organisation of important business system ownership

Ownership of important or critical business systems includes overall responsibility for the system's risk, finances, functionality and security. Finanstilsynet notes that financial institutions interpret the system owner role in different ways, and that in some institutions this responsibility is assigned to IT department employees. This organisational arrangement can create greater distance between business operations and associated IT systems, in addition to which the IT department's priorities could conflict with business area needs. In Finanstilsynet's view, financial institutions should avoid splitting up responsibility for critical systems, and business managers should have overall responsibility for important systems in their respective areas.

3.4.7 Other matters

Sophisticated types of cyber attack pose a growing threat to financial institutions and must be given high priority in institutions' risk assessments. Planning and testing disaster recovery systems and exercises in their use are essential to ensure that institutions are capable of handling real situations caused by a cyber attack.

The possibility that sensitive information may fall into the wrong hands is a real risk and should be given priority in financial institutions' risk assessments. Finanstilsynet underscores the institutions' responsibility for reducing this risk to acceptable levels. Institutions can do this by strengthening their cyber defences, by classifying information, ensuring effective access management and monitoring the documentation they send out.

3.5 Insurance

3.5.1 Underreporting of ICT incidents

Finanstilsynet has previously called attention to the underreporting of ICT incidents in the insurance sector, and notes that incidents are still not being reported. According to section 9 of the ICT Regulations:

> Incidents that lead to a material reduction in functionality as a result of breach of confidentiality (data protection), integrity (protection against unauthorised changes) or availability of ICT systems and/or data, shall be reported to Finanstilsynet. Reporting shall normally cover events that the institution itself categorises as very serious or critical, but may also cover incidents that reveal vulnerabilities in applications, architecture, infrastructure or defence mechanisms.

As a rule, financial institutions that have established incident management procedures have included an assessment of whether the incident is of such a nature that it must be reported to Finanstilsynet. As part of its supervisory activity, Finanstilsynet will make sure that financial institutions report deviations in compliance with the ICT Regulations.

3.5.2 Breach of confidentiality

In light of incidents reported, Finanstilsynet considers that insurance undertakings have not established adequate testing regimes to safeguard security when changes are made in proprietary systems.

Several types of error have been reported. Customers have been given access to other customers' information, both as a result of software errors, and as a result of inadequate testing when technical changes are made. Cases have also been reported where customers have received other customers' invoices, and where reuse of user IDs in company systems has given customers access to customer relationship information that they should not have seen. In one case, a personal identity number was stored as a customer identifier, and the personal identity number information could also be linked to the customer's website navigation activity, when it took place and from which geographical location.

The greatest risk for the insurance undertakings inherent in the reported incidents is loss of reputation.

Finanstilsynet takes a serious view of the incidents reported and has emphasised that responsibility for addressing security issues lies with the board of directors and the executive management. Insurance undertakings should have guidelines for secure development and established testing procedures that ensure that security functionality is protected in connection with all types of system changes.

3.5.3 Monitoring of outsourced activities

Inspections show improvement in insurance undertakings' monitoring of outsourced activities. However, Finanstilsynet still observes that outsourced deliveries are not monitored as closely as internal IT services. Finanstilsynet also notes that there are deficiencies in undertakings' monitoring of their own IT activities. Ongoing monitoring and follow-up of outsourced services are intended to

ensure good management and control. In Finanstilsynet's view, insurance undertakings must strengthen both first and second-line defences in order to meet governance requirements.

3.5.4 Monitoring of security activities

In its inspections, Finanstilsynet has noted that insurance undertakings have not established adequate access management, including monitoring of security in connection with employees' access rights. In some cases, there is also a lack of insight into and monitoring of service providers' access governance. Finanstilsynet's principle is that employees in business-critical systems must only have the accesses necessary to be able to perform their tasks, and that the same applies to personnel with access to service providers' infrastructure and systems. This can constitute a particular risk in cases where service providers' personnel have expanded access rights. In principle, access management is easy to define and control. However, Finanstilsynet notes that insurance undertakings find it a challenge to follow up in practice.

Finanstilsynet expects insurance undertakings' management to focus special attention on the risks inherent in poor security administration, and should ensure that monitoring and security control requirements are laid down in governing documents. This may include lists of specific activities to be carried out periodically, so that the insurance undertaking, both internally and in connection with outsourcing, ensures satisfactory compliance with security requirements.

3.5.5 ICT strategy

Finanstilsynet notes that, on the whole, insurance undertakings have established a specific ICT strategy, in accordance with section 2 of the ICT Regulations. In some cases, however, the ICT strategy established has no clear basis in the undertaking's business strategy. There are also cases of insurance undertakings in large groups that have not taken account of the group's overarching strategies in their own ICT strategy. Finanstilsynet has uncovered cases in which the ICT strategy has not been updated when the undertaking has made changes in its business strategy or in other matters that logically affect its ICT strategy.

Finanstilsynet underscores the undertaking's responsibility for ensuring that all matters of relevance for the ICT strategy are assessed by the undertaking's board of directors. In light of the high pace of change and rapid technological developments, it is important that the ICT strategy is reviewed regularly.

3.6 Audit firms

Finanstilsynet's inspections have revealed that audit firms have outsourced ICT activities without written agreements that ensure adequately that the audit firm has management of, insight into and control of the outsourced activity. Sound outsourcing procedures include identifying, assessing and managing risk related to the outsourcing, and it must be ensured that Finanstilsynet can exercise oversight of the outsourced part of the firm's activities. The requirement of sound risk management,

which includes written agreements, also applies in cases where the activity is outsourced to a company in the same group or the same network. Finanstilsynet has detected the same weaknesses in accountancy firms.

Inspections have also revealed inadequate guidelines for testing defences against cybercrime, including attacks targeting the auditing firm's systems. Guidelines and procedures are an important means of reducing the risk that testing will result in operational disruptions or that information will go astray. Guidelines and procedures must describe requirements applying to testers, and state when and how the testing is to be carried out. If such testing is outsourced, the agreement with the service provider must reflect these principles.

Auditing firms possess confidential information, including information subject to a duty of professional secrecy, personal data and price-sensitive information. It is important to have access guidelines and procedures that reduce the risk of information going astray or being misused. Significant weaknesses have been detected in auditing firms' guidelines and procedures for governance of access to confidential information.

3.7 Incidents reported in 2018

3.7.1 Incident statistics

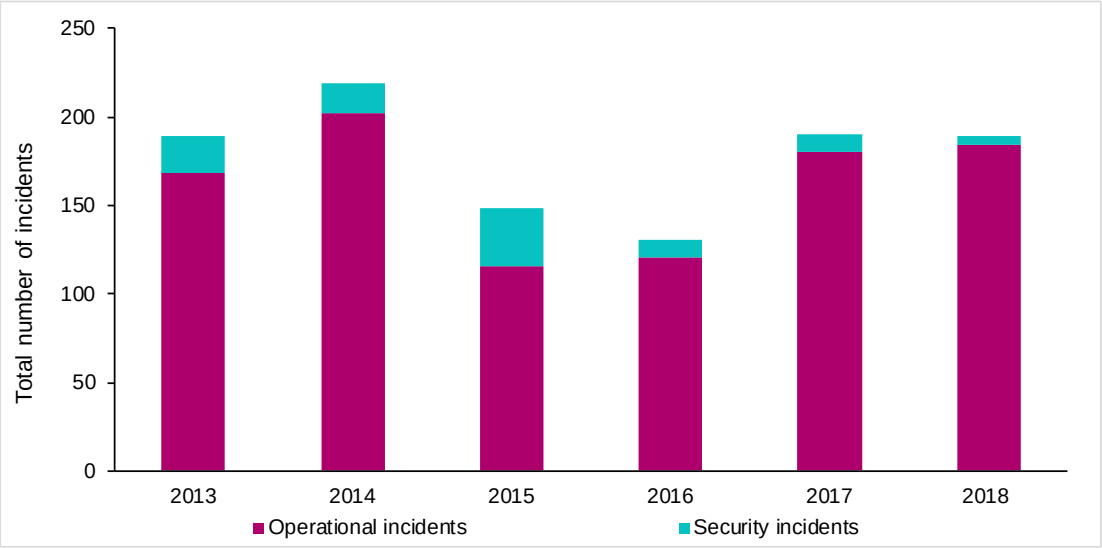
In 2018, a total of 189 incidents were reported by financial institutions subject to supervision by Finanstilsynet. Despite the fact that this is approximately the same number of incidents as in 2017, the availability of payment services was nonetheless better in 2018. This is because incidents were less serious than in the previous year, in terms of the number of customers affected and the duration of disruptions.

Table 5: 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**

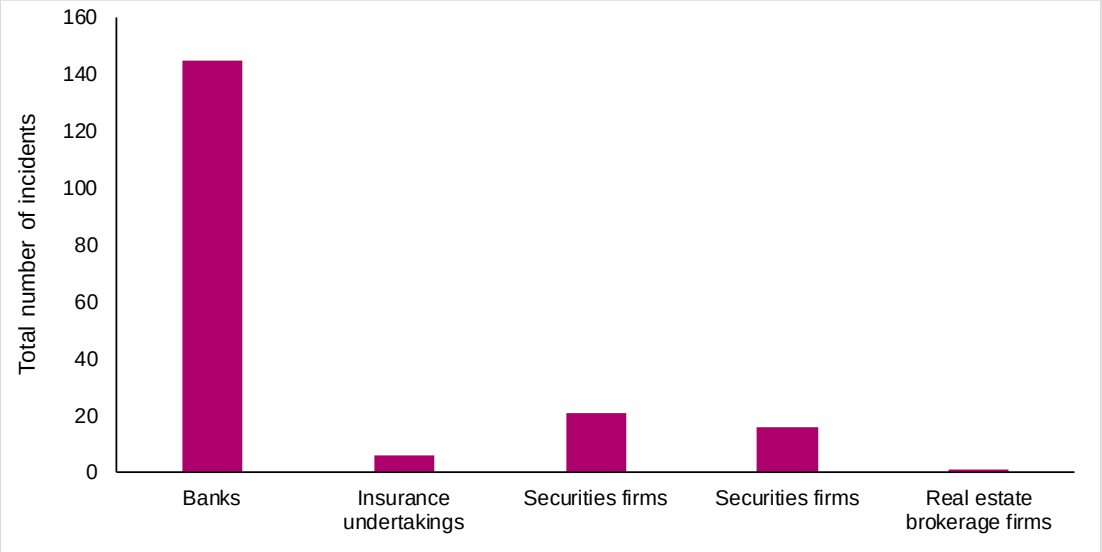
Source: Finanstilsynet

Figure 3: Incidents reported, by operational incidents and security incidents



Source: Finanstilsynet

Figure 4: Incidents reported in 2018, by type of financial institution



Source: Finanstilsynet

Figure 4 shows that banks account for 74 per cent of incidents reported in 2018.

The outbreak of fire at Nasdaq's data centre in Stockholm in April 2018 was the incident that received the most attention, even though the effect for Norwegian customers was limited.

Vipps was impacted by a number of incidents in the first half of 2018. Vipps's complex infrastructure exposes it to the operational problems of many different service providers in the value chain. As a rule, only parts of the service are affected when incidents occur. As the number of customers and functionalities increase, however, incidents that impact on a payment service like Vipps have increasingly serious consequences.

Three incidents involving DDoS attacks against banks were reported in 2018. Despite the relatively high intensity of the attacks, consequences were limited to brief periods of reduced accessibility to the banks' self-service systems.

Some of the financial institutions reported security flaws, which had not necessarily been exploited for malicious purposes. As a rule, security flaws are introduced when changes are made in the system, and are generally discovered by customers who are erroneously given access to other customers' data, or through security tests performed by the institutions. There were also cases where financial institutions' transaction monitoring systems uncovered security flaws when attempts were made to exploit the vulnerabilities.

The causes of operational incidents can roughly be divided into three categories: errors after changes, poor capacity planning, or failures in monitoring parameters such as expiry dates, storage capacity and threshold values. Changes that are not carried out in accordance with established change procedures and poor-quality testing are, as a rule, contributory causes when changes released into production result in errors.

In 2018, there were several incidents attributable to poor governance of user identities. Faulty procedures, or failure to follow established procedures, have led to reuse of user identities, as a result of which the institution's customer is presented with another customer's financial information. This is both a serious breach of confidentiality for the customer whose data are exposed, and a breach of availability for the customer who is unable to access his own data.

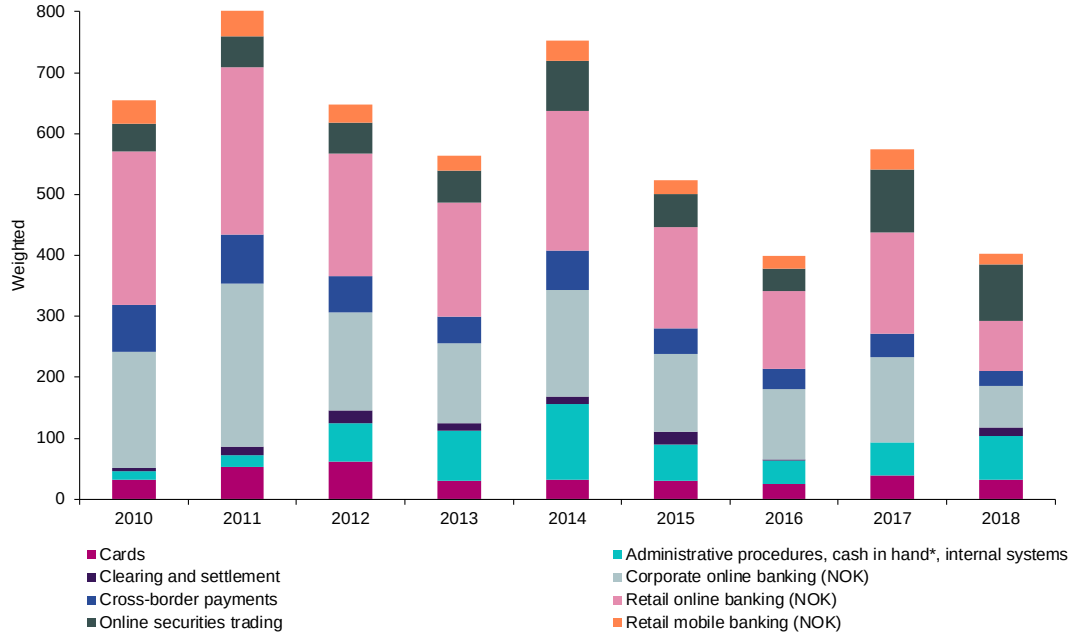
In 2018, for the first time, Finanstilsynet received a report concerning an incident caused by use of a robot. The robot performed the tasks that it was programmed to carry out, but the programmed margins of error were not sufficient to deal with unforeseen incidents involving connected equipment. As a result, letters were sent to the wrong customers.

"The robot generated proof-of-funds letters and stored them as pdf files so they could not be edited. The robot was set up to wait for quite a while for storage to take place, but in some cases the amount of time was not sufficient. If the file was not stored within the set time, the robot defined the proof of funds as "failed" and went on to the next case while the pdf file was still being stored. When the robot was to generate the proof-of-funds letter for the next customer, there was already a pdf file available, namely the one from the previous customer, which the robot used and sent to the next customer."

3.7.2 Analysis of incidents as a measure of availability

For each incident that has caused reduced availability, Finanstilsynet has considered the duration of the disruption, the number of institutions affected, the estimated 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 data are weighted (number of users affected, duration, date, substitute services) and compiled in time series, so that changes can be monitored over time. Figure 5 shows that the payment system and customer-facing systems were more readily available to customers in 2018 than in 2017 and were at the same level as in 2016. The scale on the y-axis is an index obtained on the basis of the weighting of each incident.

Figure 5: Incidents weighted by impact



Source: Finanstilsynet

3.8 Outsourcing

3.8.1 Notification of outsourcing

Finanstilsynet assesses agreements in connection with outsourcing notifications on the basis of section 4 c of the Financial Institutions Act, licence applications and documentation received in connection with ICT inspections. It is emphasised that the undertaking itself is responsible for its own ICT activities, including outsourced services; see section 12 of the ICT Regulations. Sector legislation may also contain detailed rules on outsourcing. Undertakings must establish service provider agreements that are compliant with laws and regulations, and ensure that the service provider and its subcontractors provide ICT services that meet these requirements.

In 2018, Finanstilsynet dealt with 161 notifications of outsourcing from financial undertakings that are subject to the duty of notification. The notifications show increased use of cloud services.

3.8.2 Exit provisions

The European Banking Authority (EBA) Recommendations on outsourcing to cloud service providers[14] entered into force on 1 July 2018.

In Finanstilsynet's assessment, Norwegian regulation of outsourcing of ICT services, as provided by the ICT Regulations, is very largely aligned with the EBA Recommendations. An area not covered in the current Norwegian regulatory regime is the requirement of "exit provisions". According to the EBA Recommendations, outsourcing agreements should contain provisions, including provisions regarding the obligations imposed on the service provider in the agreement, that apply in the event of a transfer to a new service provider, reverting to insourcing or when the services are no longer needed. Finanstilsynet bases its supervisory activities on the EBA Recommendations.

3.8.3 Cloud services

Finanstilsynet considers that, in the decision-making process regarding the use of cloud services, financial institutions perform necessary risk assessments and ensure that security requirements are met. Furthermore, the institutions appear to pay the necessary attention to monitoring operations and security in the outsourced activity. Finanstilsynet notes that more institutions are choosing to establish administrative systems as cloud services, which requires that data be secured by means of encryption and multifactor user authentication.

3.8.4 Vendor management

Each financial institution must ensure the necessary management of its service providers, including making sure that the service providers deliver ICT services in accordance with the stipulated requirements, including applicable legislation. Effective vendor management calls for stringent requirements with regard to the institution's expertise and organisational structure.

The challenge for small institutions lies primarily in acquiring sufficient procurement competence to ensure that all relevant requirements are included in the agreement with the service provider when the service is established, and that the institution has staff with the necessary skills and knowledge to monitor the service provider.

Through their contracts and collaboration models, major financial institutions and alliances have, as a rule, set requirements that define the parameters for vendor management. The challenge lies in the complexity and scope of the services, and the number of service providers, with subcontractors.

[14] https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf

Financial institutions must assure effective governance of the operational, strategic and administrative activities in their interaction with each service provider, and at the interface between service providers. In Finanstilsynet's opinion, the complexity of collaboration between several operators constitutes a risk, particularly if serious incidents should occur.

3.8.5 Independent assessment and review of the service provider's risk management and internal controls

Section 12 Outsourcing of the ICT Regulations states: "The agreement must ensure that the institution under supervision is given the right to control and audit activities carried out by the service provider under the agreement."

A financial institution's internal audits are the function used by the institution's board of directors and executive management to assess whether the institution's ICT service providers conduct proper risk management and internal control of services that are subject to the ICT Regulations. Finanstilsynet considers it important that service providers provide documentation of their own internal control assessments to institutions, in addition to giving institutions access to independent assessments, such as those of the service providers' internal audit.

Independent audit declarations and confirmation of compliance

The largest ICT service providers meet financial institutions' needs to a certain extent, including by issuing an audit declaration such as an ISAE 3402 Type II assurance report, in which the service provider's external auditor, or another party designated by the service provider, assesses the internal control of the service provider's processes through audit activities. Such reviews are often limited to systems that handle financial data, which in turn serve as the basis for the auditor's confirmation of compliance and approval of the institution's financial statements. The review provides a good indication of the quality of the service provider's controls in processes such as change management, access management, availability and security, but at a general level. Finanstilsynet is aware that certain service providers also issue a statement to financial institutions regarding their compliance with the ICT Regulations, where the statement is based on assessments carried out by the service provider's second and third-line defence functions.

Finanstilsynet notes that some service providers do not issue independent declarations or confirmation of compliance with requirements including the ICT Regulations.

Financial institutions should make sure that they obtain independent assessments of service providers' compliance with legislative and contractual requirements. When the institution itself does not consider the service provider's independent assessments to be sufficient, it should take the matter up with the service provider for further clarification. For instance, the institution could specify the type of controls it wishes to have carried out.

Confirmation of compliance from cloud service providers

The services established by the largest cloud service providers, including Microsoft[15], Google[16] and Amazon[17], have integrated control systems, where customers can retrieve information and documentation regarding the service providers' internal control of service deliveries. The institutions that use cloud services must acquire the necessary expertise on and insight into the control systems and choose services that meet their control requirements. This may be a challenge, but Finanstilsynet considers it absolutely essential.

Service provider audits

Finanstilsynet has observed that financial institutions' internal audit function assesses to a varying degree the operational risk and internal controls related to ICT activities in their own operations, and especially those related to the outsourced ICT services. Audits are an important and necessary control function for detecting factors that could pose a significant risk to the institution. Service providers that are not audited represent high inherent risk. In Finanstilsynet's view, financial institutions should ensure that audits are conducted of the most critical areas, including security, risk management, incident handling, access management, change management and availability. These audits can be conducted by the institution's own internal audit function, or by external specialists. In cases where small institutions use the same service provider, the institutions can collaborate on conducting a pooled audit of the service provider.

3.9 ICT security and cybercrime

Finanstilsynet receives regular status updates on the attack and threat picture from financial institutions themselves and from Nordic Financial CERT (NFCERT). Financial institutions see an increase in cybercrime in the form of more attacks, and continuous attempts to carry out targeted attacks. However, Finanstilsynet notes that there have been no security incidents to date in the financial sector that can be described as serious.

Institutions' monitoring systems are increasingly effective, and attacks are usually averted before any consequences arise. This is chiefly due to the generally high maturity of security systems in the financial sector. Nonetheless, incidents that have impacted Norwegian companies in recent years show how important it is that security activities also focus on the inner workings of the institution's network in order to detect fraudsters who have succeeding in breaching defences and establishing a digital foothold in the different zones of the network.

In other countries, where financial institutions have experienced incidents, the primary motive for the targeted attacks has been seen to be financial gain. In this respect, Finanstilsynet refers to an incident in February 2019 where a bank in Malta chose to shut down its systems because attackers succeeded in

[15] https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings
[16] https://cloud.google.com/security/compliance/#/
[17] https://aws.amazon.com/compliance/programs/

penetrating the bank's network. Unauthorised cross-border transactions totalling around EUR 13 million[18] were transferred out of the bank.

In 2018, Norwegian banks were attacked by the Retefe banking trojan. This trojan has been active in certain other countries since as early as 2013, but did not target Norwegian banks until 2018. Most of the attacks were thwarted before the transaction funds left the customer's account, but with the help of the trojan, cyber criminals managed to carry out some fraudulent transactions.

Cases have also been detected of fraudulent domains targeting the financial sector where the aim is to lure employees to click on links, thereby unwittingly installing malicious code in the institution's network. It is difficult for institutions to protect themselves against this type of criminal activity.

3.9.1 Creating a security culture through training and involvement

Finanstilsynet notes that financial institutions have established training programmes on information security and cyber security. In providing training for their employees, institutions create a security culture by increasing employee awareness of threats and vulnerabilities. The training primarily focuses on fundamental attitudes with a view to limiting the risk of the employees performing inadvertent acts as a result of social engineering, among other things. Finanstilsynet considers it important that all financial institutions ensure that their employees repeatedly receive this type of training.

Finanstilsynet has observed that financial institutions' business staff often are not involved in security activities. It is crucial that the business staff are well acquainted with the threat picture, and how it can affect systems that support their own business processes. In Finanstilsynet's opinion, business staff should be more actively involved, and the responsibility of business departments for specifying requirements should be highlighted.

3.9.2 Digital attack trends

A current trend is for attacks to target basic infrastructure and manipulate data that control infrastructure to a greater degree. Sophisticated attacks are launched on network components, and target both hardware and software. Social engineering, including phishing by means of malicious emails, is a rapidly rising threat. In Finanstilsynet's opinion, the greatest threats are posed by well-organised attackers with a high level of expertise and substantial resources.

A professional attack often begins with a reconnaissance stage in the outermost zone of the network, where the attacker identifies vulnerabilities in systems and components that are exposed to the Internet. If the network is successfully infected, further reconnaissance activities are carried out to detect weaknesses in internal zones that can be exploited. If this is successful, the attacker will, over time and undetected, be able to identify possibilities of gaining access to larger parts of the institution's

[18] https://www.timesofmalta.com/articles/view/20190215/local/not-all-money-stolen-in-cyberattack-may-be-found.702048

infrastructure and systems. Once established on the inside, the attacker can take his time acquiring the knowledge he needs before taking any action.

Financial institutions have primarily focused on protecting their networks from attacks from outside. But the fact is that a number of companies, both national and global, have experienced situations where attackers have operated inside their networks for long periods of time. As new methods of attack are developed, the institution's ability to detect and remove unwanted operators within its network will be essential for reducing risk and the scope of damage.

Finanstilsynet considers it important that financial institutions ensure that their monitoring and control do not merely consist of the traditional perimeter defences, but also strengthen monitoring and analysis aimed at identifying whether cyber criminals have established one or more digital footholds within their network.

Finanstilsynet has seen a growing awareness on the part of financial institutions of the fact that forms and methods of attack are constantly changing. Finanstilsynet emphasises that particular attention should be paid by the board of directors and executive management of all institutions to vulnerabilities and threats arising from changes in the threat picture.

3.9.3 Actions when the attacker is inside the network

Reaction times and effective measures are crucial for limiting damage when an attacker is in the process of gaining or has established a foothold inside a financial institution's network. Identifying and isolating infected systems so as to keep them from spreading necessitates predetermined procedures that should be included in the institution's business continuity and disaster recovery plan, which sets out the actions that must be taken and specifies the persons empowered to make decisions on implementation. As far as possible, institutions should identify in advance the potential consequences of the network being shut down entirely or partly, which might be necessary to limit the damage. Predetermined, well-considered action will also facilitate quick decisions, and help ensure that they are taken in the right order.

Finanstilsynet is aware that companies that have experienced this type of serious incident have lacked adequate business continuity plans, including disaster recovery and emergency response plans, and that they had insufficient training and exercises to prepare them for the incident. Continuous, long-term access to key personnel may be necessary, but this may prove difficult to ensure if institutions have not drawn up contingency staffing plans in advance.

The financial sector in Norway has been spared serious cyber incidents, and it is therefore uncertain how an institution will tackle and deal with a grave situation where attackers have established a foothold on the inside and carried out malicious actions. In general, Finanstilsynet finds that financial institutions are not adequately prepared for such situations, and may therefore face major challenges in dealing with serious cyber incidents. However, each institution is responsible for assessing whether it

needs to strengthen its own organisation and collaboration with service providers so as to be as well prepared as possible if a real situation should arise.

In Finanstilsynet's opinion, operators who have faced serious incidents possess invaluable knowledge and experience that could be useful to other institutions. This applies, for instance, to the Helse Sør-Øst[19] and Norsk Hydro[20], both of which have been impacted by serious incidents.

3.9.4 Payer manipulation

Attacks that combine digital and social engineering are the most successful. Attacks are increasing in number and variety, and caused higher losses in 2018 than in the previous year. Banks make extensive efforts to reduce customer losses due to romance fraud, investment fraud, invoice fraud, CEO fraud, etc. Financial institutions' monitoring, fraud detection and fraud intelligence activities manage to prevent around half of the potential losses. Nonetheless, losses are highest in this area of fraud.

3.9.5 Manipulation and digital attacks using artificial intelligence

Finanstilsynet believes that in the long run the financial sector will also feel the effect of "fake news". Artificial intelligence and deep learning have now made it possible to generate credible, but false, images, videos and sound. Non-existent persons, or persons purporting to be someone else, can produce messages and statements that are perceived as genuine by the recipient, but that are manipulated and controlled to influence the recipient in a desired direction. These can take the form of fake presentations targeting employees and management, or the institution's customers. They can also be fake news aimed at harming an institution or affecting the price of shares of listed financial institutions.

Artificial intelligence can be used in both attacks and defences, and the financial industry must, in its defence activities, also focus on the new threats posed by increasingly sophisticated attack methods.

3.9.6 Information leaks

Information leaks via e-mails and USB storage media

Financial institutions handle large amounts of confidential information about customers and about the institution itself. Institutions place great trust in their own employees, and expect a high degree of integrity and confidentiality from employees who are given access to confidential information. In several inspections, Finanstilsynet has observed a lack of information classification. Furthermore, documentation that is sent out as an e-mail attachment is not subjected to controls. Nor is there adequate monitoring of the use of USB storage units. Consequently, the institutions have no knowledge of whether confidential information has gone astray, through either the intentional or the

[19] Southern and Eastern Norway Regional Health Authority: https://www.helse-sorost.no/nyheter/innbrudd-i-datasystemene-til-sykehuspartner-i-helse-sor-ost
[20] https://www.hydro.com/Document/Index?name=General%20cyber-attack%20presentation%20April%2012.pdf&id=28255

unintentional actions of employees. Finanstilsynet considers this to be an unsound practice, which places the institution or its customers at high risk of suffering adverse consequences in the form of both financial loss and loss of reputation. It also poses the risk that employees who have fallen prey to social engineering send out documentation containing information that can be exploited by fraudsters. In Finanstilsynet's opinion, financial institutions should take steps to mitigate this risk.

Personal data used as diagnostic data

On 5 November 2018, the Netherlands Ministry of Justice and Security published information on a data protection impact assessment, "DPIA Diagnostic Data In Microsoft Office 365 ProPlus"[21]. The results are described as alarming, as the assessment shows that Microsoft collects and stores personal data. In the wake of this exposure, Microsoft has pledged to take corrective[22] action. Institutions that use Microsoft products should assess this risk and potential consequences, and ensure that necessary action is taken.

3.9.7 Insider threats

Trust in and expectations of loyalty on the part of trusted employees are strong in the financial sector. Nonetheless, a financial institution cannot ignore the risk that an employee might abuse this trust. Disloyal employees are a risk, and can undermine the protection of the institution's and its customers' assets, unless employee activities are also subjected to internal control, especially in business-critical systems.

In its supervisory activities in 2018, Finanstilsynet learned of no serious fraud related to or harm caused through use of the ICT systems, in which employees or service provider personnel were involved. Yet deficient or non-existent controls may be the reason why unlawful acts are not detected. This type of act entails an extremely high risk for the perpetrator of the act, and employees are less likely to perform this type of act in areas where there is a high risk of it being discovered. Skilled employees, who are aware of vulnerabilities and lack of controls, can choose to carry out unlawful acts without being discovered, and without leaving any digital traces.

In Finanstilsynet's opinion, not enough attention is focused on this type of threat, and employee activities in the systems are inadequately monitored and assessed. Logs are usually reviewed and analysed after the fact, when suspicions against an employee eventually arise.

Finanstilsynet is aware that some institutions have established a proactive control system based on tool support designed to identify abnormal activities, including activity monitoring and log analyses. This can be seen as an important means of reducing inside threats. It will also have a preventive effect in that it significantly increases the risk of discovery.

[21] https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/
[22] https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls

This is a problematic issue for financial institutions. Maintaining a balance between controls and employees' feeling of being suspected and their fear of doing something wrong can be a challenge. Finanstilsynet wishes to point out that the right to privacy must be safeguarded and that the institution's ethical guidelines must be used as a basis to ensure that this type of control is established and executed in accordance with the established rules.

Employees as a means of cyber attack

Employees of financial institutions or service provider personnel may be exploited, voluntarily or involuntarily, in fraudsters' planning and execution of digital attacks.

Employees who collaborate with fraudsters

In Finanstilsynet's assessment, there is a growing likelihood and risk of fraudsters collaborating with and successfully planting persons inside an institution, or at its service providers. To reduce this risk, Finanstilsynet recommends that institutions follow the recommendations of the guide *Sikkerhet ved ansettelsesforhold – før, under og ved avvikling* [Security in connection with employment relationships – before, during and upon terminating such relationships][23], published by the Norwegian Police Security Service, Norwegian National Security Authority, the Norwegian Police and the Norwegian Business and Industry Security Council.

Threat situations

Employees with expanded authorisations or system administration rights, developers, management staff and other persons whom fraudsters can use to perform actions for them are also exposed to being threatened into carrying out unauthorised actions. These actions can include executing transactions, disclosing sensitive information, planting malicious code or engaging in other activities that could be detrimental to the institution or its customers. Employees who are subjected to threats have limited scope for action and experience their situation as extremely difficult.

Finanstilsynet received information at one inspection in 2018 that procedures for dealing with threat situations had been documented and that exercises had been carried out. Other institutions have not established any procedures nor conducted any risk assessments. In Finanstilsynet's view, financial institutions should establish procedures whereby employees are given clear instructions on how to behave if such a situation should arise and which actions should be taken in a variety of scenarios. These procedures should particularly target persons holding positions of potential interest to fraudsters.

[23] https://www.nsr-org.no/getfile.php/139531-1505211147/Dokumenter/NSR%20publikasjoner/Veiledninger%20og%20orienteringer/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

Negligent employees and service provider personnel

There will always be some employees who are more negligent than others, who click on e-mail links, for example, or open attachments without taking the necessary precautions. This is a group of employees who can easily fall victim to social engineering, thereby involuntarily lending the fraudster a helping hand.

Financial institutions should identify such employees and focus special attention on them in their training programme. An assessment should be carried out of employees seen to be highly negligent in relation to the tasks they carry out, and of whether there are grounds for taking action. Similar measures should be initiated with regard to service providers and their personnel, especially employees who have been given expanded access rights.

Shielding of employees and service provider personnel

Shielding employees' rights and authorities from their surroundings, both internal and external, by making the employees themselves more aware of the importance of doing so and through establishing special procedures within the institution, will be an important means of reducing the risk of serious situations arising. Financial institutions should pay special attention to their own employees and service provider personnel who are in exposed positions.

Unauthorised code in applications

Financial institutions often have a very extensive applications portfolio with a multitude of applications and a substantial amount of code. Moreover, the applications are developed and managed by a large number of operators, both internal and external. In addition, numerous changes are being made, usually on an ongoing basis. Due to flexible development methods, new products and services are also being launched at a faster rate. Third-party operators, who link their systems to banks' infrastructure through the open banking system, will further add to the host of applications.

Financial institutions and their service providers have largely established a system of change management that ensures that changes are processed, controlled, tested and approved before being released into production. In some cases, however, Finanstilsynet has pointed out that institutions do not have adequate controls to identify changes that were released into production without complying with the change procedure, i.e. unauthorised changes.

Due to deficiencies in the specification of requirements, or the failure to conduct tests in accordance with the requirements that are set, changes can result in errors. Inadequate vulnerability testing can also result in a failure to detect security flaws in code, thereby exposing the institution to cyber attacks. Finanstilsynet is aware that institutions use a variety of tools to detect vulnerabilities in code, but notes that there is little focus on detecting unauthorised code planted by developers. The inadequate review and control of code changes constitute a material risk, as unauthorised code is hardly likely to be discovered unless appropriate procedures and tool support are established. Unauthorised code can be a

ticking bomb that is triggered at the worst moment, or code that continuously generates unauthorised transactions without being discovered.

Although the probability of this type of criminal activity is considered to be low, Finanstilsynet believes that greater attention should be paid to this risk. Financial institutions should make sure that testing environments, both internal and external, establish and conduct independent code reviews in new systems and in changes in existing systems, with a view to detecting malicious code, planted by their own developers or by their service providers' developers.

3.9.8 Loss of business-critical data

Ransomware, an attack method whereby hackers succeed in encrypting data in an institution's data systems, can cause irreparable damage if the data cannot be regenerated from backup. Even in cases where the data are only lost for short periods of time, the institution can suffer serious consequences. Ransomware that spreads through systems from within (self-propagating ransomware) can cause the institution's operations to shut down. In the event of such a serious incident, the challenges will primarily lie in identifying the data that are affected and the consequences that this has caused and will cause. Institutions with highly complex platforms, networks and systems will face particularly massive difficulties if struck by an attack in several places. This type of incident will be extremely labour-intensive and time-consuming, and will monopolise extensive resources in the institution and its business partners for a long period of time.

In a recent survey on business continuity management and disaster recovery systems, as mentioned in 3.3.3, Finanstilsynet identified the percentage of banks in Norway that have established controls to reduce the risk of corrupted data being stored in backups. A small proportion of banks responded that no such controls have been established. Finanstilsynet accordingly believes the risk of a bank losing all its data to be small, but there will always be uncertainty attached to technological systems, such as the possibility that they may fail or that data may be lost due to human error. Finanstilsynet emphasises that financial institutions should secure and verify that their backup systems are set up in such a way that no unauthorised encrypted data can be stored in backups. The challenge in this type of attack is the strong likelihood that the last incremental backup will also be affected. This will be particularly critical if a full backup is carried out before steps are taken to stop the process. Finanstilsynet therefore points out the importance of institutions verifying that necessary protective measures have been established to limit the extent of damage in the event of an attack. Such measures can include segmentation between systems and the backup system, or securing file systems by ensuring that files cannot be overwritten until a backup has been made. A measure considered important by Finanstilsynet is a backup strategy that not only protects data in the event of attack, but also verifies that backup data are correct by means of thorough, periodical testing.

It is important that financial institutions are prepared for this type of attack, and that specific business continuity plans for the eventuality of cyber attacks are drawn up and implemented if an incident should occur. An overview should be prepared of critical systems, system interdependence and critical

data, as well as of the order in which systems and data should be restored. Emergency response procedures should also be established to ensure that personnel are available for long periods of time, and that they are assigned clear roles and responsibilities.

In Finanstilsynet's view, financial institutions should consider extraordinary measures designed to deal with a worst-case scenario in which critical data in databases and in ordinary backups are lost. Although the likelihood of an incident that causes the loss of all data or other technological incidents that make it impossible to restore the systems is considered small, the consequences would be fatal. It would also cause major societal problems if large financial institutions are impacted by an extraordinary incident of this kind. In the most extreme situation, manual or machine recovery of data from lists on paper may be the only recourse.

3.9.9 Hardware and firmware vulnerabilities

Vulnerabilities associated with the microprocessor

In 2018 vulnerabilities associated with microprocessors (CPUs) were detected, and in the course of the year more vulnerabilities associated with various processors were found. The vulnerabilities were named "Meltdown[24]" and "Specter[25]". By exploiting them, an attacker can access the hardware memory and hence software and the operating system. Attackers can retrieve data and log-on information from PCs, mobile devices and servers used for cloud services.

Vulnerabilities associated with hardware (firmware, Unified Extended Firmware Interface Forum, UEFI)

UEFI code is stored in a chip and hence called firmware, and is processed when the computer starts up. UEFI controls the computer's operating system. Vulnerabilities associated with UEFI make it possible for a hacker to access the operating system during the start-up phase. Security may be compromised, enabling a hacker to gain full access to the computer, and the opportunities this offers.

Exploitation of hardware and firmware vulnerabilities

It is hard for attackers to exploit CPU and UEFI vulnerabilities, but as long as these vulnerabilities exist, and given that it is difficult to establish control measures with current technology, it is important for the management of institutions to take precautions by implementing the necessary measures to monitor the work of ICT service providers.

3.9.10 ID theft

It emerges from a survey commissioned by the company NTT Security and conducted by YouGov that almost half (49 per cent) of those who took part in the survey are concerned that banking and credit

[24] Breaches the insulation between the user application and the operating system, enabling an attacker to access the memory, and thereby to access other software and the operating system. This may be log-on information and sensitive data.
[25] Breaches the insulation between different applications.

data may be misused by unauthorised persons in connection with online trading, and that seven of ten are concerned about ID theft. It also emerges that the use of few or short passwords makes it simpler for unauthorised persons to steal a digital identity. Finanstilsynet refers here to the recommendations of the Norwegian National Security Authority[26] regarding passwords, which the financial services industry would do well to make its customers aware of, in order to reduce the risk of fraud and ID theft.

3.10 Framework conditions in ICT and security

3.10.1 Supervisory practice and regulatory improvements

On 8 March 2018 the European Commission published the FinTech Action Plan[27], from which it emerges that cyber risk may shake confidence in financial stability, and that cyber attacks are a steadily increasing threat. The European supervisory authorities EBA, ESMA and EIOPA were asked to survey supervisory practice in the financial services industry in the areas of ICT security and governance.

The supervisory authorities' report[28] was submitted to the Commission in April 2019, and contains proposals for establishing a common regulatory framework for supervisory practice in EU/EEA countries to ensure sound and uniform risk management, and to stipulate minimum ICT security requirements for the EU/EEA financial services industry.

3.10.2 Security testing framework

Framework for testing digital defences

In the FinTech Action Plan, the Commission also asked for an assessment of the costs and benefits of establishing a coherent framework for testing the resilience of the digital defences of significant financial sector enterprises and infrastructures.

The report[29] refers to the fact that the enterprises' testing of their digital defences has been developed into 'best practice'. Financial sector institutions operate across national boundaries, and the report points out that differences in frameworks for testing cybersecurity can lead to unnecessary costs and greater risk. The report also points out the need for coordination at European level of regulatory frameworks, and the need to pave the way more effectively for cooperation among different jurisdictions.

A report with proposed measures was sent to the Commission in April 2019.

[26] https://www.nsm.stat.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet/
[27] https://ec.europa.eu/info/publications/180308-action-plan-fintech_en
[28] https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk
[29] https://eba.europa.eu/-/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity

An example of such a framework is the European Central Bank's Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU[30]). The framework is intended to help national authorities facilitate the efforts of financial institutions to establish programmes for testing and improving their resilience to sophisticated cyber attacks through controlled and evidence-based testing of production systems regarded as critical. The testing must simulate relevant attack techniques and scenarios as closely as possible. The purpose is to make institutions better equipped to assess their own capability for detecting, protecting themselves against and managing cyber attacks.

Achieving cyber-robustness requires a comprehensive approach that includes training and information activities for both the employees and the customers of the financial services industry. The Commission established a Digital Education Action Plan designed to increase knowledge of the use of digital systems.[31].

Threat-Led Penetration Testing

Threat-Led Penetration Testing (TLPT) consists of controlled attempts to compromise the electronic defences of an enterprise by simulating tactics, techniques and procedures that are used by real threat agents. The methodology was prepared by an expert group appointed by the G7 countries and published as the G-7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE). It addresses the financial sector in particular. The Bank of England has prepared two frameworks, STAR and CBEST. These are basically the same method, but the coordination conducted by the authorities in CBEST is omitted from STAR, so that the method is equally applicable to enterprises in all sectors.

As a rule, TLPT is conducted by external specialists. The aim is to prepare special electronic defences with the aid of intelligence acquired through penetration testing, and this requires the use of effective means of minimising enterprise risk during execution. The methods must ensure best practice in the procurement of the services forming the basis for these tests, in the distribution of roles and responsibility between the institution and the provider of TLPT services, the criteria for choice of service providers and the criteria for measuring delivery quality.

The European Central Bank's version of this framework is TIBER-EU, mentioned in point 3.10.2.1.

Framework for security testing in the financial sector

Finanstilsynet, Norges Bank and other relevant authorities will consider how such a framework should be established and utilised in Norway.

[30] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
[31] https://ecb.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

3.10.3 Security framework

Procurement competency is particularly important when it comes to selecting an outsourcing partner. This applies particularly to security requirements and how the service provider can confirm compliance with stipulated requirements.

There are several frameworks and guidelines to help smaller enterprises lacking detailed knowledge of good practice requirements. Some examples are the Center for Internet Security (CIS), the Cloud Security Alliance (CSA) which offers a framework for security in connection with cloud services, the NIST Cybersecurity Framework and ISACA's COBIT framework.

Finanstilsynet points out that even when outsourcing takes place through a collaboration of several participants, such as a banking alliance, or an outsourcing process is outsourced to a third party, it is the individual institution's responsibility to ensure that all necessary security requirements are taken into account and complied with.

3.10.4 SWIFT's security programme

In 2017 SWIFT established the SWIFT Customer Security Program, in response to a serious incident in 2016[32] that affected international banks and central banks' internal systems for executing SWIFT transactions. In 2018, SWIFT users were required to implement 16 mandatory security controls. In addition there are 11 non-mandatory controls, some of which will probably become mandatory in 2019. SWIFT users must conduct an annual self-evaluation and self-attest their compliance with the mandatory requirements. SWIFT has developed a know-your-customer (KYC) tool for assessing SWIFT users, and has expanded the framework[33], which will come into force at the end of 2019. Finanstilsynet will request that self-evaluations be submitted at audits.

3.11 Institutions' ICT governance models and lines of defence

3.11.1 Governance model

An institution's documented governance model, including policies, strategies, standards, guidelines and instructions, must support regulatory requirements and the institution's own defined requirements. This framework provides the institution with the first line guidelines necessary to ensure that processes implemented are established with the necessary governance. The framework also provides the basis for second- and third-line assessments of the institution's risk management and internal control, including assessment of the institution's compliance with its own framework.

Finanstilsynet observes that institutions largely establish and manage their frameworks well, but some lack procedures for management approval of documents forming part of the framework. The

[32] https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
[33] https://www.swift.com/myswift/customer-security-programme-csp/security-controls

employees' access to the documentation may also be a challenge, and there are cases where governance documentation is neither well enough known nor operationalised.

Finanstilsynet is of the view that the board and management must take further steps to ensure that an institution's framework is subject to sound development, implementation, operationalisation and administrative procedures. Management must also see to the establishment of controls that provide the board and management with confirmation that the framework requirements are complied with. Inadequate confirmation controls constitute a risk that the conditions for compliance are not fulfilled.

3.11.2 The institution's three lines of ICT defence

High quality in an institution's three lines of defence – operational management, risk management and compliance, and internal audit – are 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, all functions in the defence lines must be independent of the areas and units they control. The defence lines must report directly to 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 defence line 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 risk management 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 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. 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 detecting situations that imply high risk.

Given the increased rate of change, both technological and in the threat picture, it is particularly important that board and management regularly assess whether lines of defence are correctly organised, with the right roles, responsibilities and competencies, and have sufficient resources.

It is not usual for small institutions to have their own, dedicated resources in the three lines of ICT defence. As a rule, the second-line role of compliance does not 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 internal audit is usually outsourced. Finanstilsynet urges institutions that do not possess sufficient expertise themselves to use external resources. This will also help to detect any serious and unknown vulnerabilities.

Finanstilsynet notes through its supervisory activities that the roles and responsibilities of the first and second lines of defence are not always clearly defined. This applies in particular in the spheres of risk management and information security. Unclear roles weaken an institution's control functions and increase the risk of the institution's governance not being appropriately assessed. Finanstilsynet stresses the importance of institutions clearly defining the roles and responsibilities of the first and second lines of defence.

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.

Finanstilsynet points out the importance of an institution's internal audit unit having adequate expertise and understanding of risk, and the board's responsibility for ensuring that the internal audit unit has the necessary expertise and resources to play its part in pace with changes in the risk picture.

Finanstilsynet will assess the ICT governance of institutions through its supervisory work, and in so doing may detect vulnerabilities that may constitute a risk. Finanstilsynet may also point out areas where improvements might reduce an institution's risk. Transparency and good cooperation are important for enabling Finanstilsynet to form a correct picture of institutions' risk and control situation.

3.12 Risk management in the area of ICT

Finanstilsynet has observed that several enterprises face challenges in establishing satisfactory risk management. One of the challenges is inadequate support in the form of tools to simplify registration of risk, thereby facilitating effective management and follow-up. At the same time, Finanstilsynet notes that institutions are working to improve their processes, including by using better tools.

The actual process of identifying risk should take a central place in an institution's risk management. Finanstilsynet notes that the risk identification process, including procedures, rules and methods, is often inadequate or absent. There is also a lack of clear rules for who is authorised to accept a risk or decide that steps should be taken to mitigate a risk. Finanstilsynet's impression is that in many cases risk identification only involves the IT management. This is a practice that may mean that important risks are not identified and reported, for example by IT operational personnel, or personnel from the business side. Cooperation between the IT department and the business side is important for establishing a comprehensive understanding of risk in the institution. Finanstilsynet believes that the business side should to a greater extent include in its risk assessment vulnerabilities associated with the use, operation and administration of systems that are critical to business operations, and should do so in cooperation with the IT department.

Risk identification, and understanding what an ICT risk is, or perceiving that a situation constitutes a risk, requires raising awareness through information and training of all relevant employees. Weaknesses in the risk identification process will constitute a risk per se.

3.13 The ICT skills situation in Norway

Finanstilsynet notes that it is difficult for financial institutions and their Norwegian ICT service providers to meet their needs for ICT skills. This is probably one important reason why institutions outsource their internal ICT services more than previously, and ICT service providers choose to outsource some or all of their tasks to operators outside Norway, or to establish their own operations outside Norway. There are also examples of institutions choosing to insource the ICT services, but at the same time to establish departments abroad for the services. The rapid digital transformation points to the struggle for resources becoming tougher still. Finanstilsynet believes this may lead to increased dependence on foreign operators in the years ahead.

Government measures

In 2014 the Norwegian Ministry of Local Government and Modernisation conducted a survey from which it emerged that the need for sophisticated ICT expertise will increase, and that there will probably be a considerably greater need in the period up to 2030. It was estimated that in the period from 2010 to 2020 the need would increase from 31 000 to 42 500 persons, and that a good 55 000 would be needed in 2030. The results of the survey are published in the report from DAMWAD[34], which also points out the negative consequences this may lead to in Norway. In an article in March 2018, Digi.no writes that Norway currently lacks 2 000 persons with ICT and data security skills. The Norwegian Committee on Skill Needs points to similar challenges in its report[35] (NOU 2019: 2) of February 2019.

The Ministry of Justice and Public Security has collaborated with the Ministry of Education and Research on a National Cyber Security Strategy for Norway[36], dated 30 January 2019. The purpose of the strategy is to "develop skills in keeping with the needs of society, working life and the individual". In its long-term plan for research and higher education 2019–2028[37], the government has also defined specific aims: "Strengthen competitiveness and innovativeness, meet major societal challenges and develop communities of academic excellence".

Collaboration between the financial services industry, educational institutions and the technology industry

In 2017 DNB, Norway's largest bank, signed a heads of agreement with the Norwegian University of Science and Technology (NTNU), the aim of which was to cooperate in areas such as cyber security and digital business models in international banking and finance. In 2018 DNB, partnering NTNU, funded three new doctorates and a post-doctoral fellowship in the areas of Big Data and artificial intelligence, including machine learning.

Certification programmes from the technology industry will enable employees or others without the necessary formal qualifications to be trained for important tasks in operations and security or other relevant areas. Training programmes can target employees or others who have developed good basic skills in the use of technology, like generation Z[38], and who do not have the necessary formal qualifications. An example of this is the special programme for training IT scientists established by DNB[39].

34 https://www.regjeringen.no/globalassets/upload/kmd/aif/dokumenter/dimensjonering_avansert_ikt_kompetanse.pdf?id=2260119
35 https://www.regjeringen.no/no/dokumenter/nou-2019-2/id2627309/
36 https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf
37 https://www.regjeringen.no/no/dokumenter/meld.-st.-4-20182019/id2614131/sec1
38 https://en.wikipedia.org/wiki/Generation_Z
39 https://en.wikipedia.org/wiki/Data_science

Short- and long-term impact analysis

The financial services industry should consider the potential consequences of inadequate skills in both the short and the long term, particularly with a view to being independent of foreign operators. This should be considered in light of changed geopolitical factors, as described below.

3.14 Geopolitical factors

The geopolitical situation is more tense than it has been for many years, and may cause situations that the financial services industry has to take into consideration. In its report "Sikkerhetsfaglige anbefalinger ved tjenesteutsetting" [Security recommendations in connection with outsourcing][40] the Norwegian National Security Authority (NSM) sets out security recommendations relating to outsourcing to other countries.

Dependence on critical ICT services from abroad

Given the current complex infrastructure, both technological and operational, and dependence on several global operators, serious crises or disasters, including war, sabotage, acts of terrorism and cyber attacks that affect global operators who deliver critical ICT services to the financial services industry could present major challenges to the maintenance of critical societal services. This will particularly be the case, in the view of Finanstilsynet, if operational personnel in other countries are cut off from performing their tasks.

Emergency response personnel in Norway

Finanstilsynet notes that several of the institutions that use operators abroad to perform critical ICT services believe that emergency response personnel in Norway or in other countries will be able to take over and perform central ICT tasks if a critical situation should arise. However, there is uncertainty regarding the extent to which institutions will be able to maintain the running of critical services over an extended period if the personnel of foreign operators are unable to perform their tasks. There is similar uncertainty concerning administration, including management of serious failures that may mean a need for close cooperation with several service providers involved. If necessary, Finanstilsynet will require that such an emergency response function be established.

The consequences of dependence on foreign operators

Finanstilsynet is of the view that ICT skills that are no longer managed and developed in Norway, and growing dependence on foreign operators may constitute a substantial risk. It is difficult, today, to foresee the full consequences of this trend, not least in light of the geopolitical situation.

Institutions and their service providers should conduct regular impact analyses, with scenarios that include the consequences of ICT services supplied by operators abroad not being available for a long period. 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.

[40] https://www.nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_enkelstsider.pdf

It is important that the boards of institutions take geopolitical uncertainty into account in their risk assessments and decision-making processes.

3.15 Developments in financial technology

Developments in financial technology are related to both new and existing services provided by institutions. Institutions focus continuously on simplifying their ICT solutions. At the same time, the complexity of the overall technical infrastructure is growing, causing a risk that is increasing with the rising number of operators, use of new technology and technology in new areas as well as a continued high rate of change.

3.15.1 Development aims

Finanstilsynet believes it is important for the board and management of an institution also to maintain a critical eye on which stakeholders create expectations and a need for faster and more extensive digital transformation, both within the institution and by external actors. If decisions are based on the wrong premises, it may cause institutions to establish strategies and change processes that lead them into costly and unsuccessful organisational and technological change projects.

The institutions are faced with the demanding task of maintaining a balance between encouraging new thinking and innovation, and having sufficient insight into and understanding of the work of identifying and defining new and realistic business models through digital transformation. Finanstilsynet regards it as important that thorough analyses be conducted in an early phase of change and development projects in order to detect factors that constitute a risk that projects cannot be carried out according to plan, or factors that mean they cannot be realised at all.

3.15.2 Open banking

There is a current trend for third parties to establish services between banks and bank customers. Integration takes place through banks' application programming interfaces (APIs), by means of which third parties access banking data and services. Through open banking, banks will be able to offer their customers access to the services of other banks, while customers will be able to elect to establish relationships with more than one bank. All banking services can be accessed from one and the same user interface, from either a bank or a third party. Open banking is expected to give bank customers access to a wide range of products and services across banks, nationally and internationally within the EEA.

Where there is regulated access to the banks' infrastructure, under PSD 2, the regulatory requirements are stringent, and banks are responsible for building adequate security, in relation both to third parties and to bank customers who use third-party solutions as part of their banking services. The requirements that apply to operators who supply services between banks and their customers are

regulated by authorisation requirements. The authorities, including Finanstilsynet, also maintain a strong focus on the risk of money laundering and financing of terrorism through new channels.

It is assumed that the attack surface will change, in that criminal activities will also target third-party operators. Attacks may take place through the exploitation of vulnerabilities in third party applications, and bank customers may be more exposed to social engineering. The banks' challenge is first and foremost to ensure that the security requirements in the new ecosystem are understood, both by the individual third party and by customers who use third-party systems.

Finanstilsynet also stresses the importance of compliance with security requirements, including the PSD 2 and GDPR requirements, in order to reduce the risk of serious incidents. Inadequate compliance and control will mean increased risk of financial loss and loss of reputation. It is also important for banks to establish good control procedures, including carrying out regular penetration testing, in order to detect vulnerabilities in the bank's own APIs. Transaction monitoring, as mentioned in 3.3.6, will be an important means of detecting abnormal patterns in transactions received from third parties. This monitoring will also be capable of detecting cyber attacks on a third-party operator. Finanstilsynet stresses the importance of institutions establishing procedures for stopping transactions of a suspicious nature and for blocking transactions from third-party operators that have been affected by an attack.

3.15.3 Blockchain

In the 2017 Risk and Vulnerability Analysis, Finanstilsynet wrote that a typical feature of technological changes, such as blockchain technology, is that it tends to take longer than expected before it is put into use, and that the consequences are often greater than anticipated. Activity to assess the potential and opportunities offered by this technology appears to be declining slightly in the financial services industry, but it is still important for institutions to remain abreast of developments and potential applications for new technology.

3.15.4 Artificial intelligence

Rapid technological developments and possibilities for collecting and processing large volumes of data, both structured and unstructured, open up new vistas. The use of artificial intelligence (AI) has the potential to change the current business models in the financial services industry. It is therefore important for institutions to establish an understanding of the technology, how it can be used, and the risks involved.

Institutions that use AI should establish a governance model that lays down essential guidelines for this use. This model should include strategic choices, roles and responsibilities, skill requirements, use of data sources etc. A governance model should be rooted in and approved by the board and management of the institution. The use of technology that is not underpinned by a clear governance model could entail risk of failed investments and serious faults in business processes, and might be in breach of the personal privacy regulations designed to protect the institution's customers.

3.16 Technical debt

The traditional bank model, in which banks largely compete amongst themselves with the same range of services, has been changing in recent years. Rapid technological development has paved the way for new business models and brought increased automation.

The challenge for many institutions and their service providers is the technical debt that has been building up for several decades. Functionality to meet business side needs has been built at the expense of the management of technological architecture. The use of customised rather than off-the-shelf solutions has also resulted in strong dependence on service providers or on individuals for the work of managing older systems. Finanstilsynet notes that the situation places restrictions on institutions' ambitions for rapid, efficient development of new services.

Finanstilsynet has been informed that both institutions and service providers spend considerable resources on the work of upgrading their infrastructure and establishing services on new technological platforms. This is work that is very demanding, extensive and costly. It also presents challenges in terms of maintaining expertise in the management and development of old systems. Finanstilsynet is of the view that it is important for the board and management of institutions to be aware of the challenges and risks this entails.

3.17 Protection of personal data

New personal privacy regulations entered into force in Norway on 1 July 2018.

Personal data are to be treated in a manner that safeguards integrity, confidentiality and availability. All institutions that process personal data are responsible for doing so in accordance with the personal data legislation. Institutions are responsible for implementing measures against unintentional or illegal destruction, loss of or changes in personal data. It is important to stress that institutions are responsible both for the actual processing of personal data and for being able to demonstrate and substantiate that this processing is not illegal.

The personal data regulations stipulate requirements regarding the protection of personal data. Institutions should incorporate deletion procedures in all specialised information and support systems. There must also be manual deletion of personal data that are stored locally or in shared areas ("unstructured data"). System solutions for logging unauthorised use of information systems and a reliable access control system applying to both employees and service providers should be in place.

With regard to communication with customers, it is important that institutions pay particular attention to unintentional sending of personal data through outgoing mail, both digital and physical.

3.18 Banks' cash services

In 2018, Finanstilsynet was tasked by the Ministry of Finance with conducting two surveys, on cash services in Norway, including deposit and withdrawal services, and on how banks comply with the requirements of section 16.4 of the Financial Institutions Act, which stipulates that "Banks shall in accordance with customers' expectations and needs receive cash from customers and make deposits available to customers in the form of cash. The Ministry of Finance may make regulations on banks' obligation to receive cash from and to make cash available to customers."

Finanstilsynet concluded from the surveys that the sum total of ATMs, deposit automats, cash withdrawals in shops, post-in-shop outlets and the various systems for paying bills will cover the day-to-day needs of most customers, but point out that there is a risk that the cash services offered may be reduced going forward. There is a need to clarify banks' responsibility to provide appropriate cash services throughout Norway, like their responsibility for meeting demand for cash in a situation where the electronic payment system fails. On 17 April 2017, the Ministry of Finance stipulated in section 16-7 of the Financial Institutions Regulations that: "Banks must have solutions for meeting any increased demand for cash in the event of failure of the electronic payment systems". Banks were ordered to meet these requirements by 1 January 2019[41].

Finanstilsynet believes there is a need for more detailed rules for basic bank services, with respect to both geographical distribution and the services that must be offered, and points out that in order to achieve effective, rational solutions, cash services should largely be based on shared systems; see Financial Markets Report 2019.

In light of Finanstilsynet's surveys and recommendations, Bits has initiated a project to investigate opportunities and future solutions for cash services in Norway.

Vipps is planning to establish a Bank-in-Shop system based on the BankAxept card scheme for depositing and withdrawing cash[42]. Banks taking part in the card scheme can enter into an agreement on the system. DNB has announced that they will discontinue their Post-in-Shop banking service and replace it with the new Vipps solution. Vipps is planning to start the service in 2020 in Kiwi and Meny supermarkets throughout Norway and in some Spar and Joker supermarkets.

3.19 Joint efforts by the financial services industry

The financial sector cooperates on technological solutions in a number of areas, particularly security and common infrastructure, services and standards.

In order to improve emergency preparedness in the electronic card payments systems, Bits has taken the initiative to increase the capacity of the card terminal back-up system.

[41] https://www.regjeringen.no/no/dokumenter/meld.-st.-24-20182019/id2642702/sec1
[42] https://www.dnbnyheter.no/nyheter/dnb-gar-for-ny-losning-for-kontanttjenester-i-2020/

In 2017, a proposal was presented for a new shared payments infrastructure with faster settlement[43] which would pave the way for continuous processing of real-time payments (BRO payments). The BRO payment solution was intended to replace the existing instant payment solution in the course of 2019.

In 2018, seven Nordic banks, including DNB, launched a project (P27)[44] to establish a Nordic payment infrastructure with systems for national and cross-border payments in several currencies (SEK, DKK, NOK and EUR) to facilitate cross-border payments and promote trade among the Nordic countries. Finance Norway and Bits and other Norwegian banks were involved. The development of the BRO payment system was put on hold as a result of the P27 project.

In autumn 2018 it was decided, independently of the P27 plans, to initiate a project for the rapid establishment of a better real time solution (Straks 2.0) than the existing instant payment solution, and with real-time settlement. In March 2019 it was learned that DNB was withdrawing from further participation in P27. Finance Norway and Bits also discontinued further participation in the P27 project, and the Executive Board of Finance Norway decided that the financial services industry will further develop the Norwegian payment infrastructure.

The public sector and financial services industry have continued their collaboration on digitalising and improving the efficiency of important societal processes through DSOP[45]. Participants in the cooperation are the Norwegian Tax Administration, the Norwegian Labour and Welfare Administration (NAV), the Brønnøysund Register Centre and the police, in the areas of:

- **consent-based loan applications** – obtaining of information from the public sector
- **control information** – exchange of control information between banks and the tax administration, the police and the Norwegian Labour and Welfare Organisation (NAV) in connection with criminal investigations
- **bankruptcy processing** – instant digital notification to banks for account blocking
- **settlements after deaths** – simplified process after deaths
- **formation of companies** – simplified process in connection with formation of companies
- **NAV sickness and disability data** – simplified, more efficient process between insurance companies and NAV
- **automated authentication of right of signature and power of attorney** – overview of who has right of signature or power of attorney for a particular entity

[43] https://www.bits.no/wp-content/uploads/2017/04/Sluttrapport-BRO.pdf
[44] https://www.project27.info/
[45] Public-public/private sector collaboration on digitalisation, https://www.bits.no/project/dsop/

- **updating of actuarial calculations** – simplified reporting of salaries to pension funds and the Tax Administration

The system of consent-based loan applications has been adopted by more than a hundred banks. In November 2018, the control data system was released into production. A pilot bankruptcy processing solution was launched in February 2019, and the system for sickness and disability data from NAV was launched as a pilot in April 2019.

There has been and will continue to be considerable cooperation within the financial services industry under the auspices of Bits in connection with institutions' efforts to adapt to PSD 2[46], which entered into force in Norway on 1 April 2019. The focus of the work has gradually narrowed to the establishment of common standards and formats for the interfaces of account providers, where Bits has elected to follow the Berlin Group's[47] initiatives.

Another important joint effort is Bits' work to establish a single international standard, ISO 20022, for file-based exchange of financial messages covering the whole value chain from customer to bank, bank to bank and bank to customer.

[46] https://www.bits.no/project/psd2-xs2a/
[47] https://www.berlin-group.org/psd2-access-to-bank-accounts

4 Institutions' and service providers' assessment of risk factors

4.1 Interviews with institutions and service providers

4.1.1 Social engineering

The institutions and service providers state clearly that social engineering constitutes a strong risk. With the emergence of social media, personal information is now shared to a greater extent than previously. Institutions and service providers believe attackers may use this information to establish attacks geared to the individual profile. For example, a (false) e-mail may look as though it comes from a good friend. The e-mail may well contain information that further confirms this. In this case, the customers themselves become the weak link, as they open and answer the e-mail. The attacker may then gain unauthorised accesses and misuse them, for example by distributing sensitive data to unauthorised persons.

4.1.2 Fraud through the use of the BankIDs of close relations

According to the institutions, misuse of entry into agreements through digital signing (BankID) is on the increase, particularly among close relations. Closely related persons may have access to one another's BankID, and persons who are not computer-literate are helped to sign. This is challenging for institutions to deal with. One institution reports that claims for compensation as a result of family fraud have been filed against the institution. Finanstilsynet stresses the customer's responsibility to ensure that information used as identification for signing and logging on by means of BankID does not go astray.

4.1.3 Pressure to deliver, security and regulations

Many institutions also report pressure to deliver as a substantial security risk. Market demands for innovation and frequent publications may present a challenge to code quality. Pressure on margins and new competitors challenge the relationship between speed and change on the one hand, and security on the other. In addition, customer-friendliness may pose a challenge to security because of the requirement of user-friendly solutions in a complex competitive picture.

The institutions state that adapting to regulations such as GDPR and Finanstilsynet's guidelines result in increased IT costs, money which could otherwise have been spent on greater security, accessibility

and innovation. They also mention that the simultaneous implementation of different regulations, such as eIDAS, PSD 2, GDPR and ISO 20022, presents a challenge.

Insurance operators mention that GDPR requirements are complicated to implement, as there is no public sector coordination of the use of test data, and institutions have interfaces with many external registers.

4.1.4 Complexity of system portfolios

Institutions state that in general their system portfolios are increasingly complex. This is attributable both to changes in payment systems due to PSD 2, which covers more operators than previously, and to the fact that the institutions' own upgrade software makes it particularly problematic in the transitional phase when new and old sets of systems have to be operational in parallel. This results in an increased exposure surface, longer delivery chains and potential fragmentation of responsibilities. Ownership and the overview of applications and detailed knowledge are also deficient. Some institutions report development projects that have failed, and that constitute a major risk for the institution because it will not be possible to comply with regulatory requirements by the deadlines that have been set.

The institutions report that over the years they have accumulated large volumes of unstructured data, i.e. data that are not stored and indexed in databases, but that are stored in the form of e-mails, private documents and in social media. There is great risk associated with the volume and contents of unstructured data because it can be very difficult for institutions to comply with the GDPR requirements.

4.1.5 Complex supply chains

Institutions report that many providers are involved in the production of a financial service. This creates vulnerability, because services are dependent on many links functioning optimally. They report challenges regarding access to BankID services and services from telecom operators relating to personal identification and signing of contracts.

Extensive outsourcing coupled with growing use of cloud services creates operational complexity with increased vulnerability. Secure exchange of data between systems, services and operation service providers thus becomes essential. Lines of communication and infrastructure, both internal and in relation to service providers, are a major challenge and are associated with high risk. There is a strong risk of errors or deficiencies in configurations and their control and management. New systems provide new access routes and technically different ways of accessing systems. In a worst case scenario, institutions believe this can result in errors and downtime.

4.1.6 Relocation of operations sites

A number of institutions report moving their operations site and changing service providers, and the technical challenges this entailed. Institutions report that extensive and abstruse legal, compliance and security requirements complicate the work of making strategic decisions on outsourcing. New legal requirements may be unclear, and there is little documentation on their interpretation. This means that there is great risk associated with long-term strategic decisions.

A central agenda-setter in the industry is of the view that financial services should not be moved into the cloud, but should (continue to) be operated in mountain caverns in Norway. The operating sites for cloud operations consist of “surface facilities”, and are vulnerable to an organised attack.

4.1.7 Digital attacks

There appears to be broad agreement among institutions that there are potential attackers today with the resources to disable payment services in Norway, and also to prevent any attempt to re-establish the services. In the event, Norway would be without payment services for an extended period. The institutions have limited plans and possibilities for providing payment services if such a situation should arise. The institutions that were asked point out that it is a government responsibility to draw up plans for such a situation.

The minor daily attacks are satisfactorily handled, and on the whole do limited damage.

4.1.8 Expertise

The institutions report challenges associated with the supply of relevant and new skills and difficulty in recruiting developers, architects, project/test management and expertise in security, compliance and risk. Some institutions believe there may be a shortage of expertise in the programming language Cobol in the offing. This may impact innovation, error correction and operations support. Experienced experts on the cloud are also in short supply.

A new national strategy for ICT security focuses on the shortage of cryptologists. Some institutions felt that cross-disciplinary business skills are equally important for handling encryption systems.

4.2 Questionnaire on vulnerability

In December 2018, as in previous years, Finanstilsynet conducted a questionnaire survey. Seventeen enterprises responded to the survey. Finanstilsynet asked the institutions to rate themselves with respect to their vulnerability to potential threats. The results appear in the tables below. On balance, institutions’ risk assessment appears to show a slight rise in 2018, as it did in 2017 and 2016.

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 going forward, i.e. as increasing, stable or decreasing. The trend expressed in the far right column of the tables 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 regarded as decreasing (the interval –0.2 to –1).

The size of the institutions is not reflected in the tables.

4.2.1 Support for strategic decisions

Table 6: Support for strategic decisions

	Vulnerability	The institutions' responses	Trend 2018	Trend 2017
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 enterprise's risk for the purpose of management and reporting to 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 enterprise employees and suppliers, so that we can consider writing these off as losses.		→	→
3	The ability of the systems to reflect customers' ability to repay debt.		→	→
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 prevalence of and faults and deficiencies in systems		→	↘
	Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed.			

Source: Finanstilsynet

There is little change from 2017 to 2018. It is worth noting that institutions believe that the risk associated with poor data quality is falling. This may be attributable to institutions putting extensive work into classifying and deleting data in connection with the EU General Data Protection Regulation (GDPR).

4.2.2 Data protection

Table 7: Data are not adequately protected

	Vulnerability	The institutions' responses	Trend 2018	Trend 2017
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, applications, software		→	→
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, the supplier must document that data have been completely deleted?		→	→
7	Unstructured data (i.e. data that users themselves evaluate the need 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.			

Source: Finanstilsynet

Institutions' risk associated with data protection looks roughly the same as in 2017. Finanstilsynet notes that risk associated with the protection of unstructured data is falling, and assumes this to be attributable to the classification and deletion of unstructured data in accordance with the GDPR.

4.2.3 Operations

Table 8: Operations

	Vulnerability	The institutions' responses	Trend 2018	Trend 2017
1	Organisation, procedures, job description, reporting and controls		→	↘
2	Agreements with suppliers 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 for ensuring stable operations		→	→
7	Logs and our ability to react to the contents of the logs		→	↘
8	"Ticking bombs", i.e. components that gradually wear out, or assets that gradually reach levels requiring intervention without our noticing it, 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 in data traffic (abnormal load, abnormal ports / protocols, irregular response times) in the operating pattern 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 suppliers		→	→
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 suppliers and to monitor deliveries		→	↗
15	The extent 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		→	→
	Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed.			

Source: Finanstilsynet

Finanstilsynet notes that the risk associated with deficiencies in organisation, job descriptions, reporting and control has moved from a falling to a stable trend. This may be due to the more complicated provider situation reported by the institutions, with many service providers in the same value chain. It is also probably partly attributable to the complexity of IT systems, which is regarded in 2018, as in 2017, as increasing.

Finanstilsynet also notes that the risk associated with pressure on deliveries is still growing as a result of extensive changes and new regulatory requirements.

4.2.4 ID theft

Table 9: ID theft

	Vulnerability	The institutions' responses	Trend 2018	Trend 2017
1	An attacker takes over a user ID uses it fraudulently		→	→
2	Controls on the issue and use of login IDs and passwords to customers and employees (BankID, employee ID, system users, admin users)		→	→
3	Controls that prevent skimming and card-not-present fraud		→	→
	Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed.			

Source: Finanstilsynet

The risk of an attacker taking over a user ID and misusing it is regarded by institutions as somewhat less in 2018 than in 2017. This may be because the institutions appear to have introduced better controls on the assignment of user IDs and passwords to customers and employees.

4.2.5 Internal fraud

Table 10: Misuse of access to IT systems

	Vulnerability	The institutions' responses	Trend 2018	Trend 2017
1	Access control		→	→
2	Our policy on segregation of duties		→	→
3	Logging and alerts		→	→
4	Analysis of "suspicious" transactions such as retroactive value dating, movements in internal accounts, transfers from customer to employee and back		→	→
5	Monitoring of employees' own-account trading		→	→
	Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed.			

Source: Finanstilsynet

Assessments of the risk associated with internal fraud underwent little change from 2017 to 2018.

4.2.6 Money laundering

Table 11: Money laundering

	Vulnerability	The institutions' responses	Trend 2018	Trend 2017
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.			

Source: Finanstilsynet

The risk of money laundering appears to have diminished as a result of improvements in the ability of IT systems to gather relevant information about customers, customer relations and customer behaviour.

This may be because the risk associated with inadequate market surveillance is exhibiting a downward trend.

4.3 National assessments of the threat picture

The *Annual Threat Assessment* for 2019 published by the Norwegian Police Security Service (PST), *Fokus 2019* from the military intelligence service and *Helhetlig IKT-risikobilde 2018* [Overall ICT risk picture 2016] from the Norwegian National Security Authority (NSM) show an increase in the last couple of years in attempted industrial espionage against financial sector institutions designed to obtain technological and financial information about Norwegian businesses.

The steadily growing threat from foreign intelligence services with extensive expertise and resources is cause for concern. One of the threats consists of efforts to recruit and control clandestine sources in Norwegian businesses. Operations are also conducted for the purpose of obtaining sensitive information and influencing decision-making processes. This applies widely: in Norwegian politics, in the administration, defence and emergency response sector, in critical infrastructure and in research and development.

Studies of both the infrastructure and vulnerabilities of networks can therefore be conducted by foreign states through computer network operations that are cheap, effective and constantly evolving. The digital assets of Norwegian businesses are based largely on cloud technology, and all communications and archiving are electronic. Valuable processes and business secrets often exist only in digital form, and are therefore vulnerable and must be protected.

Gathering of information on individuals normally takes place in advance of such computer network operations, such as their e-mail addresses, user profiles on social media or in cloud services, and their role in an organisation.

The Russian intelligence service is currently regarded as the greatest challenge, but countries such as China could also conduct intelligence operations against Norwegian targets and businesses. Successful operations could inflict great damage on Norway. The goal of Russian influence operations is to undermine political processes and increase polarisation in Europe and NATO.

Financial institutions should be aware of the global threat picture when they consider outsourcing services. Businesses may have less control over increasingly complex value chains, lose internal expertise and become dependent on external service providers in order to be able to provide their services.

5 Risk areas

5.1 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 infrastructure is designed to ensure that cash payments and transactions in financial instruments are registered, cleared and settled.

So far, cyber vulnerability has not led to any systemic crises, but there have been serious failures, and vulnerabilities have been detected. A digital collapse may occur suddenly and will have far-reaching social consequences. In addition to its own infrastructure, the financial sector is dependent on shared infrastructure such as power supply and telecommunications, including networks.

Failures suffered by key financial industry operators or occurring in shared infrastructure may have substantial societal consequences. If payments cannot be made or settled, important societal functions will no longer function satisfactorily after a short while. Sensitive information that goes astray or breach 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 compromise them or make them unavailable, this could create considerable challenges for customers and institutions, and could also impact financial stability. The societal effects could be particularly great if institutions that operate on behalf of all or several institutions are affected. The institutions' work on robust operational systems, including business continuity systems, contingency preparedness and crisis management systems, recovery plans and ICT security work, constitutes an essential part of the efforts to ensure financial stability.

There are currently several means of payment for consumers and institutions, which makes parts of the payment system less vulnerable. In 2018, requirements were also stipulated for contingency arrangements for cash [48].

[48] The obligation of banks to make contingency arrangements for cash provision in order to meet any increased demand for cash in the event of failure of the electronic payment systems is set out in regulations issued by the Ministry of Finance.
https://www.regjeringen.no/no/aktuelt/nye-krav-til-bankenes-kontantberedskap/id2598131/

Cooperation on supervision and surveillance of financial infrastructure in Norway

A robust financial infrastructure is crucial to financial stability. In its work of supervising ICT, Finanstilsynet will focus particular attention on vulnerabilities that may result in serious failure or major disruptions in the financial infrastructure and constitute a threat to financial stability.

Areas to which weight is attached in inspections are the institutions' ICT governance and security work, including measures to counteract cybercrime, the robustness of their operations and emergency planning systems and their management of change and control of access rights.

Finanstilsynet and Norges Bank have developed their cooperation on supervision and surveillance of Norway's financial infrastructure over a period of years. It includes regular meetings and cooperation on risk assessment and joint inspections.

Finanstilsynet's and Norges Bank's responsibilities for supervision and surveillance of Norway's financial infrastructure overlap to some extent. Finanstilsynet is responsible for supervising the VPS register function and securities settlement, while Norges Bank is responsible for monitoring the same functions. Finanstilsynet is responsible for supervising Norwegian banks and their payment systems. Norges Bank is responsible for supervising interbank systems in Norway. Interbank and settlement systems that are offered by banks are generally part of the banks' ordinary operating systems. Observations and feedback from Finanstilsynet's ICT inspections of these banks will thus provide important information that may be of benefit to Norges Bank in its oversight of the interbank systems.

Finanstilsynet can attend in the capacity of observer the supervisory and surveillance meetings that Norges Bank has with financial market infrastructures (FMIs), and Norges Bank can attend as an observer Finanstilsynet's inspections of banks and data centres of importance to financial infrastructure.

Through its supervisory activities and the work of the Contingency Committee for Financial Infrastructure, Finanstilsynet obtains a good, broad picture of the state of the Norwegian financial infrastructure. In 2018 there was a payment systems incident that was assessed as critical, when duplicated entries from the Norwegian Interbank Clearing System (NICS) were sent for settlement in Norges Bank.

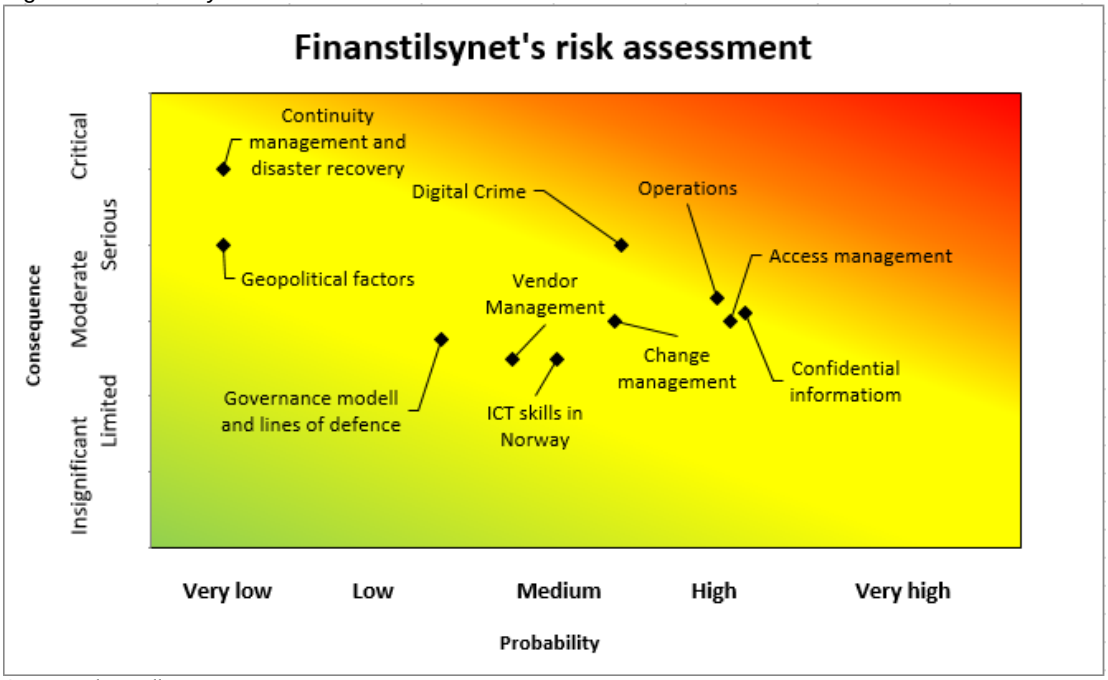
The reliability of clearing and settlement systems and communication with SWIFT, the international payment system, and CLS, the international settlement system, were also good in 2018.

Finanstilsynet regards the Norwegian financial infrastructure as robust, despite a critical incident that caused a failure in the payment system and incidents that made payment systems unavailable in periods.

5.2 The institutions

Figure 6 shows Finanstilsynet's assessment of the most central threats to 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 seriousness of the consequences for the individual institution. The basis for placement in the matrix of the various risk areas, including vulnerabilities with the probability of consequences, is described below.

Figure 6: Finanstilsynet's risk assessment



Source: Finanstilsynet

Finanstilsynet considers risk associated with vulnerability in institutions' operations, access management, business continuity management and disaster recovery systems, confidential information and defences against cybercrime, to be the most serious threats emanating from institutions' use of ICT. All these are assessed as having medium to high risk. Vulnerabilities associated with institutions' service provider management, change management, governance model and lines of defence in connection with ICT activities, and vulnerabilities associated with geopolitical factors and ICT expertise in Norway, are also threats associated with the institutions' use of ICT. These are assessed as having medium risk.

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.

Operations

The institutions' services are based on digital solutions. Vulnerabilities ensuing from an institution's operating solutions not being sufficiently robust constitute a risk of unavailable and /or unstable services.

A critical service is not robust when a deficiency in one component makes the service unavailable because components of the service's ecosystem (networks, servers, software, power supply, premises etc.) are not duplicated through redundant systems, or the business continuity system has deficiencies that cause it not to function as intended.

The integration of different service providers increases the risk of operating problems, partly because the service involves several systems that may fail and thereby make the service unavailable, and partly because multiple 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 creates operational complexity with increased vulnerability. The pressure exerted by extensive changes on providers' service provision system increases the risk of errors occurring.

The technical debt in the institutions' systems entails complex integrations and adjustments between new and old systems, and because of architectural weaknesses, this, too, constitutes a risk of operational problems. A limited supply of expertise in the management and operation of mainframe systems presents challenges for operations support. Institutions' lack of experience in the use of cloud technology constitutes a risk of error in the configuration and securing of data.

Finanstilsynet assesses the overall risk associated with vulnerabilities in ***operations*** as ***medium*** to ***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 impaired data quality as a consequence of complex integration among service providers is assessed as *medium* and the consequences as *moderate*.
- The probability of unstable and / or unavailable services as a result of increased integration among different service providers is assessed as *medium* and the consequences as *serious.*
- The probability of operating problems that impact shared operational infrastructure 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* 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 operating problems (networks and services) as a result of invalid digital certificates or invalid licences is assessed as *medium* and the consequences as *moderate*.
- The probability of operating problems as a result of deficient expertise in operating support for mainframes is assessed as *medium* and the consequences as *moderate*.

Digital crime

Vulnerabilities associated with institutions' management, defences and ability to respond, which includes assigning roles and responsibilities, security frameworks, training, contract regulations and interaction with service providers, testing, surveillance or technical security measures, constitute a risk of potential harm to the institution and its customers through cybercrime.

Finanstilsynet notes that the methods used by criminals have changed from previous years, when attacks largely consisted of implanting malware or disrupting services through DDoS attacks. The methods now used are more complex, with combinations of different kinds of social manipulation to establish a digital foothold on the inside of the institution's network, sophisticated techniques for concealing one's presence in the network, and a thorough study from the inside before launching the actual attack.

Finanstilsynet assesses the overall risk associated with vulnerability to ***digital crime*** as ***medium*** to ***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 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 employees being used involuntarily, through threats, as an instrument for a digital attack is assessed as *low* and the consequences as *serious.*
- The probability of service providers' employees being used involuntarily, through threats, as an instrument for a digital attack is assessed as *low* and the consequences as *moderate*.

- The probability of disloyal employees in the institution or in service providers' development community planting malicious code malware in critical business applications 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 *low* to *moderate*, and the consequences as *critical*.
- The probability of criminals succeeding in exploiting vulnerabilities in hardware (CPU) or firmware (UEFI), to attack a financial institution is assessed as *low* and the consequences as *moderate*.
- The probability of an institution not detecting criminals who have established a digital foothold inside the network before damage is averted as assessed as *medium* and the consequences as *critical*.
- The probability of serious security flaws not being patched 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*.

Confidential information

Trusted employees of the institutions and trusted personnel of the institutions' service providers have access to confidential information about the institutions' customers and internal affairs. Access to this information is based on background checks, work responsibilities and trust given to the individual. Finanstilsynet has found through its inspections that institutions lack systems for checking whether attempts are made to copy confidential information to mobile storage devices or to send such information as attachments to e-mails. This type of deficiency appears to be a general challenge in the financial services industry.

Finanstilsynet assesses the overall risk associated with vulnerabilities in *screening of confidential information* as *medium* to *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 confidential information going astray as a result of inadequate control of outgoing e-mails is assessed as *very high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of inadequate control of 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 inadequate control of service provider personnel is assessed as *moderate* and the consequences as *serious*.
- The probability of confidential information going astray as a result of inadequate access governance is assessed as *very high* and the consequences as *moderate*.

Access management

Vulnerabilities associated with inadequate access management represent a risk of breach of data security, including breaches of confidentiality, integrity and availability.

Through its activities in 2018, Finanstilsynet has noted that access management, as proactive control of access to systems and technical infrastructure, is a constant challenge for a number of institutions. Weaknesses in management of the access of employees and of service provider personnel with expanded access rights constitute a particular risk. Complicated, detailed lists with overviews of employee access rights and authorisation level represent a risk of misinterpretation by managers.

Finanstilsynet assesses the overall risk associated with vulnerabilities in ***access management*** as ***medium*** to ***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 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 *moderate*.
- The probability that employees or service provider personnel have administrative rights without the management being aware of it is assessed as *medium* 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* 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*.

Business continuity management and disaster recovery

Vulnerabilities in business continuity management, including disaster recovery and emergency response plans, constitute a risk if a serious incident occurs. This could be a matter of inadequate training and exercises, or inadequate testing of the institution's emergency response plan. Inadequate evaluation of tests results in risk of the institution and its service providers not being sufficiently prepared, and thus not capable of handling a crisis.

Inadequate analyses of the commercial consequences of a crisis represent a risk of the disaster recovery system not being established with the necessary technical infrastructure and capacity. The absence of requirements regarding restoration of operations (recovery time objective – RTO) and regarding how much data can be lost (recovery point objective – RPO) are also factors that constitute a risk of the system not being correctly designed. Failure to perform security updates of disaster recovery plans increases the risk of cyber attacks when the institution is in a particularly vulnerable situation.

Finanstilsynet notes that institutions have largely established disaster recovery systems, also referred to as emergency response systems or backup systems, that are to be implemented if normal operating systems are not available. However, a number of deficiencies have been detected that may present institutions with challenges when dealing with a serious ICT incident. This applies to deficiencies in

governing documents, instruction, training, exercises and testing of disaster recovery systems. Institutions should focus more attention on business continuity management and disaster recovery systems, to reduce the risk of serious incidents causing extensive damage.

Finanstilsynet regards the probability of a serious incident that requires implementation of the disaster recovery plan as *very low*. If the plan does not function as intended, the consequences are regarded as *critical*.

Finanstilsynet assesses the overall risk associated with vulnerabilities in ***business continuity management and disaster recovery*** as ***medium*** to ***high***. This is based on the following assessments:

- The probability of the institution's disaster recovery plan 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 plan has to be implemented.
- 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 incident 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 institution and service provider is assessed as *medium* and the consequences as *serious*.
- The probability of the disaster recovery system not functioning as expected owing to deficient technical tests and deficient evaluation of these tests is assessed as *medium* and the consequences as *critical*.
- The probability of deficient security updates of the disaster recovery plan is assessed as *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 in the incident of cyber attacks and inadequate training and exercises is assessed as *very high* and the consequences as *critical*.

Vendor management

Vulnerabilities due to inadequate or the absence of service provider monitoring, administrative and operational, constitute a risk of breach of compliance with agreed requirements and breach of the rules in the ICT Regulations. This also constitutes a risk of the service provider not having established adequate internal control, which in turn exposes outsourced services to breaches of data security. It may also imply a risk that serious financial problems or shortage of resources on the part of the service provider, which may threaten the service provider's ability to deliver, are not discovered. Lack of

clarity regarding the roles and responsibilities of institution and service provider and among service providers in the value chain constitute a risk of serious incidents not being resolved in time.

Undesirable dependence on service providers may arise through weaknesses in service provider management, when the provisions of the agreement for transfer of a service to another provider are not sufficiently binding. There is then a risk of prolonged instability during the process of transferring the service to another service provider, particularly when the transfer takes place as a result of the service provider being unable to meet the delivery requirements.

The main challenge for small institutions is to secure adequate procurement competencies in order to ensure that all relevant requirements are included in the agreement with the service provider when the service is established, and that the institution has employees who are qualified to monitor the service provider. As a rule, large institutions and alliances have established requirements to provide guidelines for service provider management through agreements and cooperation models. The challenge is the complexity and volume of the services, and the quantity of service providers, with vendors.

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 *limited*. 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*.
- 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 operational 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 *moderate*.
- 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 (for example, 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 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 with an independent audit report is assessed as *medium* and the consequences as *moderate*.

Change management

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 higher change rate and more rapid development of new systems are all factors that increase the risk of vulnerabilities being introduced in connection with changes in IT systems as a consequence of overly weak governance.

In 2018, Finanstilsynet noted challenges associated with institutions' change management. Incident reports to Finanstilsynet reveal that serious incidents occurred in connection with changes, both functional and non-functional.

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with ***change management*** as ***medium***. 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 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 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*.

Governance model and lines of defence

Vulnerabilities in an institution's governance model, which consists of policies, strategies, standards and guidelines, constitute a risk of the institution's risk management and internal control not being established in accordance with the institution's risk profile.

Vulnerabilities in an institution's three lines of defence constitute a risk of irregularities in the implementation of the governance model's requirements, and of monitoring and control failing to detect serious weaknesses in the institution's governance.

Finanstilsynet notes deficiencies in the administration of governing documents, in that some documents have not been formally approved or updated. In some cases the requirements in the

governing documents have not been implemented and operationalised. There are also cases where the roles and responsibilities of the first and second lines of defence have not been clearly defined.

Finanstilsynet assesses the overall risk associated with vulnerabilities in the ***institution's governance model*** and ***lines of defence*** as *low* to *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 rules not being detected as a result of inadequate supervision by an institution's operational management is regarded as *low* and the consequences as *serious*.
- The probability of important requirements in governing documents not being implemented and operationalised 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 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 inadequate or the absence of risk identification processes is assessed as *medium* and the consequences as *moderate*.
- The probability of serious weaknesses in internal control not being detected by 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*.

ICT skills in Norway

Vulnerabilities resulting from inadequate access to expertise in operations, architecture, technology, development and development methodology, and ICT security and inadequate skills management constitute a risk for operations. Inadequate skills may also lead to the institution using the wrong technology and/or not seeing the possibilities inherent in new technology.

Vulnerabilities attributable to an inadequate supply of ICT skills in Norway, and the fact that too few ICT engineers are being trained, constitute a risk of increased dependence on foreign operators. If operators are prevented from carrying out the tasks necessary to maintain secure, stable operations, there may be serious consequences for the financial services industry.

Finanstilsynet notes that access to ICT expertise and resources in Norway is a challenge for the financial services industry and its service providers. The current competitive situation in Norway is not regarded as critical, but vulnerability may be exacerbated in the years ahead as a result of limited training capacity and growing demand. In time, outsourcing of ICT services to other countries may lead to loss of expertise in these areas in Norway.

At present, Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with ***ICT skills in Norway*** as ***medium*****.** The probability of adverse incidents occurring or adverse incidents

not being adequately managed as a consequence of a lack of skills in Norway is regarded as *medium* and the consequences as *limited*. This is based on the following assessments:

- 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 regarded as *medium* and the consequences as *moderate*.
- The probability of interrupted operations and service unavailability as a result of insufficient skills is assessed as *low* and the consequences as *moderate*.
- The probability of breaches of data security as a result of an inadequate supply of security skills is assessed as *low* and the consequences as *moderate*.
- The probability of institutions' inadequate skills in services developed and operated by service providers resulting in breaches of laws and rules is regarded as *medium* and the consequences as *moderate*.

Geopolitical factors

There is growing dependence in the financial industry on ICT skills and services from abroad. This is a dependence that may create considerable challenges for some sectors of the financial services industry if serious situations arise that prevent foreign operators from continuing to supply critical ICT services. Geopolitical tendencies with increased unrest and uncertainty are factors that constitute a risk that foreign operators may be affected.

In light of national and international threat assessments, Finanstilsynet believes that these are factors that institutions must take into account in order to ensure that critical ICT services delivered by foreign operators that are affected can be taken over by other operators in Norway or abroad within the time necessary to maintain secure and stable operations.

Finanstilsynet assesses the overall risk associated with vulnerabilities in relation to foreign operators who deliver critical ICT services to the financial services industry in Norway as ***medium*** at present. The probability of undesirable incidents, when foreign service providers are cut off from delivering their services, is assessed as *very low* and the consequences as *serious*.

5.3 The institutions' customers

Log-on information gone astray and misuse of BankID

The increased digitisation has led to the institutions' customers having to use digital identification and authentication systems. This makes customers vulnerable, and constitutes a substantial risk of misuse, at worst with major financial consequences for the affected party.

Passwords and PIN codes may be difficult for some to remember, and a customer may choose to write down this information. There is then a risk of the information falling into the hands of unauthorised persons and of the customer being defrauded. Closely related persons may have access to one

another's digital ID and authorisation codes, and persons who are not computer-literate may turn over their digital signature to others to carry out their financial transactions.

BankID has a very wide area of application. In consequence, there is a concentration risk associated with misuse of BankID, as the misuse may arise in many areas, such as entry into purchase contracts, subscribing to insurance, tax information, loan agreements, etc. There has been an increase in the number of loan agreements entered into through misuse of the digital signature (BankID) of others, particularly by persons who are closely related to the person being defrauded. The police single out three main areas where BankID is used for fraud, including misuse by close relations.[49]

Identity theft

According to a new survey (2019) conducted by the Norwegian Centre for Information Security (NorSIS), more than 150 000 Norwegians aged over 18 have experienced misuse of their own identity during the last two years. The usual form of misuse is purchases of goods and services online (28 per cent), or fraudsters taking up loans or being given credit (17 per cent). The actual theft may take place through fraudsters stealing passports or bank cards that are sent by post. According to NorSIS, only 38 per cent of the victims of ID theft report it to the police. See also 3.9.10.

Social engineering

Love scams, where criminals establish a relationship with their victim over a long period before initiating the actual fraud, is a psychological game that traps the victim in an emotional relationship that it is difficult to escape from. Customers are also subjected to invoice fraud, investment fraud and other forms of financial fraud.

The situation is often experienced as highly fraught by the victim and those close to them. Finanstilsynet is aware that banks take the initiative in relation to customers if they suspect that a customer is the subject 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 engineering and fraud lie behind the cash transfers. As this type of fraud is a growing problem, Finanstilsynet urges institutions to continue to work to find effective measures in relation to the various customer groups.

Customer interface through new operators

Through open banking, including PSD 2, users will find that new non-bank operators will offer solutions whereby customers can access their accounts. Finanstilsynet is of the view that the banks and the new operators should accept joint responsibility for ensuring that customers are educated and informed about the new regulatory requirements, and what they entail.

[49] https://www.nettavisen.no/økonomi/politiet-dette-er-de-vanligste-bankid-svindlene/3423676674.html

Institutions' integrity as a result of cybercrime

Cybercrime creates uncertainty among users of an institution's services that will be heightened by serious incidents. Finanstilsynet has been contacted by customers who are afraid their funds will be lost as a result of cybercrime. This is a concern that the institutions need to take seriously.

6 Finanstilsynet's monitoring activities

6.1 Key areas for Finanstilsynet's ICT supervision

Supervisory activities are risk-based. Finanstilsynet will be focusing on the supervisory units that have the greatest influence on financial stability and smoothly functioning markets. Institutions' ICT risk will be assessed, and the institutions' own annual assessments of ICT risk will be reviewed. Emphasis will be placed on monitoring the organisation of ICT/cyber security work, the security of institutions' ICT systems and the organising of surveillance. This includes 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 will place emphasis on checking that institutions have procedures in place for ensuring that data extracts to anti-money-laundering systems are complete.

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

Supervisory activities will 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.

6.2 Work with payment systems

The EU revised Payment Services Directive (PSD 2) has been transposed into Norwegian legislation and will form the basis for Finanstilsynet's follow-up of financial institutions' payment services. Institutions will be monitored with respect to their compliance with the new regulations relating to payment service systems[50], risk related to payment services and compliance with the duty to report.

Collaboration with Norges Bank will continue.

[50] Regulations relating to payment service systems (Norwegian text)

6.3 Follow-up of incidents

Follow-up of incidents is a prioritised area. Finanstilsynet will closely monitor developments in 2019, and emphasis will be placed on identifying causes and taking steps to prevent recurrence. Incidents involving serious irregularities will be monitored for the entire life of the incident, and if needed follow-up meetings will be held. Special measures will be considered.

6.4 Contingency preparedness

The work of the Contingency Committee for Financial infrastructure (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 2019 as well, and measures linked to findings from previous exercises will be followed up.

Finanstilsynet will also participate in relevant contingency preparedness work initiated by other sectors and cooperation within the national regulatory framework for managing cyber security incidents.

Finanstilsynet will align its contingency work and management of cyber security incidents with the framework of the National Security Authority (NSM) for handling cyber security incidents[51]. The Ministry of Finance has appointed Finanstilsynet as sectoral response group (SRM) in the sphere of financial markets, and Finanstilsynet will exercise its role in collaboration with Nordic Financial CERT according to agreed information exchange rules. On the basis of NSM's framework, work is in progress to formalise cooperation between Finanstilsynet and Nordic Financial CERT in order to establish a sectoral response group for the part of the financial market sector supervised by Finanstilsynet.

6.5 Monitoring of the cybercrime threat picture

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

- the cybercrime threat picture
- contingency preparedness work targeting digital vulnerability and security
- how institutions organise and monitor their security work
- changes in payment services due to the use of new technology (fintech)
- cross-border activities

[51] https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

6.6 Consumer protection

Finanstilsynet will stress the importance of institutions making thorough provision for their customers' security. It will also monitor that institutions do not share their customers' data without consent, and that data does not fall into the hands of unauthorised third parties.

Finanstilsynet will check that institutions establish solutions in compliance with the regulations, and that the solutions launched have functionality that is in line with customer 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.

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

Finanstilsynet will check that banks discharge their responsibilities with respect to compliance with the provisions of the Financial Institutions Act[52] regarding the provision of cash. Finanstilsynet will also check that banks have established solutions in line with the provisions of the Regulations on supervision of financial institutions regarding the meeting of increased demand for cash in a crisis situation[53].

[52] https://www.finanstilsynet.no/globalassets/laws-and-regulations/laws/financial-institutions-act-2015.pdf
[53] https://lovdata.no/dokument/SF/forskrift/2016-12-09-1502/KAPITTEL_16#KAPITTEL_16
[Regulations on supervision of financial institutions]

7 Finanstilsynet's monitoring activities

Term/ abbreviation	Meaning
3D Secure	3D Secure is an XML-based protocol used in online payments. It provides an extra layer of security to card transactions by authenticating the user to the card issuer, irrespective of the payee. In connection with use of Visa, which developed the protocol, it is called Verified by Visa.
AISP	Account Information Service Provider. Operators that can obtain information from bank accounts on behalf of a customer
API	Application Programming Interface. Interface in a program that allows specific parts of this program to be run from another program.
AML	Anti-Money Laundering
BFI	Contingency Committee for Financial Infrastructure. Chaired by Finanstilsynet.
Blockchain	List of data/transactions, called blocks, that are linked together into a chain and secured by means of encryption
Check-out system	Solution with several integrated payment options, e.g. card, invoice and part payment
CLS	Continuous Linked Settlement. International settlement system for foreign exchange transactions
COBIT	IT governance framework for developing, organising and implementing sound, secure data management strategies
COBOL	COBOL is a programming language designed for commercial use. Mainframes are computers chiefly used by large organisations for their critical applications for processing large quantities/volumes of data.
CRM	Customer-relationship management. System for managing relations with existing and potential customers

Data centre	A dedicated area, or one or more buildings containing IT systems and appurtenant components such as telecommunications and data storage systems
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
EBA	European Banking Authority
ECB	European Central Bank
EIDAS	Electronic IDentification, Authentication and trust Services. A set of standards for electronic identification and trust services for electronic transactions in the European internal market
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
Fake news	Information resembling news with incorrect, deficient or misleading content or with a false originator that somebody deliberately creates and disseminates through various news channels and social media
Fintech	Financial technology
FMI	Financial Market Infrastructures. FMI is a collective term for financial market infrastructure institutions such as interbank systems, securities settlement systems, central counterparties, securities depositories, trade repositories etc.
GDPR	General Data Protection Regulation
ICT	Information and communications technology
ICT Regulations	"Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)" (Norwegian title)
ISACA	Information Systems Audit and Control Association
ISAE 3402 Type II	Insurance standard. Assurance reports on controls at a service organisation
ISO 20022	Financial services – universal financial industry message scheme
Contingency arrangements for cash	Banks' obligation to accept and make cash available to customers. This obligation is not limited to normal situations, but may be even more important in a crisis situation
Business continuity plan	A plan describing the alternative procedures a business must follow when a critical situation arises
Ransomware	A type of malware that restricts access to infected ICT systems and demands a ransom for removing the restrictions

Machine learning (ML)	Development of algorithms that enable computers to learn from empirical data and develop behaviour
Down-time	The time when a computer, service, application etc. is not functioning
NICS	Norwegian Interbank Clearing System
Nordic Financial CERT	Nordic Financial CERT is an organisation established by Nordic financial institutions to collaborate on identifying and combating cyber attacks targeting the financial industry in the Nordic countries; see www.nfcert.org.
Open banking	Open banking is an institution's open APIs (interfaces) which enable a third party to build systems that exchange information between the third party's and the institution's systems.
Above-ground facility	Data centre not established in a mountain cavern or underground
Phishing	Impersonating another and in this guise seeking information from a person. This is an attempt to exploit the person's trust in the original sender.
PISP	Payment Initiation Service Providers. Means whereby operators can initiate payments on behalf of customers
PSD 2	Revised Payment Services Directive 2015/36/EU
Audit declaration	Self-declaration that auditing of the governance system is carried out both internally and externally if the institution has an external service provider.
RPO	Recovery Point Objective
RTO	Recovery Time Objective
Cloud computing services	Cloud-based platform, infrastructure, software or storage services. Distributed computing via a network. Possibility of running software on a large number of networked servers. Cloud computing may be both private and public sector, or a combination of the two.
SRM	Sector response team Must have an overview of own sector, be an information node for all relevant activities and be the sector's contact point with NSM NorCERT.
Strong customer authentication	Transaction authentication employing two-factor authentication or more, e.g. pin code + password
SSD	Solid state drives. Electronic, flash memory-based storage unit
SWIFT	Society for Worldwide Interbank Financial Telecommunications.
Trojans	Software that presents itself as useful but in reality is harmful

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

Tel. +47 22 93 98 00
Fax +47 22 63 02 26
post@finanstilsynet.no
finanstilsynet.no

06.2019