FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

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

RISK AND VULNERABILITY ANALYSIS
2017

Risk and Vulnerability Analysis (ROS) 2017

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

Finanstilsynet, Cut-off date: 7 May 2018

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. Through its supervisory activities, Finanstilsynet maintains a broad network of contacts with financial institutions, industry associations, service providers, standardisation bodies and national and international authorities.

The purpose of the report is to describe risks and vulnerability relating to financial stability, individual institutions and individual consumers.

Chapter 2 summarises the risks inherent in the financial sector's use of ICT and payment services.

Chapter 3 presents an overview of Finanstilsynet's findings, observations and lessons learned in its supervisory activities in 2017. Technology trends considered to be of potential significance for financial institutions' use of ICT are described.

Chapter 4 reports on the financial institutions' own assessments. Furthermore, a number of key service providers and security system providers have been interviewed, and current assessments of the risk picture of relevance to the financial industry are cited.

Chapter 5 presents Finanstilsynet's overall assessment of the risk picture in 2017 based on findings, observations and trends. The assessment highlights the most important threats and vulnerabilities that could potentially be so detrimental to financial institutions' systems that they could jeopardise the goals of financial stability and smoothly functioning markets.

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

The Norwegian financial infrastructure is essentially robust. There were no ICT incidents that had consequences for financial stability in 2017. However, financial institutions' customers experienced a number of serious incidents that resulted in the reduced availability and loss of services.

Finanstilsynet has identified vulnerabilities that constitute a risk of the occurrence of serious incidents. In light of this risk, Finanstilsynet considers that institutions should strengthen their efforts to improve ICT security and to establish sufficiently robust systems. Vendor management poses a challenge for institutions, and there is a need to improve collaboration between institutions and service providers.

The high rate of change and complex value chains involving a steadily growing number of operators is a challenge to institutions' efforts to maintain good governance. The shortage of qualified personnel in the fields of security, architecture and new technology also poses a challenge.

Technological advances have a major impact on the development of financial sector services. New regulatory changes open the door for new operators and new systems that challenge established institutions and business models.

2.1 Finanstilsynet's findings and observations

Through its follow-up of reported incidents, inspection findings and other supervisory activities targeting the financial industry, Finanstilsynet obtains a thorough insight into financial institutions' use of ICT, payment systems and relevant areas of risk.

2.1.1 Areas of supervision

Payment systems

Finanstilsynet observed a number of serious incidents, in terms of both scope and duration, that affected payment systems in 2017. In some of the incidents, payment systems were unavailable to more than 30 per cent of the bank's customers for up to 24 hours. The

incidents created market uncertainty about the institutions' ability to ensure the continuous provision of payment services and execution of payment orders, and showed that in the case of certain types of payment card, no back-up systems have been established.

The payment service area continued to undergo major changes in 2017, including the establishment of a special payment institution for collaboration on Vipps, and the phasing out of MobilePay and mCASH.

In 2017, several institutions and their service providers worked to adapt their activities, both organisationally and technically, to meet the requirements of the new Payment Services Directive (PSD 2).

Finanstilsynet observed a decline in payment card fraud for the first time since registration of such fraud commenced in 2010. The number of fraudulently used cards fell by 5 per cent, while total losses were 30 per cent lower in 2017 than in 2016. It is assumed that the decline is the result of the more stringent security requirements set by payment card issuers, including strong cardholder authentication when the payment card is used, which has been an effective instrument. Online fraud also declined compared with 2016.

In Finanstilsynet's opinion, institutions should improve their management and control of the risk related to and vulnerability of payment systems.

Banks

Continual changes in the threat of digital attacks are a risk that poses a growing challenge to banks' efforts to establish risk-mitigating measures. Finanstilsynet sees a need for banks to improve their work in the field of ICT security. This applies, for instance, to the organisation of the work, performance of risk analyses of both their own infrastructure and outsourced ICT infrastructure, updating of security frameworks and proactive measures to strengthen the institutions' defences. Management and control of privileged access rights must be improved.

Finanstilsynet has noted an improvement in banks' preparation of business impact analyses as a basis for meeting requirements for business continuity and disaster recovery plans. However, incidents show that further improvements are still necessary.

Securities

A number of regulatory amendments led to a need for changes in institutions' ICT systems. The system changes gave rise to incidents and revealed weaknesses in the institutions' ICT systems, including their testing systems. In connection with the launch of a new product, the Share Savings Account, some institutions established systems that lacked the requisite functionality.

Many institutions need to improve their documentation of guidelines, procedures and plans for conducting security tests.

Insurance

In Finanstilsynet's experience, most insurance undertakings have good risk management systems, but there are also undertakings where the situation is not satisfactory.

The use of new technology in connection with new insurance products places greater demands on both use and control of collected data and necessitates risk assessments that identify relevant risk. This applies, for instance, to the use of sensor technology and monitoring of customer behaviour.

2.1.2 Incidents

The number of incidents rose by around 25 per cent from 2016 to 2017, and the availability of payment services and customer-facing solutions was reduced. Of the 190 incidents reported, only ten of the reports concerned intentional security incidents (cybercrime). The remaining 180 were notifications of operational incidents.

The most serious incidents were caused by faults in management systems which in turn caused the malfunctioning of duplicate systems intended to ensure continuity in the event of service interruptions. This affected both banks and payment services, and in some cases also insurance undertakings. These incidents showed that a failure of key management mechanisms designed to ensure redundancy and continuity in institutions' operating systems can have major consequences.

There were also a number of incidents involving BankID, which in a number of cases affected all Bank ID users. Several of the incidents occurred on days with exceptionally high traffic, revealing the service's capacity problems.

2.1.3 Outsourcing notifications

Finanstilsynet received close to 50 notifications of outsourcing of ICT services in 2017. Most of the notifications concerned outsourcing to major global cloud service providers or changes of subcontractors. Finanstilsynet has noted a steady increase in the number of subcontractors for outsourced ICT services.

In some cases, risk assessments that should serve as the basis for board decisions regarding outsourcing are inadequate.

When reviewing outsourcing agreements, Finanstilsynet has only occasionally seen a failure to comply with the requirements of the ICT Regulations regarding the right of audit and the supervisory authorities' right of inspection. In Finanstilsynet's opinion, provisions regulating

the transfer of a service from one service provider to another (exit provisions) are often not sufficiently specific.

2.1.4 ICT and information security

Cybercrime is a growing threat. Digital attacks can affect several dimensions, and it may be difficult to determine the purpose of the attack. Despite the significant rise in undesirable activity targeting institutions, only a minority of such attacks result in a security incident.

In 2017, Finanstilsynet registered organisational, operational and technical weaknesses that constitute vulnerabilities to intentional attacks and unintentional errors. Efforts to ensure ICT security must be improved and responsibility for this work must be clearly assigned in the organisation. Responsibility for managing ICT security, monitoring ICT security and for operational ICT security activities must be clearly segregated.

Finanstilsynet considers security testing carried out by qualified external personnel to be an important tool for detecting vulnerabilities in an institution's infrastructure and electronic defence system.

Another important risk-reducing measure is the institutions' preventive efforts to raise employee awareness of the different methods employed by criminals. Such methods include social engineering[1] of employees to appropriate information such as user identities and passwords, e-mails with a false sender address to deceive employees into performing unauthorised actions, and links in e-mails sent by criminals for the purpose of emplacing malicious code. Finanstilsynet notes that institutions are actively engaged in these preventive efforts.

2.1.5 Developments in financial technology

Financial technology (FinTech) advances have been made in both newly established and existing financial institution services. Technology for an institution's follow-up of and compliance with regulatory frameworks (RegTech) has also been adopted in the form of systems to promote more efficient, automated supervisory processes for both the institutions and the supervisory authorities.

Artificial intelligence and robotisation are now used by institutions to rationalise and simplify processes. Institutions are also assessing the potential of blockchain technology.

[1] Social engineering exploits human interaction and social skills to acquire or influence information (https://nettvett.no/)

2.2 Financial institutions' assessments

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

- system faults and weakened stability as a result of the increased scope and frequency of changes in institutions' systems
- data attacks, including more sophisticated and more easily available attack methods and tools
- inadequate in-house ICT expertise and capacity
- inadequate management and control of accesses for the protection of data and systems
- leakage of confidential data
- BankID that fails to function or does not function satisfactorily
- reduced possibility of securing services end-to-end in connection with outsourcing
- outsourced services that do not meet institutions' security requirements and statutory and regulatory requirements

Market expectations regarding new, simpler systems constitute a risk in the form of low system quality, since insufficient time is allocated for testing, particularly of capacity and response time. Other areas of threat cited by the institutions are the degree of complexity of IT systems, new regulatory requirements necessitating system changes, and losses arising from unauthorised use of card data in connection with online or telephone shopping (Card Not Present). Some institutions point to the risk of their systems not being of high enough precision to identify suspicious transactions or data of high enough quality to satisfy the "Know Your Customer" requirement. Another risk cited is insufficient use of information possessed by institutions to implement risk-mitigating measures.

2.3 Current areas of risk

Financial infrastructure

On the whole, Finanstilsynet considers Norway's financial infrastructure to be robust. Stability was somewhat poorer in 2017 than in 2016 and 2015, but better than in 2014. Incidents that impact shared infrastructure, providers of services to many institutions or to a single large institutions may have significant consequences.

Financial institutions

Finanstilsynet considers risks related to vulnerabilities in financial institutions' operating systems, access management, change management and cybercrime defences to be the primary threats. Vulnerabilities related to vendor management, disaster recovery and contingency planning solutions and expertise are also key risks.

Consumers

Traces left by the use of digital services can be used for fraudulent purposes by service providers. Should they fall into the hands of unauthorised persons, there is a significant risk that they will be used for criminal gain.

Due to increased digitisation, bank customers, who for various reasons do not themselves use the bank's digital services, find themselves obliged to let family members or other persons whom they trust have access to their digital signatures to use digital services. Finanstilsynet considers the potential for identity misuse to be a risk, especially when the customer's login to an online bank is carried out by the trusted person.

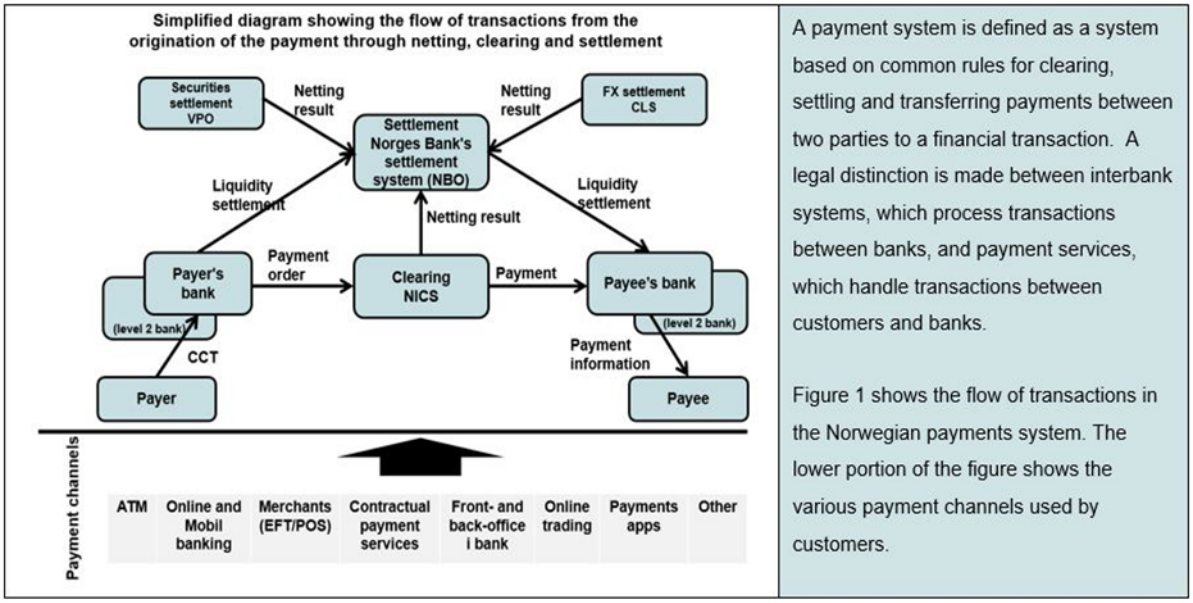
3 Finanstilsynet's findings and assessments

This chapter presents assessments based on Finanstilsynet's work with ICT and payment services in 2017, and describes observations from ICT inspections, incident reports, notifications of changes in outsourcing agreements, notifications of new payment services and changes in existing services and other supervisory activities.

Relevant regulatory frameworks and trends that in the longer terms are considered likely to be of significance for financial institutions' use of ICT, and that could give rise to changes in the risk and vulnerability situation of both institutions and consumers, are also described.

Finanstilsynet's general assessment is that there were no threats to financial stability and orderly market conditions in 2017, although certain incidents created uncertainty as to financial institutions' continuous ability to provide robust payment services and execute payment orders.

Figure 1: Flow of transactions in the Norwegian payments system



Source: Finanstilsynet

3.1 Payment systems

3.1.1 General comments regarding payment systems

Effective, robust and stable payment systems are a fundamental prerequisite for financial stability and well-functioning markets.

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)/Bits. Partly as a result of the revised Payment Services Directive (PSD 2), a number of regulatory amendments have been proposed that will affect payment systems.

3.1.2 Management and control of risk and vulnerabilities in payment systems

Good governance is crucial to ensuring robust, stable payment systems.

The scope and frequency of changes affect the risk picture. Finanstilsynet has observed the rapid rate of change, which in itself constitutes a considerable risk. The rate of change is largely influenced by increased competition spurred by customer expectations, technological advances and regulatory amendments. New operators enter the value chain, and payment

services are integrated into other services. Several financial institutions have already established application programming interfaces (APIs) which enable third-party operators to offer new services.

Financial institutions must thoroughly assess the risks related to payment services[2], with an eye both to operational risk related to service operation and maintenance and to security risk related, for example, to unauthorised use of the services. Finanstilsynet's basic rule is that comprehensive risk assessments are to be conducted prior to the launch of new payment services, especially when the payment system involves the use of new technology.

The Revised Payment Service Directive (PSD 2) sets a number of requirements for the governance of payment systems, 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.

In addition to ensuring that services and information are protected by logical and physical security measures, financial institutions must ensure a high level of quality in both operating systems and associated processes that could affect operations.

In Finanstilsynet's experience, financial institutions, particularly the large ones, invest considerable effort in their operating and contingency planning solutions in order to reduce their vulnerability to operational irregularities in payment services, among other things by establishing a larger number of alternative operating and redundant solutions for operation. However, again in 2017, Finanstilsynet has noted incidents (see 3.7.1) that demonstrate that the quality of some institutions' work in these fields is not satisfactory. Incidents in 2017 have shown that the consequences are considerable if failures occur in central control mechanisms intended to ensure redundancy and continuity in institutions' solutions for operation. Continuous surveillance, control and testing of the system components of management mechanisms must be an important part of institutions' operational tasks in order to avoid this type of incident. Finanstilsynet has also observed that services failed to function as expected due to inadequate capacity management. Capacity management is also a critical task for maintaining a continuous, stable operating situation.

The most serious incidents in 2017 caused uncertainty among customers as to financial institutions' ability to execute payment orders. As a result of one incident, some customers, such as young people with payment cards that are not covered by STIP[3], were entirely prevented from making payments.

[2] See the Norwegian regulations relating to payment service systems.
[3] A back-up system that is activated if there is no contact between the card terminal and the bank. The operations centre may authorise payment on behalf of the bank in accordance with applicable rules.

Providing customers with comprehensive information when incidents occur is important. In Finanstilsynet's experience, many institutions have established effective processes for dealing with operating system failures, including communicating information to customers and taking remedial action.

In Finanstilsynet's view, improvements are needed in several areas, such as risk-reducing measures related to key functions in operating systems and capacity management. Incidents can have significant impacts if no alternative means of payment are available. Finanstilsynet underscores the responsibility of the board of directors and executive management to ensure that the institution has procedures and systems to ensure stable operating systems and effective contingency planning solutions. This responsibility also applies to any parts of the services that are outsourced.

3.1.3 Notification regarding payment service systems

The Payment Systems Act requires that Finanstilsynet be notified without undue delay of the establishment and operation of payment services. 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 who are involved in the payment service
- a new version with a modified or new functionality of material importance for the payment service system

In 2017, Finanstilsynet received 17 notifications of new or changed payment service systems. The notifications mainly concern mobile systems and payment card systems. Notifications were also received regarding application programming interfaces with third-party service providers.

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.

3.1.4 Developments in payment services and mobile payment systems

3.1.4.1 Trends

In Norway, developments take the form of the market entry of new operators, existing 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.

In 2017, DNB entered into a partnership with several other Norwegian banks to establish the payment service provider Vipps AS[4]. The participation of other banks in this collaborative venture was made possible by establishing distribution agreements with Vipps.

At the end of 2017, a majority of Norwegian banks were participating in the Vipps partnership. As a result, the MobilePay payment system was phased out in the Norwegian market, and mCASH was wound up entirely.

Vipps is widely used in Norway for person-to-person payments and as an alternative to cash payments to groups such as clubs and associations. The services have also been expanded to applications such as e-commerce payments, in-store payments and invoice payments. Vipps, which is now the only mobile payment service in the Norwegian market, uses its own infrastructure, which means that the payee must install the same application as the payer in order for the transaction to be effected. Vipps was originally dependent on MasterCard and Visa's payment card systems, but it is now also possible to make account-to-account payments by using the fast payment infrastructure[5].

In November 2017, Vipps AS, BankAxept AS and BankID AS announced that they had entered into an agreement of intent to merge so as to be better positioned to meet international competition.

In 2017, BankAxept AS established support for contactless payment using physical cards, especially for payment of small amounts. Many merchants have previously chosen not to permit contactless payments since this technology was only available through Visa and MasterCard's international payment systems. BankAxept's system has been instrumental in increasing the use of contactless payments. In the course of 2018, BankAxept will launch account-to-account payments, which can be integrated as an e-commerce payment system.

Due to the financial industry's lack of payment system standardisation and interoperability for in-store payments, Retail Norway was established in 2016 (converted into Area Payment & Identification AS (Area) in 2017). The business concept is to offer an open payment platform that accepts all types of cross-channel payments[6] (e-commerce, mobile commerce and in-store)[7].

[4] DNB, the SpareBank 1 Alliance, the Eika Alliance, Sparebanken Møre and fifteen independent savings banks established Vipps AS in 2017.
[5] https://www.bits.no/bank/straksbetalinger/
[6] BankAxept, Visa/Visa, Electron, MasterCard/Maestro, Diners, American Express, JCB, China Union Pay, Apple Pay, Samsung Pay and Android Pay, Vipps, Alipay
[7] https://rpwp.blob.core.windows.net/wpdata1/2017/10/Aera_produktark_Betaling.pdf

The trend towards use of biometrics in connection with authentication and payment continues, and several Norwegian financial institutions now use fingerprint-based identification. The Vipps app also includes a facial recognition system, which at present can only be used on one type of smart phone. A fingerprint-based[8] payment system is being tested in Denmark.

PSD 2 requires strong customer authentification and digital certificates. Buypass[9] is positioning its electronic trust services to meet the requirements of future rules and regulations, among other things, with website certificates. In 2017, BankID AS launched a new trust service with a simple login function called xID[10], as a supplement to BankID.

3.1.4.2 PSD 2 as a catalyst for new services and operators

The new Payment Services Directive that entered into force on 13 January 2018 in the EU paves the way for increased competition and the establishment of new payment services. Several EU countries have already seen these effects in the licence applications received. Finanstilsynet anticipates a similar response when PSD 2 comes into force in Norway. Through an open payment market, and the establishment of public APIs[11] based on financial institutions' infrastructure, new and existing licensed operators will be able to offer the new payment services, payment initiation[12] service and account information[13] service.

Draft amendments to the Financial Agreements Act, the Financial Institutions Act and the Payment Systems Act, which implement the provisions of PSD 2, have been circulated for consultation and are now under consideration by the Norwegian Ministry of Finance and the Ministry of Justice. Until PSD 2 enters into force in Norway, operators will not be able to offer the new payment services on the Norwegian market unless the payment account service providers, i.e. the banks, accept them. The same applies to Norwegian financial institutions that want to offer payment services in EU countries.

The new payment services can be provided both by new institutions that establish operations as payment service providers, and by existing institutions that want to offer the new services. Vipps has already gained an important foothold through its agreements with payment account providers. Institutions licenced as payment institutions have announced that they may offer new payment services when PSD 2 enters into force.

[8] https://no.ehandel.com/artikler/tester-fingerbetaling-lover-hoy-sikkerhet/435358
[9] https://www.tu.no/filer/EVENT/Digital2017_presentasjoner/Mads_Henriksveen_Buypass.pdf
[10] https://www.bankid.no/bedrift/xid/
[11] Application programming interface. Interface in software that enables specific parts of the software to be run from other software
[12] Payment Initiation Service Providers (PISP). Operators who can initiate payments on behalf of customers.
[13] Account Information Service Providers (AISP). Operators who can retrieve data from bank accounts on behalf of customers

Finanstilsynet expects more international operators to establish payment services in the Norwegian market as a result of PSD 2. Alipay, which is described as the world's largest payment system, offers a payment system for Chinese on holiday in Norway that is linked to their account in China[14]. Alipay has been authorised as a payment institution in the UK, and in October 2017 notified Norway that it was establishing cross-border operations. Other major global operators, such as Apple Pay and Google Pay, have established operations in several European countries, but have not yet been launched in Norway. Some operators, such as Swedish Tink[15], are currently establishing a position in the Nordic market in order to offer aggregates of financial data and other information.

3.1.4.3 PSD 2 – requirements regarding management and monitoring of operational and security risk

Concerns have been expressed that the changes resulting from the introduction of PSD 2 will give rise to new risks and vulnerabilities relating to payment services. However, it is important to emphasise (see 3.1.2) that upon introduction of the Directive, the same strict requirements regarding the monitoring and handling of operational and security risk related to payment service provision will apply to both new and current operators. In order to obtain a licence, new operators will have to undergo a comprehensive quality assurance process, in which stringent requirements for procedures and processes will be set for both the institution's activities and the payment services that are to be offered.

The overall operational risk in payment services is therefore not expected to increase, beyond the higher risk entailed by a larger number of operators and longer value chains. New systems based on modern technology and development methods, combined with strict licensing requirements, are expected to limit operational risk.

3.1.4.4 PSD 2 – rules governing access to payment accounts

The aim of PSD 2 is to enable the customer to access more and better services by establishing a regulatory regime that defines specific requirements (authentication and secure communication) and that enables the market to develop more and better systems that meet these requirements. Under PSD 2, licenced institutions are to have access to account information and the right to make payments on behalf of customers. The rules governing access to account information are set out in Commission Delegated Regulation (EU) 2018/389 on regulatory technical standards for strong customer authentication and common and secure open standards of communication. The standards will become effective as of 14 September 2019 within the EU. However, documentation of technical specifications and testing facilities (sections 3 and 5 of Article 30) must be made available by the account servicing payment service provider by 14 March 2019. The European Banking Authority (EBA) has initiated the establishment of a working group tasked with defining specific

[14] http://www.betal.no/nyheter/alipay-lansert-i-norge-for-kinesiske-turister_100219_100219
[15] https://www.nordea.com/no/presse-og-nyheter/nyheter-og-pressemeldinger/news-group/2017/nordea-partners-up-with-tink.html

requirements for the communications interface between licensed third-party operators and account servicing payment service providers.

PSD 2 allows licensed operators to authenticate the customer with identity attributes issued by a licensed operator, or with identity attributes already possessed by the customer. The requirements regarding IDs and authentication are set out in the standard.

Under the standard, licensed operators must authenticate themselves to the account servicing payment service provider. This can be done by means of digital certificates that qualify for the eIDAS High Assurance level.

Finanstilsynet considers the risk related to the technical development of interfaces to be limited. The technical protocols and standards required to realise the purpose are well-known and extensively used.[16]

3.1.5 Blocking online use of payment cards

Under the EBA Guidelines on the Security of Internet Payments, which entered into force on 1 August 2015, cardholders must to a greater degree be able to set limits for the use of their own payment cards. For instance, the cardholder must be able to block online use of the card. Finanstilsynet regards this type of functionality as an important means of reducing Internet fraud.

Finanstilsynet has noted that some of the major payment card issuers had still not implemented this functionality in 2017. Finanstilsynet has pointed out this deficiency and will follow up on the institutions in question.

3.1.6 Fraud and attacks on payment services

The degree to which Norwegian online banks are exposed to fraud is limited. This indicates that the level of security makes such attacks less attractive and/or that the potential return is too low. Technically simpler scenarios with elements of traditional fraud may be more tempting.

In several cases, Finanstilsynet has observed sophisticated forms of social engineering and collection of information on individuals that give fraudsters access to the victim's assets, or assets that the victim has control of in a company. The information collected is then compiled and the potential gain is assessed before the fraud attack.

[16] See, e.g. HelseID, https://www.nhn.no/helseid/

Fraudulent e-mails and telephone calls are perceived as trustworthy by bank employees or bank customers, as a result of which criminals' social engineering and fraud attacks succeed. Customers are misled into registering and authorising transactions that prove to have a different payee than the one intended by the customer. Both private and corporate customers are exposed to social engineering fraud, but in different ways.

Finanstilsynet has been informed that the banks are seeing an increase in this type of fraud, in the form of both actual losses and averted losses. It is the customer who must cover the loss if the customer has been imprudent and given fraudsters access to login information as a result of social engineering. The banks assist their customers in attempting to stop the payments and recover the funds, and to a certain extent can warn customers about the fraudulent methods used and when fraudulent attempts have been identified. Finanstilsynet has noted that some financial institutions conduct information campaigns to warn both their own employees and their customers about this type of fraud. Finanstilsynet will encourage institutions to intensify these efforts.

3.1.7 Overview of annual losses related to payment services

The tables below present statistics for losses due to payment card and online banking fraud in recent years. The figures represent total losses, irrespective of whether the loss is covered by the customer, the bank or the payment card company.

Losses in Norway related to use of cards

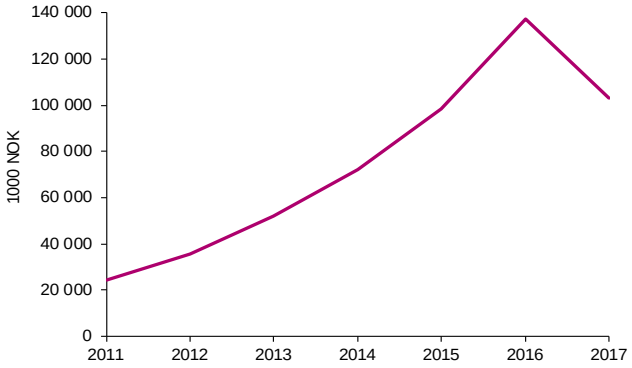
Loss statistics in 2017 show a significant decline in losses related to card-based payments. The number of fraudulently used cards decreased by 5 per cent, while overall losses related to card-based payments fell by 30 per cent. The average loss per fraudulently used card was thus substantially lower than in 2016.

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

Type of payment card fraud	2012	2013	2014	2015	2016	2017
Fraudulent use of card data, Card-Not-Present (CNP) (online transactions, etc.)	35,701	51,954	72,056	98,410	137,015	102,908
Stolen card data (including. skimming), fraudulently used with counterfeit cards in Norway	2,308	762	524	2,670	1,360	483
Stolen card data (including skimming), fraudulently used with counterfeit cards outside Norway	55,869	51,534	51,685	48,447	41,762	17,452
Original cards lost or stolen, fraudulently used with PIN in Norway	28,128	21,274	21,266	18,875	12,857	10,194
Original cards lost or stolen, fraudulently used with PIN outside Norway	8,544	9,570	13,071	14,224	10,223	9,663
Original cards lost or stolen, fraudulently used without PIN	4,603	4,949	5,510	6,033	3,286	4,891
Total	**135,153**	**140,043**	**164,113**	**188,660**	**206,503**	**145,591**

Sources: Finanstilsynet and Bits

Figure 2: Fraudulent use of card data, Card-Not-Present (CNP)



Sources: Finanstilsynet and Bits

Payment card fraud and data theft

For the first time since loss statistics were first compiled in 2010, payment card losses fell in 2017. This includes the decline in e-commerce (CNP[17]) losses, which fell by 25 per cent.

[17] Card transaction in which the card holder is not required to present the physical card at the time of payment, for example in connection with e-commerce.

Finanstilsynet believes that the lower e-commerce losses can primarily be attributed to the more stringent requirements imposed by payment card issuers, payment card acquirers and merchants with regard to strong cardholder authentication, using security protocols such as 3D Secure[18] or the like.

All cards issued in Norway have a chip. At some payment terminals (such as for the purchase of convenience goods from vending machines and payment at parking meters), payment may only be made by means of a magnetic stripe. Losses related to the fraudulent use of counterfeit cards in Norway are therefore low. Losses related to the fraudulent use of counterfeit cards are higher in countries other than Norway, however, because cards or card data stolen in Norway are used in countries where the magnetic stripe is still commonly used. Fewer and fewer countries use only the magnetic stripe, and loss statistics for 2017 show a decline of close to 60 per cent in this type of loss.

Costs related to payment card fraud

Finanstilsynet has prepared an estimate of total costs related to stolen payment card data. The calculation 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. Total direct losses are gross losses, and are covered 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.

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

Costs related to payment card fraud	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Number of cards affected by fraud	20,332	22,531	38,541	44,900	68,162	65,024
Total direct losses, see Table 1	135,153	140,043	164,113	188,660	206,503	145,591
Administrative costs for card issuer (NOK 2,250 per card)	45,747	50,695	86,717	101,025	153,365	146,304
Consumer costs (NOK 1,000 per card)	20,332	22,531	38,541	44,900	68,162	65,024
Total estimated costs	**201,232**	**213,269**	**289,371**	**334,585**	**428,030**	**356,919**

Source: Finanstilsynet

In addition to the costs presented in Table 2, there are administrative costs incurred by card acquirers, merchants and the Norwegian Financial Services Complaints Board. Furthermore, substantial resources are spent on transaction monitoring and following up on cardholders to

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

avert potential losses. The total costs related to payment card fraud are therefore considerable.

Losses related to online banking

Losses related to online banking are low and fell by almost 60 per cent in 2017. Most attempts at online banking fraud are thwarted because the transactions are aborted before execution. The banks, in collaboration with Nordic Financial CERT[19], work continuously to monitor and stop online banking fraud.

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

Type of fraud – online banking	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Attacks using malware on customer's PC or security device (Trojans)	5,064	1,327	552	3,055	2	727
Lost/stolen security device	3,367	1,285	6,655	963	8,758	1,892
Phishing and false BankID – merchants	10		539	5,815	2,428	2,057
Other/unknown	358	779	3,474	2,715	7,444	2,911
Total	**8,799**	**3,391**	**11,220**	**12,548**	**18,632**	**7,587**

Sources: Finanstilsynet and Bits

Losses related to social engineering fraud

Finanstilsynet has not compiled statistics on CEO fraud in 2017, but is aware that the banks have registered a rise in both real and averted losses. The losses have increased despite warnings and information campaigns in 2017 about CEO fraud, based on information regarding fraud scenarios in 2016.

In addition to CEO fraud, other types of fraud based on social engineering are also perpetrated, such as investment fraud and various forms of dating fraud.

The customers who are defrauded often contact the bank to ask for help in stopping the transactions and recovering the amounts paid out.

[19] Formerly FinansCERT

3.2 Banks

Finanstilsynet has identified areas in which banks should make improvements. Particular attention has been focused on ICT security, outsourcing and contingency planning. More detailed information on key findings and assessments is provided below.

3.2.1 Organisation of ICT security

Through inspections, Finanstilsynet has uncovered a need to improve the organisation of work on ICT security in banks. Due to poorly defined roles and responsibilities, important security measures may not be carried out. Clear distinctions must be made between responsibility for management of ICT security, monitoring of ICT security work and operational ICT security. Reference is made to 3.9.1.

3.2.2 Risk analyses related to ICT security

The threat picture is constantly changing, posing a continuous challenge to, and change in, the risk picture for banks. In light of this situation, banks must regularly update their risk picture and implement timely measures. Good risk analyses are crucial. However, risk analyses can also create a false sense of security if material risks are not identified and reported, and necessary action taken to address these risks.

In its supervisory activities, Finanstilsynet has noted that banks carry out risk assessments, but sees that these assessments do not adequately cover technical infrastructure that is outsourced. This applies, for instance, to risk assessments of network architecture, network quality, firewalls, the classification and protection of data, server configuration and software updates.

When reviewing risk analyses carried out by the banks' outsourcing partners (service providers), Finanstilsynet has seen that certain findings recur and/or are in the same category. This suggests that measures are not being initiated even when risks have been identified.

It is Finanstilsynet's assessment that banks must strengthen their security efforts and ensure that risks at every level of the value chain are identified, assessed and managed. Appropriate expertise and capacity are essential for attaining the level of security necessary to maintain sound operations.

3.2.3 Security frameworks and expertise

Banks' ICT infrastructure and systems undergo continuous change. New vulnerabilities are detected and others are established, partly as a result of the accelerated pace of development of new services, new technology and new operators in the value chain. Coupled with the changing risk picture, this imposes a requirement on banks and their service providers to

update their security framework, including their cyber security framework. The quality and capacity of banks' specialist communities are important factors in this work.

In Finanstilsynet's view, banks are aware of the growing and altered risk, and of the need for security expertise. At the same time, the situation poses a challenge due to the limited availability of qualified personnel. Finanstilsynet has noted banks' failure to update their security framework, for instance by not addressing changes in their risk and vulnerability situation.

3.2.4 Weaknesses in banks' defences

Banks in Norway have hitherto not been subjected to attacks resulting in serious situations. However, there is a global increase in cyber attacks, and banks are registering a rise in undesirable activity. The risk of attacks on banks, and their seriousness, is therefore expected to increase. In extreme cases, such attacks could inflict substantial losses on a bank and/or even cause the bank to fail.

Through cyber security inspections, Finanstilsynet has identified and pointed out weaknesses in banks' defences which expose the banks' systems and networks unduly to attack. Finanstilsynet has also noted the unclear distribution of responsibility and deficient procedures for software updates (patching) to mitigate known vulnerabilities.

In many cases, ICT service providers are the performing party in efforts to comply with security requirements and plug security holes. However, Finanstilsynet notes that banks face challenges in holding their service providers responsible for compliance with security requirements. Finanstilsynet emphasises the importance of security requirements being regulated in the agreement between the parties, and the financial institution's responsibility for monitoring that the service provider complies with the requirements.

3.2.5 Access management

Through inspections of banks' access management and control, Finanstilsynet has focused particular attention on personnel with extended access rights (administrative rights) who are employed by the financial institutions' service providers. This is also important when the institutions' employees have this type of extended rights.

Personnel with administrative rights or extended access rights may take advantage of their rights to unlawfully retrieve information or insert malicious code into the bank's systems. Personnel may also commit unlawful acts, intentionally or unintentionally, which destabilise operations or commit acts that render systems and services unavailable. Trace logs of actions performed can be erased by the person carrying out the actions in order to cover his tracks.

Finanstilsynet has seen that management and control of extended access rights is too weak. Findings include a lack of periodical reviews of accesses and users with access rights that exceed actual needs. Finanstilsynet has pointed out to institutions the importance of maintaining adequate control of extended access rights, also where service providers' employees are concerned, and has emphasised that extended access rights should not be granted on a permanent basis. This type of access right must be subject to effective management and control and linked to specific tasks such as an incident, a problem or a change.

It is important that banks are aware of this risk and establish necessary proactive controls to detect suspicious activity, for example through automated controls.

Special attention should be focused on access to confidential information and personal data, and access to areas such as servers, databases, system software and networks.

3.2.6 Outsourcing agreements

Finanstilsynet has reviewed outsourcing agreements in connection with outsourcing notifications and licence applications or when examining documentation received in connection with ICT inspections. This review shows that a great deal of effort is devoted to drawing up agreements with provisions intended to ensure that institutions comply with laws and regulations. The agreements reviewed show that only by way of exception is section 12 of the ICT Regulations not covered by the agreement provisions. This also applies to contracts signed with global cloud service providers.

However, Finanstilsynet has seen that financial institutions lack necessary insight into and understanding of the scope of the outsourced ICT service, as regards both the technical infrastructure used for the service and the tasks that the service provider has an obligation to perform. This applies in particular to software as a service. Finanstilsynet emphasises that financial institutions are responsible for their own ICT operations, including outsourced services (see the ICT regulations), and are expected to be able to assess and monitor outsourced services. See also 3.8.2.

3.2.7 Testing of contingency planning solutions and business impact analyses

3.2.7.1 Testing of contingency solutions

Under the ICT Regulations the contingency solutions must be tested annually. Inspections have revealed that experience from real incidents has been deemed to suffice as testing of the contingency solutions. However, it is not clear from the bank's report that the planned test was not carried out. While Finanstilsynet sees the value of experience gained by banks in

connection with real incidents, it expects banks to assess whether an actual incident provides an adequate basis for not conducting planned , and whether the incident might justify adapting the planned test. This assessment should be submitted to the Bank's board of directors.

3.2.7.2 Business impact analyses

Banks' requirements regarding business continuity and disaster recovery plans must be based on analyses of the impacts of operational disruptions on business. Established business continuity and disaster recovery plans are important steering documents when serious incidents occur, and must address both technical and organisational issues. Implementing business continuity and disaster recovery plans in the event that a situation actually arises will be a challenging process. Carefully thought-through business impact analyses and plans and testing procedures determine how effectively the bank's crisis management team, in collaboration with relevant service providers, will be able to deal with a critical situation.

Through its inspections, Finanstilsynet has registered an improvement in institutions' efforts to carry out good business impact analyses. Nevertheless, there is reason to reiterate the importance of this work and of testing contingency planning solutions. In its follow-up of incidents, Finanstilsynet has noted that institutions experience difficulties in dealing with serious operational interruptions.

3.2.8 Testing of banks' compliance with the reporting requirements of the Norwegian Banks' Guarantee Fund

In 2017, Finanstilsynet carried out inspections of banks' compliance with requirements regarding IT systems for reporting to the Norwegian Banks' Guarantee Fund. This is the fifth year that Finanstilsynet and the Norwegian Banks' Guarantee Fund have jointly carried out this testing. The conclusion was that banks seem to have made progress towards attaining a satisfactory quality of reporting.

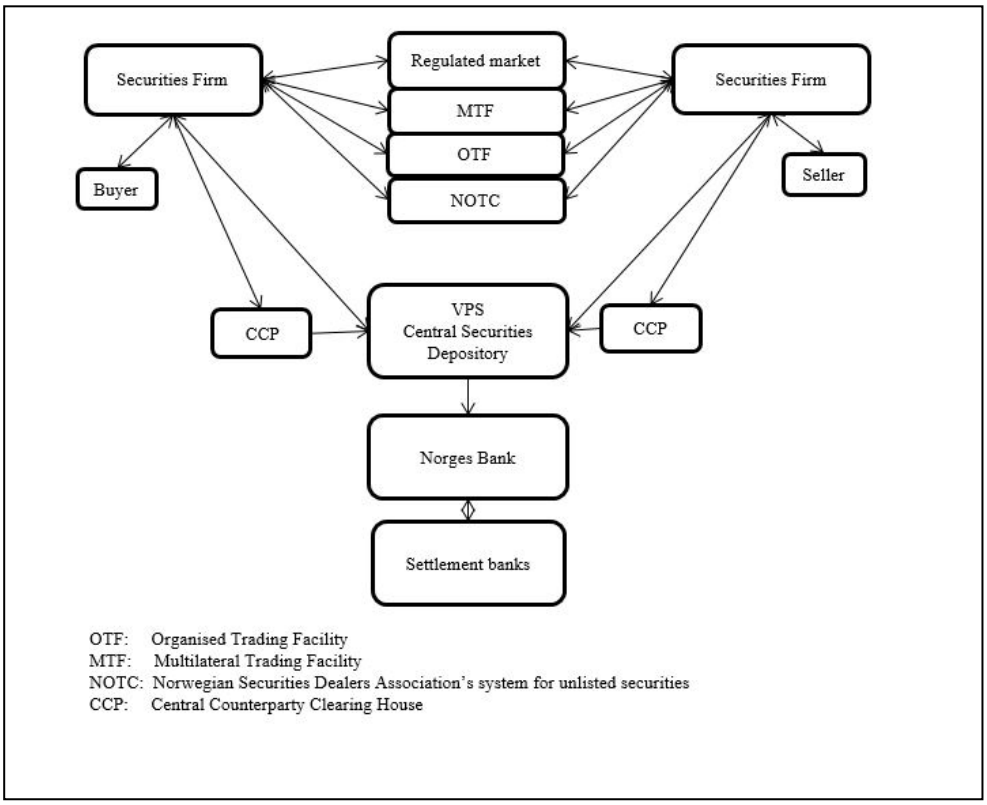
3.3 Securities

Substantial changes in the framework conditions for investment firms and market infrastructure institutions, such as implementation of the Markets in Financial Instruments Directive (MiFID II), the European Market Infrastructure Regulation (EMIR) and the Markets in Financial Instruments Directive 2004/39/EC (MiFID), which introduced extended transaction reporting obligations with effect from 2018, necessitated changes in financial institutions' systems in 2017. New products such as share savings accounts and individual pension savings schemes (IPS) were launched in 2017.

The securities sector experienced no critical or very serious ICT incidents in 2017, despite the fact that investment firms' system portfolios generally underwent numerous and, to some extent, major changes.

Through its supervisory activities, Finanstilsynet has identified areas in which financial institutions should make improvements. Further details of the most salient findings and assessments may be found below.

Figure 3: Simplified presentation of key roles and connections



Source: Finanstilsynet

3.3.1 Underreporting of ICT incidents

A number of incidents that occurred in investment firms were not reported to Finanstilsynet as required by the ICT Regulations. Finanstilsynet takes a serious view of investment firms not complying with the requirement to report significant irregularities to Finanstilsynet. This underreporting limits Finanstilsynet's possibility of monitoring institutions' handling of critical situations. By monitoring incidents, Finanstilsynet can identify factors that can

contribute to the establishment of important preventive, risk-mitigating measures, also in other institutions.

3.3.2 Unstable e-trading systems

Due to instability in the online share trading systems of some banks and investment firms, customers were unable to make changes in their portfolios. To some extent, the timing of technical failures coincided with significant market changes that resulted in higher transaction volumes. This taxed the capacity of the system solutions of certain institutions and firms. Through its monitoring of such incidents, Finanstilsynet has imposed requirements on some institutions regarding evaluations and the implementation of necessary measures. Finanstilsynet takes a serious view of such incidents and will follow up on this matter in 2018.

3.3.3 Problems relating to the introduction of share savings accounts (ASK)

In connection with the introduction of the share savings account product, Finanstilsynet noted that, during the initial period following its introduction, some banks and investment firms were unable to release and/or transfer customers' assets as ordered. Consequently, some customers were deprived of the possibility of making changes in their portfolio for some time. The reason for the aforementioned problems was the inadequate standardisation of exchange formats between investment firms and insufficient expertise in the securities sector in connection with the development of some firms' ICT systems.

3.3.4 Deficiencies in outsourcing agreements

In its review of notifications regarding the outsourcing of ICT services by investment firms, and in on-site inspections, Finanstilsynet detected deficiencies in the firms' risk assessments and in outsourcing agreements. The agreement parties were both small local service providers and large multinational companies that provide cloud services.

Finanstilsynet has stressed to the firms the importance of the requirement that risk assessments carried out in connection with outsourcing processes must be submitted for consideration by the Board of Directors. Finanstilsynet emphasises that when outsourcing services, firms must ensure that they retain unlimited rights and possibilities of exercising control of all elements of the service provider's operations that may affect the outsourced service delivery. See also 3.8.2.

3.3.5 Lack of guidelines for use of a third party in connection with security testing

Finanstilsynet has noted an increase in the use of external operators and/or consultants to carry out security tests to identify vulnerabilities in firms' infrastructure and electronic defences. Security testing is essential. At the same time, testing of firms' infrastructure could cause critical systems to become unstable or unavailable, and/or sensitive information may go astray. This requires effective management and control on the part of the firm to ensure satisfactory testing. In connection with inspections of a number of investment firms, Finanstilsynet noted the inadequacy or lack of documentation of guidelines, procedures and plans for carrying out security tests. See also 3.9.4.

3.3.6 Inadequate testing skills and testing

It is important that testing systems are kept up to date in order to achieve the requisite testing quality. Investment firms must ensure that testing systems are kept sufficiently separate from production systems to prevent the erroneous use of test data in production systems.

The risk of errors in connection with the production release of new systems or system components is great if the production release is carried out without sufficient quality assurance or control, and the testing environments are not sufficiently updated.

In 2017, Finanstilsynet noted some serious error situations that were due to deficiencies in the firms' testing systems and testing procedures. The situations arose in part as a result of weaknesses in the testing environment and deficient testing prior to production release. As a result, the quality of new functionality and new systems released into production was inadequate. Error situations also arose due to the fact that the institution's testing and production systems were not sufficiently segregated, resulting in the erroneous entry of test data in the production systems.

3.4 Insurance

Through its inspection activities, Finanstilsynet has found areas in which improvements should be made by insurance undertakings. More detailed information on key findings and assessments is provided below.

3.4.1 Reporting of incidents

Finanstilsynet has previously called attention to the underreporting of ICT incidents. The review of reporting for 2017 shows that more insurance undertakings than before reported incidents in 2017, which may indicate a certain improvement. When a comparison is made

with banks' reporting, Finanstilsynet considers that there may still be underreporting. This matter will be followed up in supervisory activities in 2018. Reference is also made to 3.7.

3.4.2 Inadequate ICT risk management

Technological changes also have an impact on the insurance industry. Changes in sales channels, use of new technology and data collection for use in the pricing and development of new products are factors that affect the risk picture. Insurance undertakings must adopt a proactive approach to these changes. See also 3.4.5.

Through inspections, Finanstilsynet has noted that some insurance undertakings do not have satisfactory risk management processes. Finanstilsynet emphasises that responsibility for establishing adequate processes for risk management and the proper handling of risk is incumbent on the board of directors and general manager.

3.4.3 Risk related to stand-alone systems for cost allocation and cost-benefit analysis

Through inspections in 2017, Finanstilsynet has considered the development, management and use of some insurance undertakings' risk models. The models are used to assess various types of market and industry risk, and to calculate capital requirements. The models are important management tools for monitoring risk and profitability.

The results of the model calculations are included in both the board of directors' assessment of the undertaking's activities, in reporting to the public authorities and in information communicated to the market. It is important that the calculation models are properly managed and quality assured.

It is common practice to use spreadsheets and develop stand-alone systems for this type of calculation. Finanstilsynet has previously pointed out weaknesses in the control of changes in spreadsheets and access control when spreadsheets are used, together with deficient integration control of data entered into such stand-alone systems. Documentation of processes is non-existent or inadequate. The aforementioned factors pose a risk of errors in calculation formulas and in manual data entry.

Finanstilsynet notes that the modelling systems often appear to be open analysis tools with poor or no integration control. Examples are the lack of functionality to ensure consistent use of parameters from one period to the next, and the absence of functionality that ensures that closing assets in one period are opening assets in the following period. This increases the risk of error in calculated results.

Dependence on key specialist personnel who manage, develop and use the calculation models is a critical factor, especially in small undertakings. Insurance undertakings therefore run the risk that analyses and reports are of poor quality, or cannot be carried out.

3.4.4 The new General Data Protection Regulation (GDPR)

Insurance undertakings manage large quantities of sensitive personal data, and many of the undertakings find it difficult to adapt their systems to the new General Data Protection Regulation (GDPR). The new Regulation requires that:

- all undertakings have a legible and understandable personal data protection declaration that explains how the undertaking processes the data subject's personal data
- the undertaking must know which personal data it holds and where the data are stored
- the undertaking must be able to document the need for the data that are stored, and who is using which data for what purpose
- data subjects may request the erasure of their personal data. Implicit in this right is a requirement for clearly defined data erasure processes
- data subjects may request to receive a copy of their personal data in a consolidated, structured data format, and data subjects may thus be able to transfer their personal data to, for instance, another undertaking

The GDPR contains a data quality requirement whereby insurance undertakings have an obligation to have consistent data. In many cases, undertakings will need to conduct a manual data quality review to be able to detect inconsistent data.

Finanstilsynet has noted that some insurance undertakings have made a late start on adapting to GDPR requirements.

3.4.5 Technological developments

InsurTech is a collective term used in the insurance sector for the technology used to achieve competitive advantages and higher profitability.

Technological advances open up for significant changes in insurance undertakings' traditional business models. There is a trend towards increased digitisation of existing business processes with a view to improving efficiency and reducing costs. This includes:

- automated advisory services
- automated claims processing

- more detailed customer data. Insurance undertakings are able to collect more data from third parties, and to link these data to their own customer data (description of the customer)
- a better overview of the value of the object insured and any attributes of the object insured that might affect the risk of an insurance event occurring (description of the object insured)
- how much and how the object insured is used. The parameters that affect the risk that an insurance event will occur (description of risk)

By using new measuring instruments and methods, insurance undertakings can collect insurance risk data in a way that previously was not possible. The actual data collection process is carried out by using smart phones, smart watches and various types of sensor that record relevant data. With more accurate data capture, the underlying data for determining insurance premiums will be improved. This could benefit the insurance undertaking and the customer alike.

The use of new technology introduces new risks that insurance undertakings must identify and address. In its supervisory activities, Finanstilsynet will focus attention on the way in which undertakings implement, document and assure the quality of systems. This applies in particular to systems where use of technology directly affects the determination of premiums.

3.5 Auditing firms

Through inspections in 2017, Finanstilsynet has noted that auditing firms have outsourced parts of their activities. Although some functions may be delegated to others, responsibility still lies with the auditing firm. In order to fulfil this responsibility satisfactorily, there must be written agreements that ensure that the auditing firm has sufficient insight into and control of the outsourced activity. This also applies to outsourcing to other companies in the same network.

Finanstilsynet's inspections have revealed a lack of written outsourcing contracts. Finanstilsynet made a closer assessment of an auditing firm that was a party to an outsourcing agreement with a cloud service provider through an agreement entered into by the auditing network. The cloud service provider in question uses a standard attachment to its agreements with financial sector customers which is intended to meet such customers' need for access to and control of information. Since Finanstilsynet's inspection, the cloud service provider and the auditing network have drawn up an attachment to the outsourcing agreement in question that is adapted to auditing services and that provides the auditing firms with necessary access and control.

3.6 Monitoring of compliance with anti-money laundering rules

Finanstilsynet carries out inspections of institutions' system support for prevention of money laundering and financing of terrorism. Finanstilsynet has observed inadequate documentation of the risk assessments on which electronic customer and transaction control procedures are based. This could result in the institution lacking insight as to whether the controls are adequate to detect the risk of money laundering and terrorism financing. Finanstilsynet has also pointed out that procedures for adopting a new electronic control in the systems, and for evaluating and monitoring such new and changed controls, must be formalised and documented to ensure that the controls established in the systems are reasonably accurate. As regards screening against sanction lists, Finanstilsynet has assessed whether customers and transactions are always screened against the most recently updated list. Any irregularities are pointed out to the institution.

3.7 Incidents reported in 2017

Financial institutions report to Finanstilsynet on irregularities and change management in connection with serious and critical ICT-related incidents in accordance with the requirements of the ICT Regulations. This reporting covers both unintentional (operational) and intentional (malicious) incidents. Most of the reports received by Finanstilsynet concern operational incidents. One reason for this is that incidents affecting a single individual, or a small number of customers, such as payment card thefts, are generally not subject to reporting. A better overview of the level of intentional incidents is therefore provided by status reports from Nordic Financial CERT and loss statistics; see 3.7.1.

3.7.1 Incident statistics

A number of serious incidents affected the availability of payment services and the bank's customer-facing systems in 2017. After a decline in the number of incidents reported in 2015 and 2016, the number rose in 2017 by around 25 per cent to 190 incidents. A total of 160 of the incidents were reported by banks. In several of the incidents in 2017, more than 30 per cent of Norwegian bank customers lost access to payment services for an entire day. These operational incidents affected the banks' technical infrastructure. Of the 190 incidents reported, ten reports concerned security incidents (intentional, malicious incidents), several of which were related to crypto virus attacks.

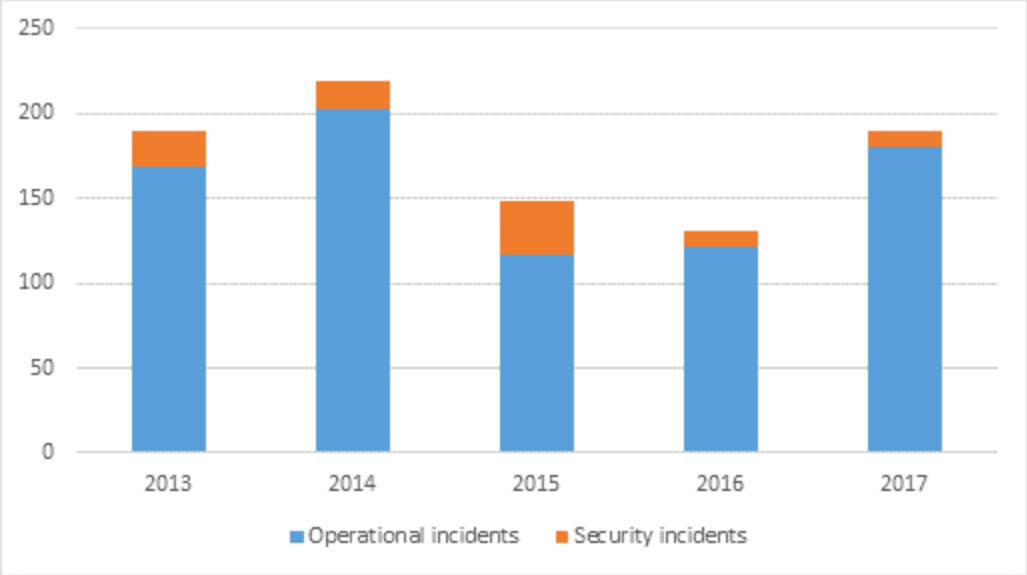
BankID, BankAxept and NICS are part of banks' shared operational infrastructure. Banks' IT operations are otherwise spread across several different operating sites and/or operations centres. If an incident does not affect the shared operational infrastructure, it is unlikely that more than about 40 per cent of bank customers will be affected simultaneously by an

incident. The banks operating in Norway have operating sites in Norway, Sweden and Denmark. Several institutions have also begun to use cloud services.

The most serious operational incidents in 2017 involved errors in mainframe management systems, as a result of which the established duplicate system failed to function as intended. One of the incidents occurred at a shared service provider and thus affected several banks, in addition to a number of insurance undertakings and investment firms. Because the solution time was underestimated and there was uncertainty as to whether the disaster recovery solution would work as expected, even though it had been tested, the disaster recovery solution was not implemented. Finanstilsynet considers these matters to be serious.
See also 3.7.2.

A number of operational incidents can be ascribed to problems that have arisen after the relocation of operations to new data centres.

Figure 4: Incident statistics



Source: Finanstilsynet

Table 4: Reported incidents

	Operational incidents	Security incidents
2013	168	21
2014	202	17
2015	116	32
2016	121	10
2017	180	10

Source: Finanstilsynet

Vipps is the most widely used service for person-to-person payments. Given the steadily expanding area of application in both the private and the corporate market, access to the service has become critically important as a great many users would be affected by incidents. In 2017, a number of incidents were reported, some of which occurred in connection with the relocation of the service to a new operating site.

In 2017, there were again several incidents involving operational irregularities in the BankID service. The incidents affected bank-stored BankID, mobile BankID and/or the production of one-time passwords. BankID has a wide range of subcontractors in the telecommunications sector, and incidents will have varying impacts depending on the individual customer's mobile subscription. On days when traffic is particularly heavy, such as when tax returns are published, Finanstilsynet registered that BankID had capacity problems again in 2017. Finanstilsynet will monitor developments and consider the need for remedial action.

In 2017 the operation of important payment systems was transferred to global cloud service providers. A number of incidents related to this operation, which resulted in unavailable payment services, were reported. As a rule, the incidents occurred in connection with changes and some entailed a long restoration period, an indication that change management processes are not sufficiently mature. The incidents also showed that cloud service providers had not established an incident handling process in conformance with the service's criticality and the bank's expectations.

Despite increasingly mature operating procedures, human factors are still a decisive contributory cause of the occurrence of an incident. Several serious incidents were due to failure to implement change management in accordance with established procedures.

Of the 190 incident reports that Finanstilsynet received in 2017, 14 were sent by investment firms and infrastructure institutions, including VPS and Oslo Børs. Various operating incidents resulted in the unavailability of share trading for a period of time, including access to updated information. Among other things, a serious transaction error was caused by

changes implemented without the error being detected during testing. One incident occurred as a result of a crypto virus[20] attack.

Finanstilsynet received ten incident reports from insurance undertakings. The reports concerned the possible exposure of customer data and various operational problems that prevented access to online services. This included two reports on crypto virus attacks.

Three incidents were reported which affected the banks' systems for electronic customer and transaction monitoring against money laundering and terrorism financing.

Assessing the degree of seriousness of an intentional incident, and whether it should be reported, can be difficult, but Finanstilsynet expects to be notified when, for example:

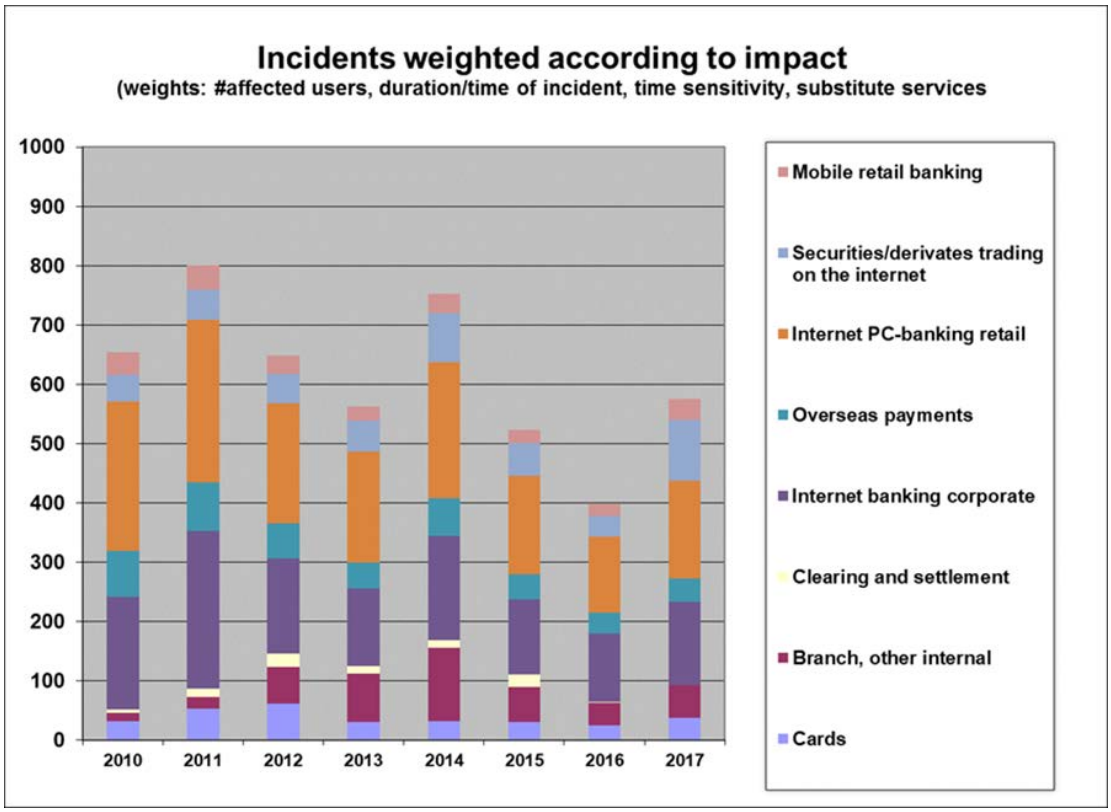
- attacks/errors have affected infrastructure
- attacks/errors have affected many customers
- many small attacks and/or errors collectively affect many customers
- new forms of attack ("modus operandi") are experienced
- the internal threat level has been raised to red

3.7.2 Analysis of incidents as a measure of availability

For each incident that has impacted 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 meet customers' needs (such as when the mobile banking service is unavailable, but the online bank is available). The data are weighted

[20] The viruses are also called ransomware, as attackers encrypt data and then demand a ransom from the victim of the attack for restoring access to his data.

Figure 5: Incidents weighted by impact



Source: Finanstilsynet

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 less available to customers in 2017 than in the two preceding years.

Examples of mobile banking incidents are when components unique to the mobile banking service, such as the mobile network, are down, mobile services (like Vipps) are unavailable, or when software components related to the mobile banking service are out of action.

3.7.3 Failure of business continuity and contingency preparedness systems

Finanstilsynet has followed up on serious operational incidents in 2017, among other things by procuring banks' assessments of how business continuity and disaster recovery systems functioned during the incidents and whether they functioned as expected. Deficiencies were detected in this connection in the duplicate systems. Finanstilsynet also noted uncertainty on the part of banks and/or operational service providers as to how long it will take to restore production using the disaster recovery system during a real emergency. Institutions have

initiated intensive testing of the disaster recovery systems to ensure that restoration is carried out as intended. Finanstilsynet will follow up on the result of these measures.

3.8 Outsourcing

Outsourcing is when the institution chooses to use an external service provider rather than operate, develop and administer its own ICT services. ICT services that support the institution's activities are covered by the ICT Regulations. Institutions have an independent responsibility to make sure and monitor that the institution and its service providers comply with the regulatory requirements. A good understanding of what this responsibility entails, for both the institution and the service provider, is a prerequisite for compliance with the rules. See also 4.1.7.

3.8.1 Notification of outsourcing by institutions

Finanstilsynet received close to 50 notifications of outsourcing of ICT services in 2017. Most of the notifications concerned outsourcing to major global cloud service providers or changes of subcontractors.

If operational services of major importance to payment systems or other financial infrastructure are outsourced to foreign operators, Finanstilsynet may impose special requirements regarding the establishment of contingency preparedness systems.

Finanstilsynet notes that institutions are using a steadily growing number of subcontractors. This is due both to the fact that systems are more complex, since they involve the participation of more service providers, and that the service provider to which the institution outsources in turn outsources services to subcontractors. This necessitates increased interaction with subcontractors and between subcontractors, also when dealing with serious incidents.

3.8.2 Outsourcing agreements

Outsourcing agreements must contain provisions that underpin the responsibility of the institution, including requirements regarding reporting and collaboration, as well as provisions that safeguard the institution's and the authorities' right to conduct audits and inspections of the operations of the service provider and its subcontractors. Furthermore, the institutions themselves must ensure that procedures are established and documented in accordance with the requirements of the ICT Regulations.

Agreements reviewed by Finanstilsynet show that it is only by way of exception that the regulatory requirements are not met. However, Finanstilsynet sees a need for greater

awareness in some institutions of the necessity of making sure that the agreements ensure as far as possible the institution's compliance with laws and rules, as well as the sound operation of the institution, and establishment of the necessary management and control of outsourced service deliveries. Possible examples are efforts to deal with critical incidents, acceptance and approval provisions and termination provisions.

3.8.2.1 Critical incidents

In some cases, Finanstilsynet's review has revealed deficiencies in agreement provisions that are applicable in the event of critical incidents. The consequences that a critical incident can inflict on an institution and/or the institution's customers have not been sufficiently assessed, and requirements regarding solution times are not always proportionate to the consequences. Nor does the agreement state clearly when contingency preparedness systems are to be put into effect. Circumstances that give the institution the right to invoke material breach by the service provider are not clearly defined in the agreement. This constitutes a risk that considerable losses may be inflicted on the institution in the event of repeated and serious operational irregularities in the service provided. Finanstilsynet underscores the importance of the institution itself and the service provider establishing insurance agreements with coverage that is proportionate to the consequences and risks related to the service.

3.8.2.2 The resource situation of small service providers

Small service providers may, due to limited resources and dependence on certain individuals, constitute a risk of instability in the provision of critical services. In Finanstilsynet's view, it is important that institutions secure access to source code by including a source code escrow arrangement in the outsourcing agreement. Moreover, the agreement should ensure that software may be transferred for further management and development by another service provider and/or to the institution itself if the service provider is unable to meet its obligations in the provision of critical services.

3.8.2.3 Provisions in connection with termination

Outsourcing that does not provide the result expected will, as a rule, result in the cessation of the service and termination of the agreement. In such processes, the institution may incur substantial costs and be placed in a difficult operational situation. Transferring the service to another service provider may pose a challenge and entail significant risk for the institution.

Finanstilsynet has seen deficiencies in, and in some cases an absence of, strategies and provisions applicable in the event of termination of an agreement. When negotiating and concluding an agreement, provisions (exit provisions) that impose obligations on the service provider when service provision is transferred, are extremely important. To ensure that such a transfer is controlled and secure, the agreement should stipulate the respective obligations of the current service provider and the institution itself in the event of the transfer of the service to a new service provider or the institution itself.

3.8.3 Outsourcing to cloud services

Finanstilsynet has not noted any agreements entered into with cloud service providers in 2017 that are not in compliance with the regulatory framework. Although institutions have included assessment of outsourcing to cloud services in their risk management framework, Finanstilsynet considers that risk assessments that are submitted with the outsourcing notification, and that serve as the basis for decisions made by the institutions and their boards of directors, should be improved.

3.8.4 Cloud service providers' handling of critical service incidents

Finanstilsynet requires that outsourcing to cloud service providers is subject to the same management and control by institutions as applies to outsourcing to other service providers.

The introduction of cloud services for operating institutions' critical services also entails new challenges when serious operational disruptions occur. Well-functioning cooperation models that clearly define the roles and responsibilities of all parties are essential for effective problem solving when incidents occur.

Through a serious incident in 2017, weaknesses were revealed in the incident handling of a cloud service provider. The process was not sufficiently well established to deal with incidents that affected time-critical services, including procedures for cooperation with the affected institution and the institution's other service providers. Finanstilsynet notes that this experience was a factor that prompted the institution to take action with regard to the service provider.

3.8.5 Outsourcing rules

The European Banking Authority (EBA) has drawn up recommendations for outsourcing to cloud service providers[21] that will apply as from 1 July 2018. The EBA guidelines for outsourcing are currently being revised and will replace the aforementioned recommendation. The guidelines will also cover outsourcing of ICT services and will be expanded to cover outsourcing to cloud service providers.

[21] https://www.eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions

3.9 ICT security

ICT security is the focus of growing attention. This applies in particular to cyber security, where risk is regarded as high and increasing, in light of international attacks and incidents targeting both nations and large financial institutions, such as Equifax.[22]

3.9.1 Organising ICT security work

The board of directors of institutions must arrange for sound organisation of operations, and is responsible for ensuring that the institution's management organises and executes security work in line with requirements for sound organisation and operation, applicable legislation and good practice. This presupposes that both the board and the management have the necessary qualifications, and that the institution's security work receives the necessary attention and priority.

Goals must be set for the institution's ICT security organisation and work. Organisational roles and responsibilities must be clearly defined. Responsibility for managing ICT security, for monitoring ICT security and for operational ICT security must be clearly separated.

Finanstilsynet considers it important that the business function is involved in and owns the ICT security in its own business area.

3.9.2 Observations of cybercrime

Cybercrime that targets financial institutions may take the form of attacks on availability, on confidentiality through unauthorised retrieval of information, and on integrity, through unauthorised payment transactions. Digital attacks may affect several dimensions, and it may be difficult to determine the purpose of the attack.

As a result of meetings with institutions to follow up on incident reporting, Finanstilsynet is aware that they have observed a substantial increase in undesirable activity. A small proportion of this undesirable activity results in security incidents that are reported to Finanstilsynet; see 3.7.1.

[22] https://www.theguardian.com/technology/2017/oct/11/personal-details-of-almost-700000-britons-hacked-in-cyber-attack

Data security: safeguarding of information, whether digitally stored or not. Data security means ensuring that information is not disclosed to unauthorised persons (confidentiality), is not altered unintentionally or by unauthorised persons (integrity) and is available as needed (availability)

ICT security**:** safeguarding of information and communication technology (ICT), i.e. hardware and software.

In the report, ICT security is used as a joint designation for data security and the security of ICT systems.

3.9.2.1 Phishing and social engineering

Finanstilsynet is aware from follow-up meetings on incident reporting and interviews with institutions that they observe a steady increase in "phishing" and social engineering of customers, the aim of the attackers being both financial fraud and the acquisition of information. These methods are regarded as simpler for penetrating an institution's IT systems than demanding technical attacks. The methods used are evolving, and becoming more and more ingenious and sophisticated. Personal data from social media, e-mail addresses, user names and passwords are bought and sold among criminals, and the information is then used for targeted attacks.

Criminals who succeed in gaining access to e-mail servers can monitor the traffic and thereby acquire knowledge of patterns and behaviour. Criminals can also step into an ongoing exchange of e-mails and change the contents, for example account number and details, or acquire information that can be used in other criminal contexts.

Finanstilsynet is aware that CEO fraud and similar fraud are still a major challenge, and that they have become more sophisticated. At the same time, Finanstilsynet sees an improvement in financial institutions' prevention of this type of incident through employee training and awareness programmes.

3.9.2.2 Technical measures to detect unauthorised e-mail

As mentioned, considerable challenges continue to be posed by false e-mails. It may be difficult, if not impossible, for the recipient of a false e-mail to detect that the e-mail is false. Specific measures are used to block phishing e-mails.

Domain-based Message Authentication, Reporting & Conformance (DMARC)[23] is one method of protecting an institution's own domains against false e-mails, blocking false e-mails from external domains and reporting cases where false e-mails are detected. This method is used to create a policy with IP addresses and signing information against which a check must be made in the transmission. This information is stored in the Internet Domain Name System (DNS), and institutions are then able to check incoming e-mails as part of their evaluation of the sender of the e-mail.

3.9.2.3 Serious global cyber attacks in 2017

The impact of cyber attacks by the malware WannaCry, in May, and NotPetya, in June 2017, was felt across countries and sectors. Both had elements of cryptovirus. The attacks caused great damage when the virus succeeded in penetrating corporate networks, and illustrate how powerful a massive cyber attack can be. Defence weaknesses such as unsecured network access and inadequate segmentation of networks into zones were exploited.

The Norwegian financial sector was not affected, probably because the financial sector is better protected and has long experience of protecting itself against attacks.

3.9.3 SWIFT's security programme

SWIFT is an international communication network for the transfer of cross-border payments and large domestic payments. The biggest banks in Norway, Norges Bank, and the Norwegian Central Securities Depository (VPS) use SWIFT and are SWIFT members.

The security incidents in 2016 that impacted banks and central banks attracted considerable attention. According to SWIFT, the incidents were linked to the affected banks' internal payment systems, and not to SWIFT systems. In response to the incidents, SWIFT established the Swift Customer Security Programme[24] for its customers in 2017.

All SWIFT members are responsible for the security of the system, but SWIFT has undertaken to assist its customers with expertise and competencies to withstand cyber attacks. The security programme consists of 16 mandatory security controls which all SWIFT users, whether they are linked to SWIFT directly or indirectly, must implement. SWIFT users must submit a self-attestation every twelve months to the effect that they comply with the requirements. Finanstilsynet will monitor the institutions' self-attestation work.

3.9.4 Testing security by means of third-party operators

Security testing is an important means of verifying robustness and detecting vulnerabilities in institutions' technical infrastructure and organisation. The tests require careful planning, and

[23] See https://dmarc.org
[24] https://www.swift.com/myswift/customer-security-programme-csp

must be carried out according to defined requirements in an institution's security framework. The institution's board and management have the ultimate responsibility for ensuring that a security framework is established in conformity with good practice, and that security tests are performed accordingly.

The security tests expose technical infrastructure to instability and/or unavailability of critical systems, and tests of this type also constitute a risk of sensitive information going astray if they are not conducted with the necessary management and control. Risk assessments should be performed to identify factors that may trigger undesirable incidents as a consequence of security tests.

Finanstilsynet notes that security tests are often limited to tests of the penetrability of the institutions' technical infrastructure, including firewalls. Methods such as social engineering, DDoS attacks and other forms of attack are used to a lesser extent. Third party operators are increasingly being used to monitor, test and improve the security level of institutions' technical infrastructure, partly because the institutions themselves do not have the necessary expertise. It is important to use operators who are qualified for these tasks, particularly when the operators that are engaged gain access to details about the institution's technical infrastructure, data and organisation.

The Norwegian National Security Authority (NSM) has established a pilot project for quality-assuring operators that deliver security services. An overview of quality-assured operators is published on NSM's website. It is important that institutions have thorough processes for selecting security service providers.

3.9.5 Vulnerability reporting

Finanstilsynet is aware that one incentive used by institutions to meet the challenge of inadequate ICT security expertise is to reward persons who discover vulnerabilities in the institution's defences. One precondition is that the detector feeds back the necessary information about the vulnerability, and pledges confidentially about weaknesses discovered until they are remedied.

This measure may reduce weaknesses and improve the ICT security of institutions. The basis of experience is limited at present. Finanstilsynet will follow up developments to determine whether this practice results in negative consequences for the institution, for example reduced operating stability due to an increase in the number of cyber attacks.

3.9.6 User identity and password gone astray

The use of digital services, both private and work-related, on devices such as smart phones, tablets and television, has become an important part of digital everyday life. There are many

providers of these services, and use of the services increasingly demands user authentication in the form of e-mail address and password.

In recent years, a number of incidents have been recorded where hackers have succeeded in retrieving registers of e-mail addresses and passwords as a result of vulnerability in operators' infrastructure. These data are now being offered through digital marketplaces and are subsequently used by criminals for their own activities. Employees who use the same log-on information for several digital services therefore increase the risk of the information falling into the hands of criminals. This makes it simpler for the criminals to identify the roles and responsibilities of employees, for example through social media. Identified employees run a high risk of social engineering and threats, and of the criminals succeeding in gaining access to the institution's systems. The risk of employees being coerced into carrying out unauthorised actions also increases.

Raising of employee awareness should be an ongoing process. The use of two-factor authentication and establishment of a normal, sound practice for the institution's security system, including obligatory change of password and password structure requirements, are important risk-reducing measures. There are services that can detect whether an e-mail address has been compromised[25]. For employees who may be subject to social engineering, it will be useful to investigate this.

3.9.7 Upcoming security rules

The EU Directive on security of network and information systems (NIS Directive) will be transposed into Norwegian law. The Directive requires that providers of services that are vital to society must conduct risk assessments of networks and information systems, implement the measures necessary to prevent, detect and mitigate the consequences of incidents, and report incidents. The Directive states that where there is already a regulatory framework in place which imposes requirements that are at least equivalent to the Directive's requirements, other law shall be used. Finanstilsynet's assessment is that the current regulatory framework for the financial sector in Norway largely covers the requirements in the Directive.

A new Norwegian Act relating to national security (the Security Act) enters into force on 1 January 2019. In autumn 2017, a project was established to draft regulations to the Act. The draft regulations will be circulated for comment in 2018, and the aim is for them to enter into force at the same time as the Act.

[25] https://haveibeenpwned.com/

Work is also in progress under the ICT Security Committee[26], which is a cross-sectoral Norwegian committee with a mandate to determine whether the current regulation and organisation of ICT security in Norway is appropriate.

3.10 Management of competencies when changes occur

The expression "Run the Bank" as opposed to "Change the Bank"[27] is used to illustrate the challenge of balancing the distribution of resources between secure and stable operations on the one hand, and adapting the institution, for example to new products or services or the use of new systems and new technology, on the other. This also involves determining what competencies the institution must have in the short and long term, so that in addition to handling planned tasks, it is capable of handling unforeseen tasks.

Finanstilsynet's impression is that in a downsizing situation, institutions allow the needs of the future to take precedence. Finanstilsynet believes that it is important for institutions also to attach weight to and maintain competencies for managing day-to-day operations, and to place more emphasis on being able to maintain stable and secure operation of existing services.

Finanstilsynet has noted that institutions have used outsourcing processes to make staff cutbacks, and subsequently rebuilt the competencies that were lost. This may indicate underestimation of the need for competencies for running daily operations. There are also indications that contractors were not capable of performing all the expected tasks.

3.11 Joint initiatives in the financial industry

There is cooperation across a number of areas in the financial sector, particularly security and shared infrastructure, services and standards.

In April 2017, a working party consisting of representatives of the financial industry and Norges Bank delivered a report on the BRO project which concerns the establishment of a new, shared infrastructure for payments with faster settlement[28]. The proposal includes adjustments to Norges Bank's settlement system. The proposed infrastructure will lay the groundwork for continuous processing of real-time payments, called BRO payments. It is

[26] https://www.regjeringen.no/no/dep/jd/org/styre-rad-og-utval/tidsbegrensede-styrer-rad-og-utvalg/IKT-sikkerhetsutvalget/id2570775/

[27] "Run the bank" describes activities intended to ensure secure, stable operations. "Change the bank" describes the process of adapting the institution to new products and services, and changing it with the aid of new systems and new technology.

[28] https://www.bits.no/wp-content/uploads/2017/04/Sluttrapport-BRO.pdf

proposed that all banks must undertake to integrate their payment systems with the new shared infrastructure, and thereby offer their customers real-time payments, and that this must be carried out according to the schedule set by the establishment project for the BRO solution. The banks plan to start implementation in 2018, with the aim of establishing a system in the course of 2019.

The largest Nordic banks[29] have announced that the possibility of a Nordic payment infrastructure with common products is being examined. The goal is to establish systems for domestic and cross-border payments in several currencies (SEK, DKK, NOK and EUR) in the Nordic countries to facilitate cross-border payments and promote trade among the Nordic countries. Information from the initiative-takers indicates that the goal is consistent with existing national infrastructure projects in Sweden and Norway; see the BRO project. The aim is to establish solutions that meet needs both within and across the Nordic countries, rather than those of a specific country.

The public sector and the financial services industry are collaborating on digitising and improving the efficiency of important societal processes through the DSOP project[30] on digital cooperation between public and private sector. This involves cooperation with the Norwegian Tax Administration, the Norwegian Labour and Welfare Organisation (NAV), the Brønnøysund Register Centre and the police in the areas:

- **consent-based loan application** – retrieval of information from the public sector
- **verification information** – exchange of relevant verification information between banks and the Tax Administration in connection with investigation[31]
- **bankruptcy proceedings** – immediate digital notice to the bank to block accounts
- **company establishment** – simplify the process of establishing companies
- **information on sickness and disability from NAV** – simplify and improve the efficiency of the process between insurance institutions and NAV

There is also considerable internal cooperation in the financial services industry coordinated by Bits, through the work on the PSD 2 and XS2A projects[32], established to consider potential shared systems and the establishment of common standards in line with PSD 2.

In 2017, the Nordic banks established Nordic Financial CERT, which is based on and replaces the Norwegian financial services industry's FinansCert. The purpose of Nordic Financial CERT is to improve the security of institutions and their customers by sharing information, expertise and experience relating to cyber security.

[29] http://www.hegnar.no/Nyheter/Naeringsliv/2018/02/Nordiske-banker-utreder-muligheten-for-felles-betalingsinfrastruktur
[30] https://www.bits.no/project/dsop/
[31] https://www.bits.no/project/kontrollinformasjon/
[32] https://www.bits.no/project/psd2-xs2a/

3.12 Developments in financial technology

Developments in financial technology relate to both new and existing services provided by institutions, but the technology is also used for institutions' monitoring of compliance with regulatory frameworks.

3.12.1 FinTech

The financial industry is constantly changing, and more new operators will establish themselves in the financial sector as service providers. Although the financial services industry has been well to the fore in the use of ICT, we now see a steady emergence of new initiatives to challenge the established institutions.

The term 'FinTech' covers technological developments in all parts of the financial services industry, but more specific terms such as BankTech, PayTech and InsureTech are often used when talking about the use of new technology in the various service segments.

Technological innovation changes the industry through the use of new systems, increased competition and new operators in value chains. The progression in developments in artificial intelligence, machine learning, robotisation, increased use of big data together with new technology such as blockchains and cloud services, is contributing to a wave of digitisation that influences and challenges the institutions' business models.

Finanstilsynet is monitoring developments, and watching how established institutions and new operators adapt to laws and regulations. The considerations to which Finanstilsynet attaches importance are financial stability, secure services and sound customer protection. To achieve these, the same risk should be treated the same way, irrespective of business model.

Finanstilsynet has set up an information site[33] on which FinTech institutions can find relevant information and information on how to contact Finanstilsynet for advice, both in advance of and during the process of establishing a business model and preparing an application for a licence.

The European Banking Authority has prepared the EBA's FinTech Roadmap[34], based on a study of FinTech within the EU/EEA, which describes the work that has been initiated and is to be carried out in 2018/2019. The EU Commission has also drawn up a FinTech action plan[35].

When new technology is introduced or existing technology is used in an alternative way, Finanstilsynet assumes that risk assessments will be conducted to identify relevant risk.

[33] https://www.finanstilsynet.no/tema/fintech/
[34] http://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf
[35] https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

Relevant risk in this connection is risk of misuse or failure, risk of misreporting and the risk in connection with the responsibility the institution has assumed by implementing the new technological systems.

3.12.2 Artificial intelligence (AI) and machine learning

Artificial intelligence technology has reached a level that has caused institutions to turn their attention in recent years to the opportunities inherent in advanced forms of data processing and of self-learning systems.

Finanstilsynet underscores the necessity of establishing controls to ensure that systems based on artificial intelligence do not act in excess of expectations and stipulated requirements. If adequate quality control of development, testing and verification of results is not conducted after self-learning systems are put into production, use of the technology in the institutions' business processes and support functions may result in serious incidents.

Artificial intelligence could be used by criminals to carry out sophisticated attacks on the financial sector. The increased threat that this implies requires that institutions work together to establish resources and expertise to ensure ongoing upgrading of their defences.

3.12.3 Robotisation

Robotisation is contributing to the automation of manual tasks that are carried out today by an institution's customer service staff and executive officers. Advanced forms of robotisation use technology such as AI and machine learning, and "chatbot"[36] is also used in the customer interface. This is a natural development that will mean that interaction between institutions and customers increasingly proceeds without human contact on the part of the institution.

Finanstilsynet will monitor this trend and carry out inspections to assess how institutions manage and control their use of the technology.

3.12.4 Blockchains

It is maintained by many that blockchain technology could revolutionise the financial services industry in the years ahead. Finanstilsynet notes a high level of activity both in Norway and globally to evaluate the potential of this technology. Norwegian bank DNB has entered into a collaboration with several major banks on the use of the technology in trade

[36] Software that handles customer queries through spoken commands or text. Advanced chatbots employ AI.

finance[37]. The Bank of England is considering using the technology when renovating its settlement system[38].

This kind of technological change typically takes longer than expected to be put into use, and the consequences are often greater than anticipated. Few systems based on this technology have been introduced in the financial services industry as yet.

Finanstilsynet believes that it is important that the board of directors and management of institutions are prepared for how new technology, such as blockchains, can affect the financial services industry, including how and in which commercial areas new technology can be employed. Use of the technology may entail a need for changes in the organisation and working methods of institutions.

The technology may cause substantial changes for institutions and for cooperation among institutions. Finanstilsynet will monitor further developments.

3.12.5 Initial Coin Offerings (ICO)

ICO is the raising of capital[39] by issuing a virtual currency. The objective is fast, low-cost raising of capital for start-up companies and companies with new ideas that are in need of financing. ICO has also been used by established companies to raise capital. Investors mainly pay with virtual currencies such as Ethereum or Bitcoin, and are allotted tokens, which will be the start-up company's own virtual currency. After conducting an ICO, the issuer establishes a marketplace where the institution's tokens are exchanged for Bitcoin or Ethereum.

Risk to investors

ICOs are not currently covered by the regulatory framework for securities unless investors are given the right of co-determination in the company, profit-sharing rights, etc. If an ICO is not covered by the regulatory framework, investors cannot expect protection.

In connection with subscription to an ICO, a "whitepaper" is issued, which describes the project or company, and is analogous to the prospectus for an IPO[40]. There is no regulation or quality control of the contents of a whitepaper.

[37] https://e24.no/boers-og-finans/dnb/dnb-inngaar-globalt-blokkjedesamarbeid-med-flere-storbanker/24267065
[38] https://www.bankofengland.co.uk/-/media/boe/files/payments/rtgs-renewal-proof-of-concept.pdf?la=en&hash=2367D4475E64266B1C1F0399851C19DA05749543
[39] https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2017/lanebasert-folkefinansiering-crowdfunding--en-veiledning-om-laneformidling/
[40] IPO (Initial Public Offering) – the first public offer of shares in a company)

Finanstilsynet is aware that some false ICOs have been established internationally for the sole purpose of defrauding investors. There have also been international cases of ICOs "disappearing", for example when operators have seen that the business idea was not as viable as previously assumed, and the operators behind it have not honoured their commitments to their investors. There have also been cases of fraudsters establishing fake copies of an ICO issuer's subscription site, so that incoming payments have been made to the fraudster's account.

Investors also run a risk of an ICO allowing the funds to be used for purposes other than the intended one, for example if the amount subscribed in an ICO is higher than the value of the product or value of the company the ICO was supposed to finance. There is also a risk that investors may become involved in money laundering.

Finanstilsynet has published a warning against taking part in ICOs[41]. The warning is based on that of the European financial supervisory authorities. A large proportion of ICOs are intended to finance the realisation of a business idea or the development of a product that does not yet exist. This therefore often makes them synonymous with high-risk investments.

Developments in Europe

In their FinTech plan[42], the EU Commission have announced that they want to develop and harmonise a regulatory framework for the use of ICOs as a means of improving the effectiveness of cross-border raising of capital. This will be done in collaboration with the European financial supervisory authorities, and the risks, possibilities and appropriateness of the existing regulatory framework will be evaluated.

3.12.6 Virtual currencies (cryptocurrencies)

Prices for virtual currencies have been highly volatile since the summer of 2017, and the European financial supervisory authorities (EBA, EIOPA and ESMA) are concerned that a growing number of consumers are buying virtual currencies without understanding the risk this entails.

Finanstilsynet has published a warning about buying and owning cryptocurrencies[43]. The warning is based on the ESAs' warnings. Virtual currencies are highly risky and speculative products, and investments entail a strong risk of losses. The same applies to financial

[41] https://www.finanstilsynet.no/markedsadvarsler/2017/initial-coin-offerings-icoer---advarsel-til-investorer-og-foretak/
[42] http://europa.eu/rapid/press-release_IP-18-1403_da.htm?utm_campaign=unspecified&utm_content=unspecified&utm_medium=email&utm_source=apsis-anp-3
[43] https://www.finanstilsynet.no/markedsadvarsler/2018/finanstilsynet-advarer-forbrukere-om-kryptovaluta/

instruments that give exposure to virtual currencies. These currencies are not regulated, but are traded on unregulated marketplaces without price transparency. Virtual currencies are regarded as unsuitable for short- and long-term saving for most consumers.

3.13 Development of technological systems for complying with a new regulatory framework

Financial institutions spend substantial resources on complying with current rules and regulations and keeping abreast of and implementing new requirements. Manual processes in the preparation of internal reports and reports to the authorities are time-consuming. Finanstilsynet notes that there are growing efforts to develop technological systems designed to assist both institutions and authorities in their work.

RegTech (Regulatory Technology) is a collective term for technology-based systems designed to assist the institutions in identifying and meeting existing and new national and international regulatory requirements, including EU/EEA legislation. The risk of human error can be reduced, and internal and external reporting made more efficient. RegTech solutions are used for detecting money laundering and financing of terrorism, among other things.

Finanstilsynet regards it as positive that institutions are using this sort of technology as a means of ensuring and following up compliance with laws and rules, and as a means of reducing risk. At the same time, it places demands on the institutions' knowledge of and management and control of the technology.

4 The participants' assessment of risk factors

This chapter considers the principal threats brought up by the institutions themselves in interviews and in their responses to Finanstilsynet's questionnaire.

4.1 Interviews

4.1.1 Changes

The institutions mention that systems changes are many and frequent, and there is great competition for services and functions. There is uncertainty associated with the institutions' compliance with new regulatory requirements. This applies in particular to PSD 2 and the new EU General Data Protection Regulation, which the institutions believe will require substantial changes in procedures and processes.

4.1.2 Data attacks

Financial institutions are concerned that data attacks are becoming more sophisticated, and point out that the methods and tools for making attacks have become more readily available. The NotPetya attack in 2017 is mentioned as an example. The attackers do not necessary attempt to penetrate an institution's defences directly, but smuggle in malware in software used by the institution.

The institutions state that massive resources are being used in the work of protecting their own operations. Measures such as security upgrading (patching), DMARC (e-mail protection) and Response Policy Zone (filtering of web traffic) are monitored closely and must be constantly adjusted and adapted if they are to function as intended. If not, the measures could impact on operational stability and lead to delivery deficiencies. The result can be downtime, long response times and service failures.

4.1.3 Expertise and capacity

A number of institutions report challenges associated with ICT expertise and capacity. The challenges are greatest in the areas of development and security, and in particular in encryption. The challenges presented by server and network operation are not as great.

4.1.4 Access control

Control of access to data and systems means controlling:

- employee accesses
- application and software accesses
- external user accesses
- accesses that attackers can acquire
- accesses of contractors and subcontractors, and which unauthorised persons could acquire
- attempts to escalate privileges
- unauthorised mapping of weaknesses (lateral movements)

A number of institutions regard access control as a significant challenge, and in 2017 some institutions discovered weaknesses in their access control. Good access management entails monitoring a number of areas and disciplines, and access control is only as strong as the weakest link. Large investments in strong control are wasted if there is one weakness the attacker can exploit.

A weakness of this kind may be that the security of business continuity systems is not updated, so that unsecured versions of software are released into production after a switch to the business continuity system, or software that the institution doesn't use, or uses very seldom, and the security of which has not been updated may be installed. The attacker can exploit a vulnerability of this kind as a port of entry for penetrating further into the institution.

4.1.5 Data leakages

A consequence of the access control challenge is data leakage from the institution. The institutions referred to cases where programming errors in the online bank led to information falling into the hands of unauthorised persons and to cases where account and customer information was sent in clear text by e-mail, even though e-mail is an unsafe means of communication. Also mentioned are cases of errors linked to use of the mail merge function, whereby e-mails were sent to the wrong recipient.

The institutions were concerned about data leakage. A provider of security services believes this constitutes a threat, as institutions risk substantial fines for breach of the new General

Data Protection Regulation (GDPR). The challenge concerns a possible increase in attacks, with threats to publish stolen personal data if the institution does not pay ransom money.

4.1.6 BankID

Some institutions report challenges presented by increasing numbers of cases where BankID does not function, or does not function satisfactorily. There has repeatedly been instability in connection with transmission of a message to a mobile phone that the user is required to approve (push messages).

4.1.7 Outsourcing and security

A growing number of institutions report outsourcing to cloud services. The institution gains access to a large community of expertise, and systems that are well tested and redundant. At the same time, interaction and interconnection in increasingly distributed service deliveries make end-to-end securing of services more demanding.

An increasing proportion of Internet traffic is encrypted (https). Decryption, re-encryption and final decryption at recipient's end lead to complicated operations (certificate administration) and errors.

A number of institutions mention that in order to avoid spoofing[44], institutions can protect their Internet traffic by using a technology called certificate pinning, whereby one or more public keys is linked to the Internet domain from which the service is delivered. However, this will fail if the Internet traffic is decrypted and monitored in a server set up between sender and recipient.

Several institutions report that it is challenging to establish sufficient sec urity to ensure that their service provider and provider's subcontractors deliver services that satisfy the institution's security requirements and requirements ensuing from acts and regulations.

A number of serious delivery deficiencies were detected in 2017. In some cases, institutions have changed their follow-up, and in some they have combined into customer groups that cooperate on follow-up of service providers.

4.2 Vulnerability questionnaire survey

As in previous years, Finanstilsynet conducted a questionnaire survey in 2017 on assessment of ICT vulnerability. Twenty-one institutions took part in the survey. Finanstilsynet asked

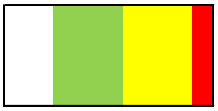
[44] Spoofing: falsification of sender identity

them to rate themselves with respect to their vulnerability to potential threats. The results are shown in the tables below. Green expresses low vulnerability for the institutions, yellow medium vulnerability and red high vulnerability. No colour indicates that the institution did not reply.

They were also asked to rate their vulnerabilities going forward, i.e. as increasing, stable or decreasing. The trend that emerges in the column on the far right in the tables below is an expression of the average of the assessments submitted. The interval –0.2 to +0.2 is indicated by a horizontal arrow and implies a stable trend. Arrows pointing up indicate that vulnerability is considered to be increasing (the interval +0.2 to +1), and arrows pointing 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.

Table 5: Support for strategic decisions

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Systemes evne til å hente informasjon fra eksterne og interne kilder og sammenstille og synkronisere informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering		→	→
2	Systemenes evne til automatisk å gi et totalbilde av risikoen, for eksempel slik at hvis en hjørnestensbedrift går konkurs, så varsler systemet automatisk om lån til ansatte i bedriften og lån til leverandører til bedriften, slik at vi kan vurdere å tapsavskrive på disse		→	→
3	Systemenes evne til å reflektere kundens evne til å betjene gjeld		→	→
4	Datakvaliteten i våre systemer og registre		→	→
5	Integrasjon og synkronisering mellom systemene		→	→
6	Når nye IT-løsninger skal utvikles, tar vi i betraktning behovene og løsningene til alle relevante avdelinger? Dette for å unngå utfordringer forbundet med "silo-løsninger", slik som omfattende vedlikehold av programmer, komplisert drift og utfordringer med synkronisering av data		→	→
7	Grad av kompleksitet i IT-systemene		↗	↗
8	Omfanget av feil og mangler i systemene		↘	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Source: Finanstilsynet

Some things do not change, including:

- Risk reporting is dependent on manual operations, with respect both to internal follow-up and management and reporting to authorities
- New, more integrated solutions increasingly expose weaknesses in integrations with existing core systems
- There are more integration points because of the increased functionality of self-service channels
- Increased requirements for communication among systems explain high and growing risk

- The increase in the system portfolio and in complex systems amplifies the risk of data quality deficiencies

Table 6: Operational irregularities

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Organisering, rutiner, stillingsbeskrivelse, rapportering og kontroll		↘	↘
2	Avtalene med leverandørene sikrer oss rett til innsyn i alle forhold som gjelder leveransen?		→	→
3	Test-systemene er "produksjonslike", dvs. at testdata, applikasjoner, programvare, styresystemer (SW) og maskinvare er det samme for test som i produksjon?		→	→
4	Vi gjør endringer i infrastrukturen ("ikke- funksjonelle" endringer) i trafikkstille perioder, og kan reversere endringen og rulle tilbake på kort tid hvis nødvendig?		→	→
5	Vår evne til å avdekke alle svakheter		→	→
6	Intrusion Detection og Intrusion Prevention, brannmur, antivirus, kontroll av web-trafikk, sikring av e-post, og andre tiltak for å sikre stabil drift		→	→
7	Logger og vår evne til å reagere på innholdet i loggene		↘	→
8	"Tikkende miner", dvs. komponenter som gradvis slites eller verdier som gradvis når nivåer som krever inngrep, og vi oppdager det ikke, for eksempel minnelekkasje, sertifikater som går ut på dato, elektroniske komponenter som slites, energiforsyning som "slites" (batterier, brennstoff til nødstrømsaggregat)		→	→
9	Vår evne til å avdekke avvik i datatrafikken (unormal belastning, unormale porter/protokoller, avvikende svartider) i driftsmønsteret og ta aksjon før skade		→	→
10	Vår beskyttelse mot dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)		→	→
11	Kvaliteten på kontinuitets- og katastrofeløsningene våre, jf. IKT-forskiften § 11		→	↘
12	Samarbeidsrutiner med leverandører		→	→
13	Leveransepresset vi er utsatt for i markedet gjør kvaliteten i løsningene ikke alltid er god nok		↗	↗
14	Tilgang på kompetanse, herunder kompetanse til å stille krav til leverandører og følge opp leveransene		↗	↗
15	Omfanget av endringer		↗	↗
16	Nye regulatoriske krav som gjør at vi må endre systemene våre		↗	↗
17	Vår kunnskap om hvor datalinjene går og redundans når det gjelder datalinjer		→	→
18	Tilgangskontroll, adgangskontroll og dual kontroll		→	→
19	Medarbeidernes årvåkenhet når det gjelder trusler og angrep		→	I/A
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Source: Finanstilsynet

The following are prominent:

- Balancing the implementation of major regulatory amendments, changing technology, business development and digitisation is challenging
- The complexity of administration and operations is growing, partly owing to an escalating rate of change

- The work associated with maintaining intrusion detection and prevention, firewalls, antivirus software, monitoring of web traffic, protection of e-mails and other measures to ensure stable operations is complex and time-consuming.
- Greater technical complexity and a wider range of services increases the risk of the security measures failing to detect attacks
- Greater security risk attributable to increased exposure of services – integration and transparency, data sharing
- Challenges ensuing from dependencies among services and service providers in the ecosystem (telecommunications, banking, ID)
- Large volumes of unstructured data (e-mail, Office documents, private files). Tightening up in connection with the GDPR
- The risk of being outcompeted in technology – new user experiences / new operators / new systems
- Balancing the administration of complex value chains and system portfolios against demands for frequent changes
- Migration / moving of portfolios from old to new technology
- Open banking and PSD 2; how will the market change? Great uncertainty concerning PSD 2
- It is difficult to recruit appropriate expertise in several areas. Access to crucial expertise is limited: security, development, the architecture of new technology
- Changes in expertise, transition to partnerships with expertise. Value chains are shifting towards partners through closer cooperation
- Transition to cloud solutions and standardised solutions that will reduce the complexity of serviced solutions
- Outsourcing by service providers makes monitoring more difficult
- Service providers face challenges relating to their subcontractors
- Business continuity (failover) systems do not function

Table 7: Data are not adequately protected

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Våre retningslinjer for klassifisering av strukturert (databaser) og ustrukturert (word, e-post) informasjon og beskyttelse av informasjonen		→	→
2	Tilgangskontroller – ansatte, konsulenter, leverandører, applikasjoner, software		→	→
3	Våre systemer for logging og evne til å reagere på innholdet i loggene		→	↘
4	Nettverkssegmentering, perimetersikring, kryptering		→	→
5	Sikring av data på bærbart utstyr		→	→
6	Ved terminering av avtaler om datalagring, må leverandøren dokumentere at data er fullstendig slettet?		→	→
7	Ustrukturerte data (dvs. data der brukeren selv vurderer behovet for å beskytte dataene) som e-post, presentasjoner, tekstdokumenter blir gjennomgått regelmessig med tanke på beskyttelse, eventuelt sletting?		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Source: Finanstilsynet

The following features appear to be prominent:

- Greater technical complexity and a wider range of services increases the risk of the security measures failing to detect attacks
- Professional attackers and more attacks necessitate increased resources and more stringent control
- Internal expertise: correct use of IT systems and data quality

Table 8: ID theft

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	En angriper tar over en brukerid og misbruker denne		→	→
2	Kontroll når det gjelder utlevering og bruk av logon-id og passord til kunder og medarbeidere (BankID, ansatte-ID, systembrukere, admin-brukere)		→	→
3	Kontroller som forhindrer "skimming" og "Card not present"-svindel		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Source: Finanstilsynet

Efforts targeting ID theft are characterised by the following:

- This is a priority area for the majority of institutions
- A number of institutions report that they are working on a new zone structure and new access regime
- Increased use of DMARC to prevent receipt of unauthorised e-mails; see 3.9.2.2

Table 9: Misuse of access to IT systems

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Tilgangskontroll		→	→
2	Våre rutiner når det gjelder tjenestedeling		→	→
3	Logging og varsling		→	→
4	Analyse av "mistenkelige" transaksjoner som tilbakevalutering, bevegelser på interne kontoer, overføring fra kunde til ansatt og tilbake		→	→
5	Overvåking av ansattes egenhandel		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Source: Finanstilsynet

Employees misuse access to data, either indirectly, by picking out potential target groups that can be defrauded, or directly, by taking money from accounts that are not adequately monitored.

The risk appears to have decreased slightly in 2017 compared with 2016.

Table 10: Money laundering

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Markedsovervåking		→	→
2	IT-systemenes evne til å samle informasjon om kunde, kunderelasjoner og kundeadferd (KYC– Know Your Customer)		→	→
3	Elektronisk overvåkning av transaksjoner og transaksjonsmønstre – presisjon i flagging av mistenkelige transaksjoner		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Source: Finanstilsynet

There is still uncertainty concerning the precision of flagging of suspicious transactions. The responses indicate that the institutions are making continuous efforts to improve the ability of their systems to detect suspicious transactions.

4.3 National assessments of the threat picture, and ENISA's

Published reports[45] with assessments of the threat picture in Norway single out ICT resource centres with state support, mainly from Russia and China, as a growing threat. The operators attempt to compromise and infiltrate Norwegian authorities and enterprises in order to obtain information about traditional political and military targets, and engage in industrial espionage. For the financial sector, industrial espionage implies a risk that information about Norwegian enterprises that is stored with banks and financial institutions may be compromised.

The operators' interest in energy companies and industrial control systems may indicate that the ambition of these operators is to be in a position to sabotage the electricity supply infrastructure. The risk of loss of electricity must be taken seriously, and is therefore included in the risk assessments and infrastructure and ICT action plans of Norwegian institutions and authorities.

In 2017, a number of attacks on Western democratic election processes were detected, which showed the potential impact and consequences of cybercrime. The network of the South-Eastern Norway Regional Health Authority was also found to have been hacked, which showed that operators from foreign states target Norwegian activities and systems that traditionally do not administer secret or sensitive information, and which have not previously been regarded as potential intelligence targets.

In 2018, the intelligence services anticipate that there will still be attempts at recruitment, with the aim of acquiring sources of information and agents for subjecting Norwegian enterprises to mapping and network attacks. Norwegian enterprises are also expected to be

[45] The Norwegian Police Security Service (PST): *Annual Threat Assessment 2018*, the Norwegian Intelligence Service's *Focus 2018*, the Norwegian National Security Authority's *Risiko 2018*

subjected to attempts to unlawfully acquire information and technology by the agents of foreign powers.

The collaboration established among authorities, police and ICT service providers has led to several cybercriminals being stopped, arrested and taken to court.

International cooperation has resulted in the exposure of several criminal networks and government-subsidised criminal activities, and their methods and instruments of attack.

ENSA's[46] report relates that cross-border and cross-sectoral measures are appropriate means of enhancing the quality and effectiveness of efforts to counter cybercrime. Teams specialised in security testing have been established for the financial sector in Europe, to put relevant institutions and institutions in a position to prevent attacks.

The reports also show that investment in ICT security measures and systems, both proactive and reactive, was record-high in 2017. They also show that cyber attacks have grown in number and complexity. The complexity consists of the attacks increasingly concealing their presence and their tracks, and being more adaptable to new tasks and changed premises in the victims' systems.

The motivation for most cybercrime is money. The use of virtual currencies to anonymise payments for blackmail and other criminal activities has proved an effective means of concealing actions.

[46] ENISA Threat Landscape Report 2017

5 Risk areas

Finanstilsynet's primary objective is to contribute to financial stability and smoothly functioning markets. Financial services cannot be provided without well-functioning ICT systems. The use of new technology and new digital solutions increases efficiency and helps to lower costs, but also entails increased vulnerability. Developments in cybercrime also increase vulnerability.

5.1 Financial infrastructure

The financial infrastructure consists of the payment system and security settlement system as well as the Norwegian Central Securities Depository (VPS), marketplaces and central counterparties. The infrastructure shall ensure that cash payments and transactions in financial instruments are registered, cleared and settled.

If payments cannot be made, completed or settled, important societal functions will cease to function satisfactorily after a short while. Sensitive information gone astray, or breach of rules for managing insider information may undermine confidence in marketplaces and the financial system. If criminals succeed in gaining access to large quantities of customer and account data and compromising them or making them inaccessible, this can create considerable challenges for an institution and could also impact financial stability. Institutions that operate on behalf of all or several financial institutions are particularly vulnerable. The institutions' efforts to achieve robust operational systems, including business continuity systems, disaster recovery and emergency planning systems, data recovery plans and ICT security, are essential parts of the work of safeguarding financial stability.

Today there are alternative means of payment that make parts of the payment system less vulnerable. Requirements have also been set for contingency plans for cash availability.[47] However, incidents in 2017 revealed that failure of management systems intended to ensure redundancy and business continuity in the institutions' operating systems had major consequences. Some incidents led to payment services being unavailable for a whole day for

[47] The Ministry of Finance has set out in regulations the obligation of the banks to have contingency systems to meet any increased demand for cash in the event of failure of the electronic payment systems. https://www.regjeringen.no/en/aktuelt/new-requirements-on-banks-contingency-arrangements-for-cash/id2598131/

more than 30 per cent of banking customers. This created great uncertainty, both among customers and in the market, concerning the institutions' ability to continuously deliver robust payment services and to execute payment orders.

BankID is an important component of the financial infrastructure, and the only permitted system for PKI-based digital signatures in banking. It is also used extensively outside the banking industry. Customers are not permitted to use alternative PKI-based digital signatures that could be used when BankID is down. In 2017, too, there were many BankID incidents.

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.

Finanstilsynet obtains a good, broad-based picture of the state of the Norwegian financial infrastructure through its supervisory activities and work in the Contingency Committee for Financial Infrastructure, which includes reviewing incidents in financial institutions and financial market infrastructures (FMIs).

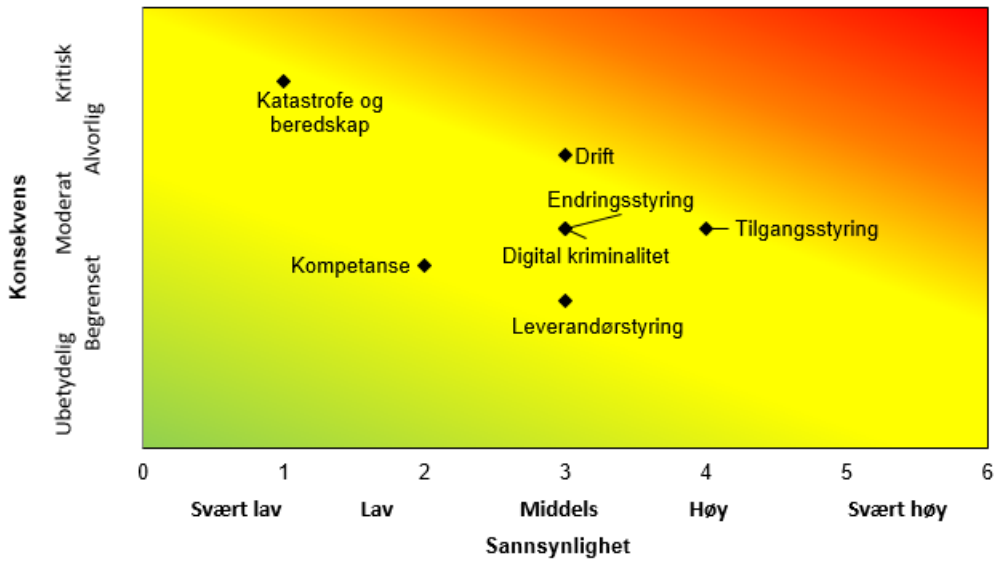
The regularity of clearing and settlement systems and communication with the international payment system SWIFT and the international settlement system CLS were also good in 2017.

Although there were incidents that made payment systems unavailable for long periods, and the availability of payment systems was somewhat poorer than in 2016, Finanstilsynet nonetheless considers the Norwegian financial infrastructure to be robust on the whole.

5.2 The institutions

Figure 6 below shows Finanstilsynet's assessment of the most central threats to and vulnerabilities of the institutions' systems. In the figure, the various risk areas are classified according to the probability of a negative incident occurring, and the consequences if the incident occurs.

Figure 6: Finanstilsynet' risk assessment



Source: Finanstilsynet

Finanstilsynet considers vulnerabilities in system operations, inadequate access control, inadequate change management and defence weaknesses to be the primary risks facing

financial institutions. Incidents in 2017 show that their system operations are not sufficiently robust. Inspections reveal deficiencies with respect to control of access to systems and data. Finanstilsynet also notes organisational, operational and technical weaknesses associated with institutions' ICT security work.

Vulnerabilities associated with vendor management, disaster recovery and emergency planning systems and inadequate competencies are also key risks.

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.

Establishing satisfactory risk management, including a sound risk assessment framework, presents a challenge to a number of institutions. Finanstilsynet believes this may be a contributory factor to some of the weaknesses that have been identified through supervisory activities. A critical review of the risk assessments is important for ensuring that major risks facing an institution are identified, analysed and evaluated.

The following is a more detailed account of the vulnerabilities in the institutions' ICT services that Finanstilsynet believes to be the most central. These are all vulnerabilities that may be a threat to secure, stable operations.

Operations

The institutions' services are based on digital solutions, and vulnerabilities ensuing from the fact that an institution's system operations are not 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 (network, servers, software,

power, premises, etc.) are not duplicated in the form of redundant systems, or the business continuity system has deficiencies that cause it not to function as intended.

The extent to which different service providers are integrated increases the risk of operating problems, partly because there are several systems involved in the service which may fail and thereby cause the service to be unavailable, and partly because the integration of many service providers makes it more complicated to maintain an overview of vulnerable components. New, more integrated solutions increasingly expose weaknesses when integrated with existing core systems. The extent of integration points among different systems is increasing, partly because of increased functionality in self-service channels.

The increase in the system portfolio in combination with complex systems also increases the risk of poorer data quality. The data structures are characterised by the fact that the same data are stored in several places. There is no "master" version of the data, but there are several versions, each of which is the "master" for its application domain. This makes synchronising all the versions challenging.

Deficiencies in the duplication of the system operations, faults in the system controlling transition to the duplicate solution, and human error are some of the causes of serious operating problems and service unavailability in 2017. A shortage of qualified personnel and challenges associated with incident management in collaboration with or among service providers contributed to a long recovery time. Some incidents were a result of capacity management deficiencies.

Finanstilsynet assesses the overall risk associated with system **operation systems** vulnerability as **medium**. The probability of undesirable incidents is assessed as *medium* and the consequences as *serious*. This is based on the following assessments:

- The probability of impaired data quality as a result 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 regarded as *medium* and the consequences as *serious*.
- The probability of operating problems that impact shared operational infrastructure is regarded as *medium* and the consequences as *serious*.
- The probability of service unavailability as a result of deficient capacity control is assessed as *medium* and the consequences as *serious*.
- The probability of system components in redundant systems failing as a result of inadequate monitoring 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*.

Disaster recovery and emergency planning systems

Vulnerabilities in disaster recovery and emergency planning systems constitute a risk if a serious incident occurs in the institution's system operations, including business continuity and high availability systems, that may make it necessary to employ the disaster recovery and emergency planning system.

Inadequate testing or failure to test the institution's disaster recovery and emergency planning system and emergency planning management, and inadequate evaluation of tests constitute a risk of the institution and its service providers not being adequately prepared, and thus not capable of dealing with a crisis or disaster.

In the event of a crisis, inadequate analyses of business continuity consequences constitute a risk of disaster recovery and emergency planning systems not being established with the necessary technical infrastructure and capacity. The absence of requirements relating to restoration of operations (recovery time objective – RTO) and how much data can be lost (recovery point objective – RPO) are also factors that constitute a risk of the solution not being correctly dimensioned. Failure to perform security updates of disaster recovery systems increases the risk of digital attacks when the institution is in a particularly vulnerable situation.

Finanstilsynet's experience is that institutions are not sufficiently prepared for a serious crisis or disaster. Lack of, or an inadequate disaster recovery and emergency planning system is a challenge for a number of institutions, and Finanstilsynet also finds that institutions generally face challenges when it comes to handling serious operational disruptions. This is a concern that is intensified if a crisis or disaster occurs.

Finanstilsynet regards the probability of serious incidents occurring that require the implementation of disaster recovery and emergency planning systems as *very low*. Nonetheless, the consequences of the system not functioning according to expectations is regarded as *critical*.

Finanstilsynet assesses the overall risk associated with vulnerability in **disaster recovery and emergency planning systems** as **high**. This is based on the following assessments:

- The probability that the institution's system has not been established in accordance with the institution's needs, as a consequence of inadequate impact analyses and requirements, is regarded as *medium*, and the consequences if the system is implemented as *critical*.

- The probability of institutions not being adequately prepared for a serious situation, as a result of inadequate and unrealistic exercises, is considered *high* and the consequences as *serious*.
- The probability of the system not functioning as expected, as a consequence of the inadequate conducting and evaluation of technical tests, is assessed as *medium* and the consequences as *critical*.
- The probability of inadequate security updates of systems is regarded as *medium* and the consequences as *serious*.

Expertise

Vulnerabilities due to lack of access to expertise in operations, architecture and ICT security, and inadequate management of competencies constitutes an operational risk. Inadequate expertise may also lead to an institution using the wrong technology and/or failing to see the possibilities offered by new technology.

Finanstilsynet has noted that the institutions are challenged when it comes to securing necessary and crucial technological expertise in areas such as security, architecture and development, and to understanding and applying new technology. Establishing a balance between maintaining the expertise required for daily operations and the expertise necessary to develop new solutions is demanding.

Finanstilsynet assesses the overall risk linked to vulnerabilities associated with **expertise** as **low** to **medium**. The probability of undesirable incidents arising or of undesirable incidents not being dealt with adequately due to lack of expertise is regarded as *low* to *medium* and the consequences as *limited* to *moderate*. This is based on the following assessments:

- The probability of inadequate management of expertise resulting in loss of and/or lack of expertise to maintain proper operations is regarded as *medium* and as having *moderate* consequences.
- The probability of operational disruptions and service unavailability as a result of inadequate expertise is assessed as *low* and the consequences as *moderate*.
- The probability of breaches of data security as a result of inadequate access to security expertise is assessed as *low* and the consequences as moderate.
- The probability that inadequate expertise in an institution regarding the services that providers operate and develop will result in breaches of laws and regulations is assessed as *medium* and the consequences as *moderat*e.

Vendor management

Vulnerabilities as a result of lack of or inadequate service provider follow-up, administrative and operational, represent a risk of breach of compliance with agreed requirements and of the provisions of the ICT Regulations. They also includes a risk that the service provider has not established adequate internal control, which puts outsourced services at risk of being in

breach of data security. This in turn represents a risk of failure to detect serious economic problems or inadequate resources on the part of service provider that may threaten the service provider's ability to deliver. Unclear roles and responsibilities between institution and service provider, and among service providers in the value chain, constitute a risk of serious incidents not being resolved in time.

Undesirable service provider dependency may arise as a result of weakness in vendor management, where the provisions of the agreement on transfer of services to another provider are not sufficiently binding. This implies a risk of prolonged service instability during the process of transferring the service to another service provider, particularly where the transfer is a result of the service provider not meeting the delivery requirements.

In the course of its supervisory activities in 2017, Finanstilsynet has noted several factors that constitute a risk that institutions will not detect deficiencies in their service providers' internal control.

Institutions report that it is challenging to establish sufficient security to ensure that their service provider and the provider's subcontractors deliver services that satisfy the institution's security requirements and requirements pursuant to laws and regulations. It is also challenging for the institutions to anchoring their security requirements with their service providers.

The interaction between institution and service providers in connection with incidents and changes is challenging, and in some cases institutions have inadequate knowledge and understanding of what the outsourced service comprises.

Finanstilsynet assesses the overall risk associated with **vendor management** vulnerability as **medium**. The probability of undesirable incidents is assessed as *medium* and the consequences as *limited.*

This is based on the following assessments:

- The probability of substantial deficiencies in the service provider's internal control not being detected by institutions is assessed as *medium* and the consequences as *moderate*.
- The probability of security breaches occurring as a result of inadequate monitoring and establishment of security requirements in service providers is assessed as *medium* and the consequences as *moderate*.
- The probability of an unacceptably long recovery time in the event of seriously disrupted operations as a result of unclear roles and responsibilities in the cooperation with service providers is regarded as *medium* and the consequences as *moderate*.

- The probability of service unavailability as a result of deficient monitoring of service quality is assessed as *low* and the consequences as *moderate*.
- The probability of undesirable service provider dependency as a result of inadequate regulations (for example exit provisions) 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 institution's outsourced services is assessed as *medium* and the consequences as *limited*.
- The probability of the lack of risk assessments (periodic) leading to failure to detect weak service provider sustainability due to a demanding liquidity situation (risk of bankruptcy), an unsatisfactory resource situation, or other factors that may threaten the service provider's ability to deliver, is regarded as *low* and the consequences as *moderate*.

Access management

Vulnerabilities relating to inadequate access management constitute a risk of data security breaches, including breach of confidentiality, integrity and availability.

In the course of its activities in 2017, Finanstilsynet noted several factors that have resulted in this type of breach, or detected or observed factors that represent a risk of a breach occurring.

Access management, in the form of proactive control of access to systems and technical infrastructure for both the institution's own employees and those of service providers, is a challenge to the institutions. Finanstilsynet has also detected weak control of personnel with extended rights among the institution's service providers. Institutions have limited control of information that is sent from them by e-mail or copied onto memory sticks.

The potential consequences of identified vulnerabilities are many and include: confidential or classified information falling into the hands of unauthorised persons, authorised changes being made in customer data or unauthorised changes in payment transactions. The results of unauthorised actions may be system unavailability or serious operating problems. The vulnerabilities may result in harm to the institution and its customers and / or to their being severely fined for breach of rules and regulations.

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

- The probability of confidential and / or classified information going astray as a result of employees' sending e-mails or copying to memory sticks is regarded as *high* and the consequences as *moderate*.

- The probability of confidential and / or classified information going astray as a result of service provider's security breaches is regarded as medium and the consequences as *serious*.
- The probability of employees or service provider's employees conducting unauthorised transactions or changing a transaction is assessed as *low* and the consequences as *moderate*.
- The probability of the institution's employees illegally altering data is assessed as *low* and the consequences as *limited*.
- The probability of employees of service provider or provider's subcontractors breaking rules in their performance of operating tasks is assessed as *medium* and the consequences as *serious*.

Change management

Vulnerabilities associated with inadequate change management represent a risk of unauthorised changes occurring, and of changes with vulnerabilities or deficiencies 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 as a consequence of overly weak governance.

In the course of its activities in 2017, Finanstilsynet noted challenges associated with institutions' change management. Incident reports to Finanstilsynet have revealed that serious incidents occurred as a result of changes. This applies to both functional and non-functional changes.

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

- The probability of service unavailability as a result of non-functional changes (changes in the configuration of operating components) is assessed as *medium* and the consequences as *moderate.*
- The probability of functional changes (software) introducing vulnerabilities into institutions' defences is assessed as *low* and the consequences as *moderat*e.
- The probability of the escalating rate of change leading to new services being released into production without the necessary quality is assessed as *high* and the consequences as *moderate*.
- The probability that institutions' uncertainty with respect to the PSD 2 requirements results in necessary changes not being made is assessed as *medium* and the consequences as *moderate*.

Cybercrime

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, monitoring or technical security measures, constitute a risk of potential harm to the institution and its customers by cybercriminals.

The institutions' security framework, training of employees, security requirements in contracts with service providers and organisation of security form the basis for a good security culture in the work of preventing cybercrime.

Attacks take many forms. Examples are ID theft, social engineering (see 3.9.2.1) and attacks on service, such as DDoS attacks.

In 2017, Finanstilsynet noted organisational, operational and technical weaknesses that result in vulnerability to intentional and unintentional attacks and errors. Particular mention is made of unclear responsibilities, inadequate security updates, inadequate security testing and lack of systems to identify false e-mails.

External assessments of institutions' network infrastructure identified major security weaknesses due to lack of segmentation, including inadequate zoning of enterprises' internal and external networks. Vulnerabilities were found where a service provider's employees were able to acquire the user names and passwords of employees in several institutions.

With regard to payment cards, Finanstilsynet noticed that some of the biggest card issuers have not implemented functionality in accordance with guidelines for secure online payments.

Finanstilsynet assesses the overall risk associated with vulnerabilities in institutions' defences that may lead to harm as a result of **cybercrime** as **medium**. The probability of undesirable incidents is assessed as *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of institutions being impacted by malware is assessed as *medium* and the consequences as *serious*.
- The probability of classified or confidential information going astray is assessed as *medium* and the consequences as *moderate*.
- The probability of vulnerabilities in the institution's defences not being detected as a result of inadequate expertise and security testing is assessed as *medium* and the consequences as *serious*.
- The probability of little-used systems in the institution's network not being security-updated is assessed as *medium* and the consequences as *moderate*.

- The probability of employees with authorisations being identified by criminals and coerced into performing unauthorised actions is assessed as *medium* and *the* consequences for the institution as *limited*.
- The probability of one or more of the institution's customers revealing log-on information for payment services as a consequence of social engineering is assessed as *high* and the consequences as *limited*.

5.3 Users

The use of digital systems leaves traces. This is a challenge to privacy. The traces can be used for profiling, blackmailing, mapping, ID theft and engineering. The use of cash ensures that a customer's consumer behaviour remains a private matter. However, an increasing number of merchants no longer accept cash payments, and the number of ATMs is being reduced.

Digital systems predominate. Non-digital services are being priced steadily higher, to give customers incentives to use digital services. A number of customers do not have the skills and capability necessary to use the digital services. According to Statistics Norway's publication on ICT in households48, over 400,000 people feel excluded because of technological developments.

An estimated 220,000 bank customers in Norway do not use digital banking services, including paying bills and making account transfers with the aid of online or mobile banking. They are called "analogue customers", and use traditional payment services such as mail giros and over-the-counter payment.

The pricing of traditional services and/or the fact that many people are reluctant or are not capable of using digital services has led to a number choosing to leave the payment of bills to others, by turning over their digital ID to family members or others they trust who are users of the digital services. Finanstilsynet itself believes this constitutes a risk of misuse of trust, particularly where online banking is established for the customer and the customer's log-on information is used by the trusted person.

The banks, for their part, have focused on helping this customer group to make the transition from analogue to digital systems by providing information and courses. Finanstilsynet has the impression that these initiatives have helped a number to cross the threshold into the digital world.

[48] https://www.aftenposten.no/norge/i/gPp38L/Norge-er-i-digitaliseringstoppen-400000-mennesker-star-utenfor?spid_rel=2

At the same time, there are still customers who will remain analogue because the digital systems are too complicated, they want anonymity, or because they simply do not want to be digital.

6 Monitoring by Finanstilsynet

6.1 Key areas for Finanstilsynet's ICT supervision

Supervisory activities are risk-based. Finanstilsynet wishes to focus attention on the supervisory agencies that have the greatest influence on financial stability and smoothly functioning markets. Institutions' ICT risk will be assessed, and their own annual assessments of ICT risk will be reviewed. Prioritised review topics will be ICT governance, the institutions' emergency response work for business continuity and crisis solutions and testing thereof, and outsourcing of ICT systems to detect money laundering and financing of terrorism. Emphasis will also be placed on supervision of the organisation of ICT/cyber security work, the security of institutions' ICT systems, and the organisation of their monitoring.

Other relevant topics for inspection are the institutions' control of access to systems, especially systems that contain sensitive information, and the development of new systems that involve new technology. Institutions that make major changes in their ICT function, thereby potentially increasing their operational risk, will be subject to scrutiny.

Supervisory activities will also extend to the institutions' risk evaluations in connection with outsourcing of ICT, the quality of contracts and monitoring of contracts between institution and service provider.

6.2 Work with payment systems

Finanstilsynet will monitor the institutions' payment services with respect to the regulations[49] to the Payment Systems Act and compliance with the duty of notification. There will also be follow-up with respect to the regulations on interchange fees in card schemes. When the revised EU Payment Services Directive (PSD 2) is transposed into Norwegian law, Finanstilsynet will make it the basis for its monitoring of institutions' payment services.

Compliance with guidelines for secure online payments will be monitored through spot testing and penetration testing of online systems.
Collaboration with Norges Bank will continue.

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

6.3 Follow-up of incidents

There was a negative trend as regards serious incidents in 2017 compared with previous years. In 2018 Finanstilsynet will follow developments closely and consider the need to take action. Emphasis will be placed on identifying causes, and steps will be taken to prevent repetition.

Incidents involving serious non-conformities 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. This includes reviewing incident scenarios and determining whether the responsibilities in crisis situations are sufficiently clear. Emergency response exercises are planned for 2018 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 in cooperation within the national regulatory framework for management of ICT security incidents.

Finanstilsynet will align its contingency work and management of ICT security incidents with the framework of the Norwegian National Security Authority (NSM) for managing ICT security incidents[50]. In line with the framework, there are plans to formalise cooperation between Finanstilsynet and Nordic Financial CERT to establish a sectoral response group (SRM) for the part of the financial sector that Finanstilsynet supervises. Finanstilsynet has the formal role as SRM and will perform this function collaboration with Nordic Financial Cert according to agreed rules on exchange of information.

6.5 Monitoring of the cybercrime threat picture

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

- the digital threat picture
- contingency preparedness work targeting digital vulnerability and security
- how institutions organise and follow up their security work
- changes in payment mediation through the use of new technology (FinTech) and for cross-border activities

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

6.6 Consumer protection

Finanstilsynet will stress the importance of institutions making sound provision for their customers' security. There will also be monitoring to ensure 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 line with the regulations that enable consumers to protect themselves, for example by blocking cards for online use; see 3.1.5.

In the event of incidents, Finanstilsynet will check that the institutions provide users with information depending on how they are affected and how the institution or user can mitigate the situation themselves.

Glossary

Term/abbreviation	Meaning
3-D Secure	3-D Secure is an XML-based protocol used in internet payments. It provides an extra layer of security to card transactions by verifying the user in relation to the card issuer, irrespective of the payee. In connection with use of Visa, which developed the protocol, it is called Verified by Visa.
AIS	Account Information Supplier
AISP	Account Information Service Providers (in PSD 2). Operators who can retrieve data from bank accounts on behalf of customers
AML	Anti-Money Laundering
API	Application Programming Interface
App	Application – on a tablet or mobile telephone
BFI	Contingency Committee for Financial Infrastructure. Coordination committee for financial sector crises. Chaired by Finanstilsynet.
Blockchain	List of data/transactions, called blocks, that are linked together into a chain and secured by means of encryption.
CEO attacks	Internet attacks that use CEO fraud
CEO fraud	Fraudster claiming to be the head of a company. Also called Fake President Fraud or Business E-mail Compromise
CERT	Computer Emergency Response Team Expert group that handles Internet security breaches
Cloud computing	Data processing distributed 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.
Cloud computing services	Cloud-based platform, infrastructure, software or storage services
CLS	Continuous Linked Settlement. International settlement system for foreign exchange trading
CNP	Card Not Present. Fraud with the aid of stolen card data, mainly in connection with online trading.

CPMI/IOSCO	The Committee on Payments and Market Infrastructures / International Organization of Securities Commissions
CVC code	Card verification code. The last three digits on the reverse of most credit cards.
Data security breach	Breach of integrity, confidentiality or availability
DDoS attacks	An Internet attack that overloads a server by directing a huge amount of traffic to the server, usually by means of a botnet. The purpose is to prevent normal access by ordinary users.
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DSOP	Digital cooperation between the public and the private sector
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 internal market
EIOPA	European Insurance and Occupational Pensions Authority
EMIR	European Market Infrastructure Regulation
ENISA	European Union Agency for Network and Information Security
ESMA	European Securities and Markets Authority
Fintech	Financial technology
FMI	Financial Market Infrastructure. FMI is a collective term for financial market infrastructure institutions such as interbank systems, securities settlement systems, central counterparties, securities depositories, data warehouses etc.
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a service (cloud service)
ICO	Initial Coin Offering
ISP	Internet Service Provider - supplier of Internet access and domain names
Malware	Collective name for software with “hostile intent” such as viruses, Trojans, ransomware etc.
MIF Regulation	The Multilateral Interchange Fee Regulation. Regulation (EU) 2015/751 on interchange fees for card-based payment transactions

MIFID II	Directive on Markets in Financial Instruments is applicable to securities firms, regulated markets, data reporting services and trading in commodities derivatives and emission quotas.
NBO	Norges Bank's Settlement System.
NICS	Norwegian Interbank Clearing System
NIS Directive	Network and information systems. EU directive designed to secure a high common level of network and information security in the EU
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.
PaaS	Platform as a Service (cloud service)
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.
PIS	Payment Initiation Services
PISP	Payment Initiation Service Providers. Denoted PISP under PSD 2. Parties who can initiate payments on behalf of customers.
PKI	Public-key infrastructure. Consists of hardware, software, procedures, guidelines and personnel necessary to create, manage, distribute, use, store and revoke digital certificates.
PSD 2	Revised Payment Services Directive 2015/2366/EU
Ransomware	A type of malware that restricts access to infected ICT systems and demands a ransom
RegTech	Technological solutions intended to aid financial institutions to improve risk management and to comply more effectively with regulatory requirements.
SaaS	Software as a Service (cloud service)
SMTP servers	Simple Mail Transfer Protocol servers. Used to send and receive external mail.
Spoofing	Falsifying the address of a sender, for example of an e-mail
SSL	Secure Sockets Layer. An older encryption method, now replaced by TLS.
STIP	Stand-in processing. If the operations centre for handling transactions does not achieve contact with a card-issuing bank/credit card company, the operations centre, Nets, for example, can authorise processing or payment on behalf of the bank. The same applies to

	Visa and MasterCard International. In situations like this, individual limits apply that may vary from one card to the next
Strong authentication	Authentication employing several methods, e.g. pin code + password
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFIT	Taskforce on IT Risk Supervision – EBA working group
TFPS	Taskforce on Payment Services – EBA working group
TLS	Transport Layer Security. A protocol that is used between e-mail servers to encrypt messages and deliver them safely. Prevents unauthorised viewing and falsification between e-mail servers
TPP	Third Party Providers. Term from the PSD 2 Directive. These are service providers that provide payment services and that do not normally operate payer's or payee's accounts
TRS	The transaction reporting system of investment firms
xID	xID supplements BankID for websites and services that require simple logging on, a safer and better option than user name and password
XML	Extensible Markup Language. Data exchange technology

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

05.2018