



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

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

RISK AND VULNERABILITY ANALYSIS

2016



Risk and Vulnerability Analysis 2016

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

Finanstilsynet, 26 April 2017
English translation as of June 2017

Table of Contents

1	INTRODUCTION.....	3
2	SUMMARY	4
2.1	Finanstilsynet's findings and observations	4
2.2	Financial institutions' assessments	7
2.3	Regulatory changes	7
2.4	Current areas of risk	8
3	FINANSTILSYNET'S FINDINGS AND ASSESSMENTS.....	9
3.1	Payment systems	9
3.2	Banks	18
3.3	Securities	20
3.4	Insurance	23
3.5	Estate agencies – settlement	24
3.6	Monitoring of compliance with anti-money laundering rules	24
3.7	Joint efforts by the financial industry	25
3.8	Changes in outsourcing	27
3.9	Incidents reported in 2016	28
3.10	Observations of digital crime (cybercrime)	31
3.11	Developments in financial technology	32
4	THE PARTICIPANTS' RISK ASSESSMENT	35
4.1	Interviews	35
4.2	Questionnaire on vulnerability	37
4.3	National assessments of the threat picture	40
5	REGULATORY CHANGES	42
5.1	Coordination within the EU and changes in EU rules and regulations.....	42
5.2	Changes in the Norwegian regulatory framework	45
6	RISK AREAS	48
6.1	Financial infrastructure.....	48
6.2	The institutions	50
6.3	Users and consumers	54
7	MONITORING BY FINANSTILSYNET	56
7.1	Key areas for Finanstilsynet's ICT supervision.....	56
7.2	Work with payment systems.....	56
7.3	Follow-up of incidents.....	56
7.4	Contingency preparedness	57
7.5	Monitoring of the threat picture associated with cybercrime	57
7.6	Consumer protection	57
8	GLOSSARY	58

1 Introduction

The Financial Supervisory Authority of Norway (Finanstilsynet) performs an annual risk and vulnerability (RAV) analysis of the financial sector's use of ICT. The purpose of the report is to describe risks and vulnerability relating to financial stability, individual institutions and individual consumers.

Through its supervisory functions, Finanstilsynet maintains a broad network of contacts with financial institutions, industry associations, service providers, standardisation bodies and national and international authorities. The report makes an assessment based on these sources of the potential impacts of identified risks on the financial sector in Norway.

The report provides an up-to-date picture of the risks inherent in the financial sector's use of ICT and payment services, summarised in chapter 2 of the report.

Chapter 3 presents an overview of Finanstilsynet's findings and observations in 2016. 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 national assessments of the risk picture of relevance to the financial industry are cited.

Regulatory amendments that could necessitate substantial changes in financial institutions' system solutions are described in chapter 5.

Chapter 6 contains a summary of Finanstilsynet's overall assessment of the risk picture in 2016 based on findings, observations and trends. The assessments focus on 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 7 describes the areas to which Finanstilsynet will pay particular attention in the future.

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

2 Summary

In 2016 there were no serious ICT incidents that had consequences for financial stability. Compared with the previous year, there were fewer incidents with consequences for individual enterprises or consumers. The number of incidents of fraud also declined. However, losses in NOK on payment cards and online banking fraud continued to increase in 2016.

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

2.1 Finanstilsynet's findings and observations

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

Payment systems

Finanstilsynet considers payment systems to have been generally robust and stable in 2016. Nonetheless, there is room for improvement. In several financial institutions, deficiencies were observed in capacity monitoring, capacity management and disaster recovery plans. Improvements can also be made in operational risk management.

As new payment solutions are developed, the vulnerability and consequences of deficient operating systems, the inadequate quality of testing in connection with changes and inadequate capacity monitoring and management also increase. This applies both to new systems and in connection with the further development of existing payment systems.

Changes in payment systems are driven by the entrance of new operators, new services offered by current operators through existing channels, and the establishment of new partnership constellations between banks or between banks and new operators.

Losses in NOK related to payment card transactions rose by 9.5 per cent. In 2016, losses were largely related to Card-Not-Present fraud, which alone increased by 39 per cent. The number of cards involved rose by 52 per cent. Total estimated costs related to card fraud (direct losses and processing costs) increased by 28 per cent, to NOK 428 million, of which direct losses amounted to NOK 206 million.

There was extensive online banking fraud, and related losses rose by 48 per cent to NOK 18.6 million. The fraudulent activity primarily targeted the corporate online banks. FinansCERT reports that many attacks were stopped.

Finanstilsynet does not know of any fraudulent mobile payments, despite the growing level of threat.

Banks

In 2016, banks continued to undergo major change processes in the ICT area, but the changes were generally carried out without significant consequences for operational stability. Towards the end of 2016 and at the start of 2017, however, there was a decline in operational stability.

The risk of digital attack is on the rise, and efforts to strengthen ICT security should be further intensified. Finanstilsynet sees a need to improve the quality of system access management. As far as contingency preparedness systems are concerned, Finanstilsynet has noted that the consequences of the failure of one or more applications have not been sufficiently assessed.

Implementation of the anti-money laundering rules' requirement that customer screening controls be updated when sanctions lists are amended¹ poses a challenge. Finanstilsynet has also observed that the electronic monitoring scenarios are inaccurate. This results in a large number of false positive identifications, making it necessary for banks to put in place extensive controls to distinguish them from genuine identifications.

Securities

The growing outsourcing of ICT systems with sensitive information, coupled with the fact that the information is concentrated in a small number of operating companies, poses challenges when it comes to protecting sensitive information. In the light of the increasing threat from external agencies, better protection is required for sensitive information.

Insurance

Many insurance undertakings still need to improve their risk analyses in order to obtain an accurate picture of the overall risk attached to the institution's use of ICT. In Finanstilsynet's experience, the risk assessments are often fragmented and thus not an effective risk management tool. The IT risks related to outsourced activities have often been inadequately assessed and are not always included in the annual reviews of overall IT risk.

Outsourcing notifications

Operators outsource ICT services to service providers whose service portfolio has not traditionally included development or operating services for the financial industry. In a number of cases, when processing outsourcing notifications, Finanstilsynet found that the agreements were not in compliance with the requirements of the ICT Regulations. Under pressure from Finanstilsynet and the financial

¹ Including the UN Consolidated Sanctions List and the EU's consolidated list of persons, groups and entities subject to EU financial sanctions.

industry, these new service providers have adapted their contracts to bring them into compliance with the regulations.

Incidents

The number of incidents reported is declining, and the availability of payment systems and customer-facing services was higher in 2016 than in the previous year. Conversely, the volume of fraud attacks increased. In 2016 more financial institutions were the target of attacks with demands for ransom (ransomware).

Together with the provision of more payment services for mobile devices, in particular BankID, telecom suppliers have acquired greater significance for the availability of payment services.

Cybercrime

Criminals are increasingly using phishing and social engineering to penetrate the systems of financial institutions, both to retrieve sensitive information and to manipulate payment orders. It is essential that financial institutions protect themselves against cyber attacks. The number of distributed denial-of-service (DDoS) attacks remains high, but the institutions' defences are effective. There have been some ransomware attacks. To Finanstilsynet's knowledge, no ransom has been paid.

A new type of fraud has been observed, in which a virus is planted in websites naturally visited by employees of financial institutions (waterholes). The virus is then transmitted to the computer systems at the employee's workplace, where it provides access that can be used by cybercriminals.

New technology

FinTech is a collective designation for various ways of changing and/or influencing traditional financial services through the use of technology, often solutions developed by technology companies. A multitude of new operators have entered the financial market, either as competitors of or in collaboration with existing operators. In practice, the Norwegian financial industry has been engaged in technological development since it first began to use IT in its operating systems.

Some countries are experimenting with a "regulatory sandbox", where new solutions (FinTech) are subject to somewhat more relaxed regulatory requirements during a start-up period, provided that the solutions are closely monitored by the supervisory authorities. After the start-up period, ordinary rules and regulations apply. This type of sandbox has been established in the UK and Singapore, among other countries. At present, the Norwegian regulatory framework does not allow such solutions. However, Finanstilsynet offers guidance with regard to both rules and regulations and the planned services.

Distributed Ledger Technology (DLT) is one of the technologies that is expected to contribute to further digitalisation and rationalisation of financial sector processes; see further details in 3.11.2. Although today's solutions are neither many nor visible, the technology is highly relevant as a foundation for the development of new solutions, for example for interbank money transfers.

The use of DLT is being examined by the Norwegian central securities depository Verdipapirsentralen ASA (VPS), in a joint project with Deutsche Börse, with a view to developing a cross-border system for furnishing collateral. Research and development projects have also been established in several banks and IT companies.

2.2 Financial institutions' assessments

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

- inadequate focus on security in the design of solutions
- security and access management
- protection of corporate information
- complexity of ICT systems
- scope of changes and implementation of regulatory requirements in systems
- cybercrime and system penetration
- disruptions in BankID availability, particularly on mobile devices

Other areas of threat identified by the institutions are the supply of qualified personnel, inadequate knowledge of management and control of the use of cloud-based solutions, losses arising from the unauthorised use of cards in online or telephone shopping (Card Not Present) and the fact that ICT systems do not provide satisfactory support for decision-making, customer service or administrative processes.

Market expectations of new, simpler solutions constitute a risk in the sense that insufficient time is allocated for testing, particularly of capacity and response time.

Several financial institutions also see a risk of their being unable to develop systems with high enough precision in identifying suspicious transactions or data of high enough quality to satisfy the "Know Your Customer" requirement.

2.3 Regulatory changes

In 2016, a number of EU processes related to proposals for new, or amendments to existing, directives, regulations, technical standards and guidelines were carried out. These will affect Norwegian institutions as and when they are transposed into Norwegian legislation. The regulatory changes will necessitate changes in financial institutions' systems or IT processes and procedures in several areas.

The most important regulatory change is the EU's new Payment Services Directive (PSD 2) and the regulatory technical standards that have already been or will be established. Other major regulatory changes are the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, the EU Directive on the Security of Network and Information Systems, a new agreement on the transfer of personal data between the EU/EØS and the US, the proposed new national regulatory framework on anti-money laundering and a Regulation on interchange fees for card-based payment transactions.

2.4 Current areas of risk

Financial infrastructure

Finanstilsynet considers Norway's financial infrastructure to be robust. Stability was good in 2016, on a par with 2015, even though incidents occurred that resulted in unavailable payment solutions, as a result of which sensitive information could have gone astray.

Financial institutions

Finanstilsynet considers unlawful access to systems and data, data leaks and cybercrime to be the primary threats to and vulnerabilities in financial institutions' systems. Complex operations, concentration risk, network faults are also key threats and vulnerabilities. Other areas of risk are inadequate business continuity systems, insufficient expertise and capacity, complex system portfolios and faults arising in connection with system changes.

Consumers

Consumers who trade actively through electronic securities trading systems are vulnerable to loss of access to the system, while professional operators often have access to alternative electronic trading systems for the execution of transactions.

Some groups of consumers encounter difficulties when digitalisation results in the termination or complicates the use of manual payment services.

The failure of payment service providers to comply with guidelines on the security of internet payments reduces consumers' possibilities of protecting themselves against fraud.

3 Finanstilsynet's findings and assessments

This chapter presents findings and assessments based on Finanstilsynet's work with IT and payment services in 2016. The chapter describes observations from IT inspections, incident reports, notifications of changes in outsourcing agreements, notifications of new payment services and changes in existing services and other supervisory activities.

Trends that in the longer term are considered likely to be of significance for financial institutions' use of ICT, and that could result in changes in the risk and vulnerability situation of both institutions and consumers, are also described.

In Finanstilsynet's general assessment, there were no threats to financial stability and the smooth functioning of markets in 2016.

3.1 Payment systems

3.1.1 General comments regarding payment systems

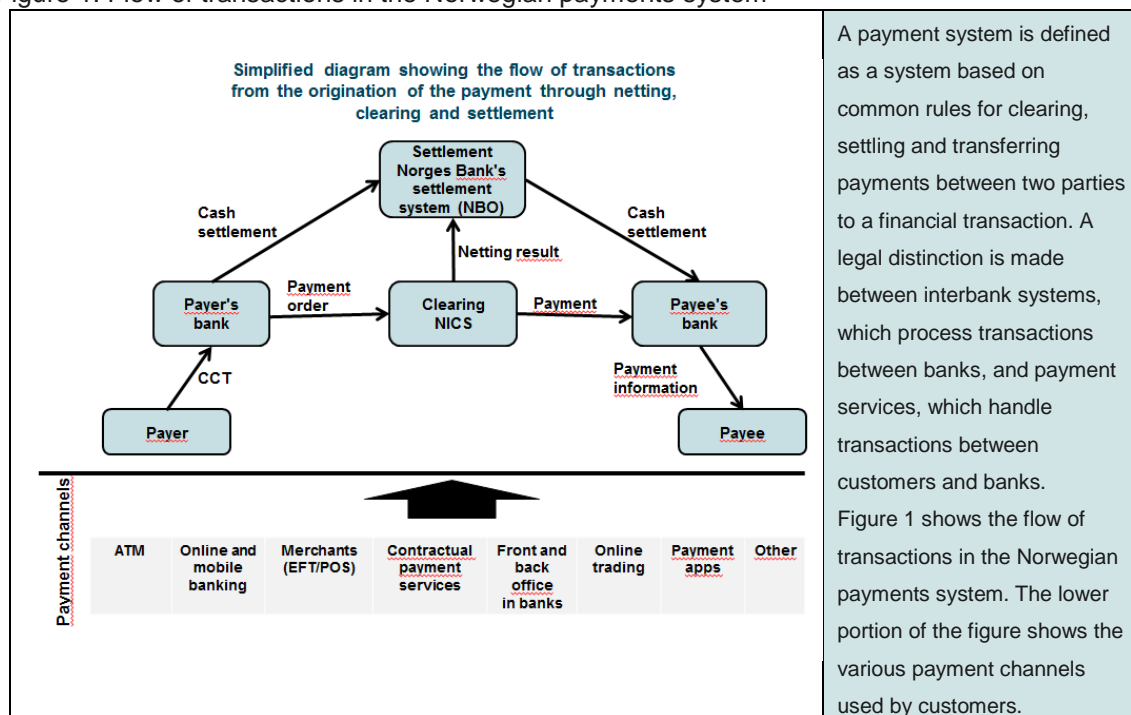
Financial stability means that the financial system is sufficiently robust to execute payments, channel funds and redistribute risk in a satisfactory manner. Effective, robust and stable payment systems are a fundamental prerequisite for financial stability and well-functioning markets.

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. The Financial Contracts Act is designed to safeguard consumer interests and protect consumer security and rights. Relevant regulatory changes relating to payment systems are described in chapter 5.

3.1.2 Management and control of risk and vulnerability in payment systems

As new payment solutions are developed, both as an alternative to cash payments and for already established electronic payment systems, the vulnerability of operating systems and the consequences of deficiencies in such systems, the inadequate quality of testing in connection with changes and inadequate capacity monitoring and management also increase. The risk factors also apply to existing payment solutions, where both payment services and the technologies used are constantly evolving, resulting in an ongoing need for modifications.

Figure 1: Flow of transactions in the Norwegian payments system



Source: Finanstilsynet

The rapid rate of change is in itself a considerable risk. It is therefore important that financial institutions carry out thorough risk assessments in connection with payment services², with regard to both operational risk related to service operation and maintenance and security risk related to unauthorised use of the services. In addition to ensuring that the services are protected by logical and physical security measures and that information is adequately protected, the institutions must ensure a high level of quality in both the operating systems and in associated processes that might affect operations.

Finanstilsynet has noted that several financial institutions, particularly the large ones, have invested considerable effort in their operating and contingency preparedness systems. Both more operating sites and redundant operating systems are used to reduce the institutions' vulnerability to irregularities in payment services.

In 2016, however, Finanstilsynet observed a number of incidents that show that the quality of the work of certain institutions in these areas is unsatisfactory. In particular, inadequate capacity management appears to be the cause of a range of incidents. Several incidents were also observed where the redundancy of operating systems, which is intended to ensure the continuity of these systems, has not functioned satisfactorily when irregularities occur.

² See the Payment Services Directive

It is a management responsibility to ensure that the institution's management and control of payment services accord with the pivotal role played by payment services in a smoothly functioning digital economy. The institution is responsible for the service in its entirety, including outsourced parts.

3.1.3 Preparedness for distribution of cash in times of crisis

Through previous joint inspections, Finanstilsynet and Norges Bank have determined that the contingency preparedness of the electronic payment system is inadequate, and that none of the banks inspected had satisfactory preparedness measures for cash distribution in the event of a crisis. Since the scope of the banks' obligations under section 16-4 of the Financial Institutions Act may be perceived as unclear, Finanstilsynet and Norges Bank were commissioned by the Norwegian Ministry of Finance to assess the need for a more precise definition of banks' obligation to ensure preparedness measures for cash distribution in times of crisis, and have proposed that this obligation be set out in specific terms in regulations. The Ministry of Finance has circulated draft³ Regulations on contingency preparedness for cash distribution for comment.

3.1.4 Notifications 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 system
- a new version with a modified or new functionality of material importance for the payment (service) system

In 2016, Finanstilsynet received 20 notifications of new or modified payment service systems. Almost all of the notifications concerned mobile systems. The other notifications concerned other types of payment systems or security systems related to the use of payment services.

On the basis of the notifications received, some institutions were asked to provide supplementary information. Among other things, the institutions were asked for information on risk and vulnerability analyses and security measures for the service in question; see the requirements set out in the Regulations on payment service systems.

3.1.5 Developments in payment services and mobile payment systems

The payment service sector is undergoing major changes, due in part to technological advances, changes in customer behaviour, e-commerce and regulatory changes. PSD 2 will make the sector subject to new regulation, which will open up the payment market and give new operators access to the customer relations and services of existing operators. "Open banking" or "API4-banking" are terms

³ <https://www.regjeringen.no/no/dokumenter/horing---beredskap-for-kontantdistribusjon/id2537040/>

⁴ API: Application Program Interface = interfaces are opened as a result of regulation or voluntary cooperation

used to describe this change, which is taking place globally and as a result of which banks are allowing new operators to develop new, value-added services for customers based on access to existing activities, such as account and customer data. In the establishment phase, in particular, these changes in payment services could potentially give rise to new risks and vulnerabilities that must be addressed.

In Norway, this trend can be observed in the advent of new market operators, the offering by current operators of new services through existing systems, the establishment of new collaborative constellations between banks or between banks and other operators, and collaboration between payment service users.

New operators such as Facebook and Amazon have established e-money institutions in the EEA and given notification of cross-border operations. However, no operations have as yet been established in Norway. Other operators like Apple and Google are also expected to enter the market, along with new Norwegian operators such as Payr⁵.

In 2016, new payment applications began to be used, such as SPING⁶ (by a number of savings banks) and Eika Safe⁷ (the Eika banks). New services were developed, as well as new functionality in payment applications such as MobilePay and Vipps. However, mobile payment applications still largely use their own infrastructure, which means that the payee must install the same application as the payer in order to access the transferred amount.

In 2016 and at the start of 2017 there was a significant consolidation of payment applications, aimed at meeting competition from global operators when PSD 2 comes into force. Nordea and Gjensidige Bank have entered into a partnership with Danske Bank on MobilePay. DNB, together with the Sparebank 1 alliance, the Eika Alliance and a number of other savings banks are collaborating on Vipps.

Up to now, international payment cards have been a prerequisite for using the mobile payment systems. BankAxept has now been adapted for use in mobile payment applications. In practice, this means that BankAxept can also be used for contactless payment using a mobile device, if the mobile payment application has been adapted for contactless payment. In 2016, BankAxept launched a contactless payment system using physical cards, with the same functionality as the one already offered by the international payment systems VISA and Mastercard. In the course of 2017, BankAxept will launch systems for account-to-account payments, for use in both e-commerce and mobile payment applications.

⁵ <https://www.payr.no/>

⁶ <https://www.sbm.no/naringsliv/betalingstjenester/sping/sping---lag-og-organisasjoner/514/2284/>

⁷ <https://esbank.no/betale/kredittkort/eikasafe>

Due to the lack of standardised point-of-sale terminals, some large merchants established Retail Payments in 2016 to counter the financial industry's failure to standardise mobile payment systems. The aim is to establish a single, common infrastructure with a single EFT/POS terminal system for unified settlement platform. This means that the system must be able to handle both physical cards and mobile-based payment, by means of QR codes, bluetooth communication, wireless communication (NFC) or the Internet. Other service providers, such as Nets and Verifone, are also developing new payment terminals that will enable payment by means of mobile devices to largely replace payment with physical cards in the course of 2017.

In previous risk and vulnerability analyses, Finanstilsynet has pointed out that insufficient interoperability between payment systems could reduce the efficiency and increase the costs of payment services, making it necessary to adopt regulatory measures. It is therefore positive that more banks are now allowing the use of "instant payment" services, and that the industry has set a deadline for making it possible to receive such payments⁹. A project under the auspices of Norges Bank, Finance Norway and Bits has also been established, with a mandate to assess and recommend common infrastructure for payment systems for the purpose of achieving speedier settlement.¹⁰

Developments in the use of biometrics in connection with authentication and payment are giving rise to new ways of making payments, such as the use of fingerprinting in EFT/POS terminals¹¹. Finanstilsynet assumes that extensive risk assessments will be carried out before new technology in payment systems is put into operation.

In step with the rising use of mobile systems, particularly those related to payment, the threat is also increasing¹², despite the possibilities for secure mobile payment services offered by technological advances. A growing volume of new malware, which is also more sophisticated and complex, has been observed.

3.1.6 Locking payment cards against use in online transactions

The EBA's Guidelines on the Security of Internet Payments came into force on 1 August 2015. Under the guidelines, cardholders must be able to lock their payment cards against use in online transactions. Finanstilsynet has noted that not all payment card issuers have implemented this functionality in their systems in accordance with these guidelines.

Finanstilsynet has pointed this deficiency out to the payment card issuers in question, asking them to report on their plans to implement the functionality in accordance with the guidelines. See also 3.2.3.

⁸ <http://www.dn.no/nyheter/2017/03/06/2127/Finans/mobilepay-har-fatt-nokkel-til-10000-butikker-i-norden>

⁹ <http://www.bits.no/wp-content/uploads/2016/10/2016-Bits-rundskriv-02-Krav-om-mottak-av-Straksbetalinger.pdf>

¹⁰ <http://www.bits.no/wp-content/uploads/2016/12/Mandat-Betalinger-med-raskere-oppgjør.pdf>

¹¹ <https://www.dn.no/nyheter/2017/03/01/2046/Teknologi/fingeren-kan-bli-bankkort>

¹² <https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf>

3.1.7 Payment terminals – payment cards

Finanstilsynet is aware that, contrary to the provisions of the payment card companies, payment systems are offered where the payment terminal can only read data from the magnetic strip on the payment card. The payment terminals offered today must be capable of accepting transactions where data are extracted from the card's chip.

Terminals deployed before 1 May 2014 and which read only from the card's magnetic strip may, subject to certain conditions, be used up until 1 January 2021 at the locations where they were deployed. These terminals may not be moved and used elsewhere.

These rules have been established by the payment card companies¹³, primarily for the purpose of limiting payment card fraud. Skimming, where fraudsters install a device in the terminal that reads the data in the magnetic strip, after which the card is used for online purchases, is one form of fraud currently in use. In practice, it will not be possible for an attacker to read information from the card's chip.

3.1.8 Attacks on payment services

The majority of attacks on payment services consist of attacks on payment transactions, which are described in greater detail below. Observations of cybercrime targeting the financial sector in a broader perspective are reported under 3.10.

Three different methods are used in fraudulent payment transactions:

- a) The fraudster initiates a transaction that is not authorised by the customer
- b) The fraudster changes a transaction that has been authorised by the customer
- c) The fraudster manipulates the customer to initiate a transaction

According to the incident reports received by Finanstilsynet in 2016, there were slightly fewer malicious attacks on payment services than in 2015. Although banks and payment service institutions are required to report incidents to Finanstilsynet, incidents involving fraudulent attacks on individual customers are not reported, unless the fraud scenario is new and exposes special vulnerabilities. For an overview of losses, see 3.1.9. Many of the banks are members of FinansCERT, which monitors attacks on payment services. Information from FinansCERT, together with the loss statistics, supplements Finanstilsynet's own incident reporting.

Online banking fraud

During a period in 2016, there was a high level of online banking fraud activity. The methods consisted of both Trojan attacks that infected the customer's PC and real-time phishing attacks to obtain single-use codes. The fraudsters initiated transactions that were not authorised by the customer. The fraud activity was more extensive than is indicated by the loss figures. Action taken by banks and through FinansCERT helped to detect attempted fraud attacks and halt them in time, for instance by

¹³ Reference is made here to Visa Member Letter 69-13.

stopping transactions in the payee's bank. An important preventive measure is to identify mule¹⁴ accounts, so that an alarm is triggered when attempts are made to execute transactions to such accounts.

Mobile payment fraud

Despite the growing number of mobile payment systems and escalating threat picture, Finanstilsynet is not aware of any attempted fraud attacks in Norway based on infected mobile telephones.

Consumer information

In Finanstilsynet's opinion, the information provided by financial institutions to consumers on how they can protect themselves against payment card, online and mobile-based fraud is steadily improving.

3.1.9 Overview of annual losses related to payment services

The tables below present figures for the last five years for losses due to payment card and online banking fraud in Norway.

A working group under SecuRePay is currently in the process of defining rules aimed at harmonising the reporting of loss statistics in Europe¹⁵; see 5.1.1.

Losses in Norway related to use of cards

In 2016 there was a 39 per cent increase in Card-Not-Present (CNP) fraud, while skimming fraud declined. In total there was a 9.5 per cent increase in payment card losses in 2016, while the number of fraudulently used cards rose by over 50 per cent. The average loss per fraudulently used card was lower than in 2015.

The volume of card transactions using cards issued in Norway rose by 6 per cent from 2014 to 2015, while the volume of payments using cards issued in Norway for online transactions increased by 16.8 per cent¹⁶. Fraudulent online transactions (CNP) increased by 39 per cent from 2015 to 2016. Slightly more than 0.17 per cent of all online transactions were fraudulent. Of the total volume of payment card transactions in Norway, around 0.02 per cent were fraudulent¹⁷.

¹⁴ Mules: Persons who make their own bank account available for rapid transfers of money out of the country.

¹⁵ The working group's mandate is to implement the requirement in PSD 2, Article 96(6) of annual reporting of fraud statistics.

¹⁶ <http://www.norges-bank.no/Publisert/Publikasjoner/Norges-Bank-Memo-/2016/Norges-Bank-Memo-12016/>

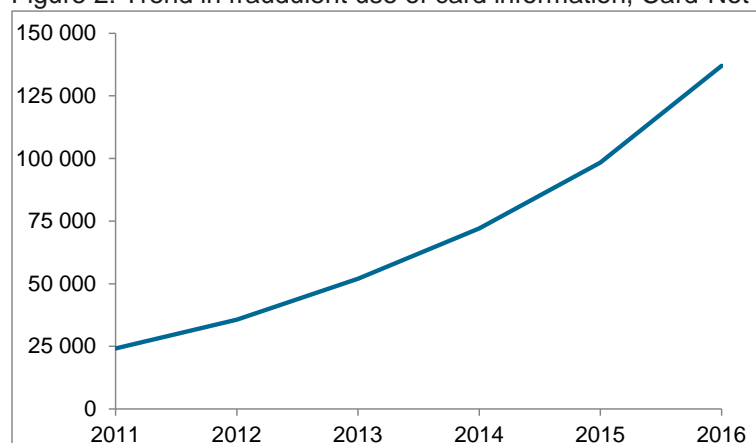
¹⁷ Norges Bank does not publish figures for 2016 until May 2017. The comparisons are therefore based on Norges Bank's figures for 2015. Figures from Norges Bank show that the total value of online purchases in 2015 was NOK 80 billion. CNP losses totalling NOK 137 million account for 0.17 per cent of NOK 80 billion. Card payments totalled NOK 855 billion in 2015. Payment card losses, which totalled NOK 206 million, accounted for 0.024 per cent of NOK 855 billion.

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

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

Sources: Finanstilsynet and Bits

Figure 2: Trend in fraudulent use of card information, Card-Not-Present (CNP)



Sources: Finanstilsynet and Bits

Payment card fraud and data theft

All cards issued in Norway have a chip, and only a few payment terminals (typically related to the purchase of convenience goods from vending machines and payment at parking meters) in Norway use a magnetic strip; see 3.1.7. Losses related to the fraudulent use of counterfeit cards in Norway are therefore low. On the other hand, cards or card data stolen in Norway are used in countries where the magnetic stripe is still commonly used, which is the reason why losses related to fraudulent use of counterfeit Norwegian cards are higher outside than within Norway.

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 payment card losses and the estimated average administrative cost for the card issuer per fraudulently used card. A cost per card has also been estimated related to the costs incurred by the consumer in connection with stolen card data. (Administrative and consumer costs have been kept constant for the period 2012–2016).

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

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

Source: Finanstilsynet

In addition to the costs presented in Table 2, there are further costs related to payment card fraud, including administrative costs incurred by card acquirers, merchants and the Norwegian Financial Services Complaints Board and, in some cases, costs in the form of lawyers' fees and court costs. The total costs related to fraudulent card use are therefore substantial. A total of 68,162 cards were fraudulently used in 2016, a 50 per cent increase on the previous year. As a percentage, the total costs of payment card fraud thus increased far more than the direct card payment losses in Norwegian kroner.

Losses related to online banking

Losses related to online banking increased slightly in 2016. In addition to the fraud reflected in the amounts presented in Table 3 below, a large number of losses were averted because the transactions were stopped before they were executed, or because the funds were returned by the payee bank. The banks, in cooperation with FinansCERT, work continuously on monitoring and stopping 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
Attacks using malware on customer's PC or security device (Trojans)	5,064	1,327	552	3,055	2
Lost/stolen security device	3,367	1,285	6,655	963	8,758
Phishing and false BankID – merchants	10		539	5,815	2,428
Other/unknown	358	779	3,474	2,715	7,444
TOTAL	8,799	3,391	11,220	12,548	18,632

Sources: Finanstilsynet and Bits

Losses related to CEO fraud

The volume of CEO fraud increased in 2016. In CEO fraud, customers are manipulated into authorising transactions. The fraud scenario is based on social engineering, and not on exploiting technical vulnerabilities or weaknesses in the banks' systems. Banks often help to stop the transactions at the payee bank and have the funds returned. CEO fraud caused considerable losses in 2016. The figures are certainly not complete, as customers do not necessarily contact the bank every time they experience this type of fraud.

The losses reported to Bits show CEO fraud losses of almost NOK 300 million in 2016. This exceeds payment card losses and the loss per case¹⁸ is high, on average nearly NOK 1.4 million per case.

Table 4: CEO fraud losses (amounts in NOK 1,000)

CEO fraud losses	2016
Number of cases	214
Average loss per case	1,374
TOTAL	294,061

Sources: Finanstilsynet and Bits

3.2 Banks

Banks continued to undergo major change processes in the field of ICT in 2016. The changes have largely been carried out without material consequences for operational stability. However, stability declined towards the end of 2016 and in early 2017.

3.2.1 Backdoors into the core system

Through its ICT inspections Finanstilsynet has observed varying management of access to businesses' administrative and core systems, where the same types of tasks can be performed through both accesses. The findings show that the front-end systems have good access management which limits the actions of someone using the systems, while no similar restrictions have been established in connection with direct log-in to the core system, such as in connection with access to the loan system. This makes it possible to circumvent the way the systems are intended to be used. Banks must use coordinated access management to ensure a consistent approach to what a user can do in a system regardless of which access is used.

3.2.2 Access management

In 2016, Finanstilsynet carried out a number of ICT inspections that focused particular attention on financial institutions' access management and control. The inspection findings show that the institutions are devoting increasing effort to work related to access management and control. Nevertheless, it is Finanstilsynet's assessment that this area must be given high priority by financial

¹⁸ One case can consist of several transactions.

institutions since the risk of fraudulent use or unintentional incidents may be substantial. Users with special privileges, such as administrative users, should be monitored particularly closely, but monitoring must also include verification of compliance with the processes for establishing, modifying and terminating a user identity.

3.2.3 Compliance with guidelines for online payments

In September 2015, Finanstilsynet published guidelines on the security of online payments. These guidelines define the European Banking Authority's view of what is considered good supervisory practice in the European financial supervisory system, and set minimum requirements for secure online payment. The guidelines are based on the Payment Services Directive (PSD) (2007/64/EC).

Through inspections, Finanstilsynet has identified some systems that do not comply with the guidelines' requirements of strong customer authentication. In Finanstilsynet's view, establishing authentication systems in accordance with the guidelines will contribute effectively to reducing fraud related to Card-Not-Present payments (online payments).

3.2.4 Outsourcing agreements

Finanstilsynet's inspections have revealed a number of cases where financial institutions have established outsourcing agreements that are not in compliance with applicable rules. The Financial Institutions Act lays down rules for outsourcing for financial institutions; see section 13-4 of the Act.

Under the Act, financial institutions are responsible for any activities they outsource. The Act further requires that the outsourcing must not render supervisory activities more difficult (transparency of outsourced activities). Ensuring that institutions have the requisite expertise to deal with outsourced activities is implicit in the requirement that the activity must be conducted properly. Section 12 of the ICT Regulations requires that agreements be in written form, which is crucial for the fulfilment of general corporate governance requirements, including the obligation of notification.

Institutions subject to supervision which are not covered by the Financial Institutions Act are governed by the Regulations relating to risk management and internal control.

3.2.5 Contingency preparedness systems and business impact analyses

Financial institutions are focusing increasingly on contingency preparedness systems designed to ensure secure, efficient operations, also in the event that normally accessible technical systems should fail. Finanstilsynet has observed weaknesses in institutions' analyses of the possible consequences of the failure of one or more applications (business impact analysis). These weaknesses are related to deficiencies in the institutions' documentation of the technical infrastructure required to establish a smoothly functioning contingency preparedness system.

3.2.6 Distribution of sensitive information through open e-mails

In 2016, Finanstilsynet observed cases where bank account statements and other information containing sensitive data were distributed to bank customers through open e-mails. Open e-mails pass

many hubs on their way from bank to customer and can be read on the way. Finanstilsynet therefore does not consider e-mails to be a direct or secure form of bank-customer communication. Reference is made in this connection to Finanstilsynet's circular 10/2007, which deals with the confidentiality rules that apply to the financial industry with regard to customer information, etc.

3.2.7 Introduction of the ISO 20022 message standards for file-based euro payments

Under section 9 (3)¹⁹ of the Financial Contracts Act, as of 31 October 2016 credit transfers and direct debits in euro must be executed using the ISO 20022 message standard²⁰. To ascertain whether banks are complying with this requirement with regard to its business customers, Finanstilsynet conducted a survey among Norwegian banks and branches of foreign banks. A not insignificant number of business customers had not converted to ISO 20022 for file-based euro payments prior to expiry of the deadline, but most of them will be in compliance in the first quarter of 2017. Several banks offer their business customers a conversion system, which is external to the online bank, until the company itself can deliver the payments in the correct message standard.

3.3 Securities

ICT systems in the Norwegian securities sector are still of high quality and high stability. However, in light of the current threat picture and due to the sector's growing outsourcing of ICT systems with sensitive information, ensuring that risk remains at an acceptable level will be a challenge. A number of major regulatory changes will affect the risk picture for the sector.

3.3.1 Operators' motives for cyber attacks on the Norwegian securities sector

Information systems in the securities sector contain large quantities of sensitive information on Norwegian business enterprises. The threat assessments issued in 2017 by the Norwegian Police Security Service (PST), the Norwegian Defence Security Service and Norway's security authorities indicate that sensitive information is the primary target for information gathering by foreign operators supported by foreign states (state-sponsored industrial espionage). For more information regarding the aforementioned threat picture, see 4.3.

Foreign state operators can have a number of reasons for compromising ICT systems in the securities sector. One motive might be to gather information to provide their own institutions with information on competing Norwegian companies' strategies, plans and technology in order to strengthen their own country's industry. Their motivation might also be to obtain information that will facilitate the acquisition of institutions possessing desirable expertise, systems and technology.

¹⁹ In accordance with Annex XII no. 3a to the EEA Agreement (EU Regulation 260/2012).

²⁰ The requirement applies when a payment service user who is not a consumer or a very small enterprise executes or receives single credit transfers or single direct debits that are not transferred individually, but collectively.

If unauthorised parties gain access to and make use of price-sensitive information, confidence in the integrity of the Norwegian financial industry may be affected, thereby reducing investors' willingness to invest in Norwegian business and industry, which in turn will have a negative impact on the Norwegian economy and jobs.

3.3.2 Findings in the securities sector

In 2016, Finanstilsynet registered several cases in which financial institutions had inadequate control of access to systems with sensitive information after outsourcing their systems. This gives grounds for concern as more and more of the administration of information systems in securities institutions is outsourced.

Finanstilsynet has observed that many institutions attach great importance to risk analyses carried out by data centres without the institution itself being involved. This could lead to the risk analysis not being adapted to the level of risk for the institution's particularly sensitive data.

Through its ICT inspections Finanstilsynet has found examples of outsourcing agreements in which institutions have waived the right to conduct inspections and audits of its own systems in the operating companies. This is a breach of section 12 of the ICT Regulations on outsourcing. Institutions have also been registered that do not monitor the access of operating company employees to the institutions' own systems. The activities carried out by operating company employees and the data that they access, have also been found to be inadequately logged, including for systems that process and store price-sensitive information.

Finanstilsynet has seen cases in which employees of ICT operations centres have traded (in) securities in institutions for which they conduct ICT operations during restricted trading periods, an indication that both the institution and the operations centre have inadequate procedures and low awareness of risk in this area.

3.3.3 ICT operations centres

In the Norwegian securities sector, a small number of operating companies dominate the market for outsourced ICT operations services. These companies have traditionally been used to operate ICT systems for banks and firms. New types of institutions also want to make use of the operational security, cost effectiveness and scalability of the systems provided by the established operations centres. For instance, listed companies, law firms and investment firms may want to store and process accounting data, strategy documentation and correspondence relating to acquisitions and financing in systems that are outsourced to this type of service provider. Systems likely to be outsourced are e-mail systems, filing systems and accounting systems.

The threat picture for operations centres, which may include strongly motivated interested parties who possess sufficient resources, such as leading state-sponsored hacker groups, cannot be neutralised solely by means of updated firewalls, anti-virus programs, information campaigns, effective processes and microsegmenting. The methods for accessing information in the data centres will not be limited to

electronic attacks. The attackers may also use various forms of social engineering, such as blackmail, to gain access to data. Financial institutions subject to supervision must therefore regularly carry out their own risk assessments of ICT security in their operations centres and ensure that security measures are adapted to the type of data/information that is stored and processed.

When several different operators, both institutions subject to supervision and those not subject to supervision, use the same operations service provider, the result is concentrated storage of large quantities of sensitive information. The operations service provider's systems and procedures for data protection may in actual fact basically be of higher quality than those of the individual institutions. The concentration of sensitive information will be a strong motivation for unauthorised parties to obtain access to the systems that store the information, necessitating higher standards of security. When conducting a risk analysis in connection with system outsourcing, institutions subject to supervision must take into consideration the concentration of sensitive information in the operating company.

Operating companies are neither responsible for nor adequately equipped to carry out impact analyses of the consequences of their customers' sensitive information falling into the hands of unauthorised parties. Analysing risk related to data is the responsibility of the institution that owns the data; see section 3 of the ICT Regulations.

Finanstilsynet expects institutions subject to supervision to maintain closer control of its ICT operations companies and their systems and personnel, so as to prevent information leaks.

3.3.4 Weak ICT security management and control at Nasdaq

In the light of findings following the ICT inspections carried out by Finansinspektionen (the Swedish financial supervisory authority) at Nasdaq Clearing AB and Nasdaq Stockholm AB, where the institutions were given financial sanctions of SEK 55 million, Finanstilsynet will continuously assess Nasdaq Oslo ASA's monitoring of its cybersecurity activities in order to ensure that the institution establishes relevant processes and measures to protect its systems.

Finansinspektionen's inspections were held in accordance with the Swedish regulatory framework, into which the EU European Market Infrastructure Regulation (EMIR), which includes provisions regulating ICT activities, has been transposed. In the inspections, special emphasis was placed on scrutiny of cybersecurity. In Finansinspektionen's view, the institutions do not meet the requirements relating to management and control of risk in their own operations, particularly because management and control have been outsourced to Nasdaq's parent company. According to the report, risk relating to the Swedish institutions is not dealt with separately. The basis for local control of risk in the Swedish institutions was therefore deemed to be deficient or unnecessarily complicated. Particular attention was drawn to the fact that the institutions' business continuity plan did not contain any type of measures to prevent cyber attacks. Consequently, the institutions lacked back-up systems and plans for critical functions and ICT systems.

3.3.5 Regulatory changes that affect the level of risk

A number of regulatory amendments in the securities sector are giving rise to new requirements for investment firms' systems. The level of risk is affected because systems must be changed, or because the firm risks incurring substantial fines if it fails to comply with the rules.

The EU's Markets in Financial Instruments Directive (MiFID II) and Regulation on Markets in Financial Instruments (MiFIR) set new requirements for investment firms' and trading venues' systems for trading in financial instruments. Examples include new requirements for time synchronisation of trading systems, modified requirements regarding the identification of participants in a transaction and extended TRS reporting. Commodity derivative positions will be subject to reporting and will necessitate new ICT systems. Following the introduction of EMIR, all institutions have a duty to report concluded and modified derivative transactions to one of the EU trade repositories.

The General Data Protection Regulation (GDPR) will replace personal data protection legislation in Norway as from May 2018. The GDPR ensures higher protection and assigns greater responsibility to financial institutions that process personal data. The institutions' ICT systems must also meet high standards, and institutions that process personal data will have to make changes in their systems. Breaches of GDPR provisions may result in substantial sanctions.

For further details of regulatory changes and systemic requirements, see 5.1.2.

3.4 Insurance

3.4.1 Risk related to inadequate risk assessments

In Finanstilsynet's experience, the performance and understanding of the importance of risk assessments are still areas for potential improvement for a number of insurance undertakings. Risk assessments submitted to Finanstilsynet are often deficient and fragmented, and do not always seem to be an appropriate means of ensuring that the institution's level of IT risk is acceptable.

Insurance undertakings, like banks, focus a great deal of attention on cyber security, primarily in connection with malicious criminal attacks. Finanstilsynet emphasises that this is a serious risk, but not the only one. Insurance undertakings must also be aware of other risks related to their IT operations.

Insurance undertakings' use of outsourcing is on the rise. Finanstilsynet has noted that the IT risks related to the outsourced operations are often not adequately assessed and are not always included in the overall annual review of IT risk required by the ICT Regulations.

3.4.2 Risk related to the use of spreadsheets

Some insurance specialists, such as actuaries, make extensive use of spreadsheets in their work. Spreadsheets form the basis for business and accounting reporting and decision-making and are therefore of major importance.

In many cases, inadequate systems and limited access to IT resources are the reason for the development and use of spreadsheets, which have a low user threshold. The challenge is that while the systems development carried out in an IT organisation is based on carefully considered processes and procedures grounded in recognised standards and methods, spreadsheets developed locally by a specialised unit are not normally based on equally well-thought-out processes. Nor, very often, is sufficient attention paid to user authorisations and access management. The use of spreadsheets can therefore pose a risk of errors, unintentional changes and breaches of confidentiality. Institutions that use spreadsheets of importance to their operations should establish common processes and procedures for developing and using spreadsheets, which encompass task-sharing, quality assurance, testing, change management and access management.

3.4.3 Non-compliance with the ICT Regulations' incident reporting requirement

In previous RAV analyses, Finanstilsynet has pointed out that few incidents are reported by insurance undertakings. The failure to report serious IT incidents prevents Finanstilsynet from obtaining the necessary knowledge of insurance undertakings' risk picture. When Finanstilsynet learns of incidents that should have been reported, it takes the matter up with the undertaking concerned.

3.4.4 New personal data protection directive?

Insurance undertakings face a need for extensive systems development in connection with the implementation of a new personal data protection regulation; see section 5.1.2.

3.5 Estate agencies – settlement

In 2016, thematic inspections were carried out of security in the settlement function of estate agencies. The thematic inspection covered settlement firms with various settlement systems that handle settlements in around one fourth of real estate transactions in Norway. The risk of error or intentional manipulation is greatest during the preparation of vouchers, before the bank files are generated or directly in the completed payment files. It is important that estate agencies establish systems that ensure that the files generated by the settlement system are checked against the payment data files in the online bank.

3.6 Monitoring of compliance with anti-money laundering rules

In 2016 Finanstilsynet carried out inspections that covered system support for anti-money laundering and anti-terrorism financing. The financial institutions had challenges related to ensuring that their customer controls are updated when sanction lists are changed. Financial institutions are required to have electronic monitoring systems to detect suspicious transactions. Some of the electronic monitoring scenarios are imprecise and result in so many false positive identifications that the banks need to have extensive control/checking resources to distinguish between false positive and genuine identifications. Finanstilsynet has pointed out the importance of continuously evaluating the scenarios, and of this being done in close collaboration between business and IT personnel.

3.7 Joint efforts by the financial industry

Banks, other key financial sector operators and Finance Norway collaborate on security, the development of shared infrastructure, services and common standards. The financial industry's new infrastructure company, Bits, is tasked with securing and improving efficient payment services and payment infrastructure in Norway, as well as with contributing to infrastructure development in other areas.

In line with technological developments and utilisation of the possibilities afforded by new technology, there is a need for open collaboration on the establishment of efficient, smoothly functioning infrastructure. This often implies comprehensive changes in infrastructure, in the individual financial institution and in technological interoperability, both within the industry and with other operators. Changes are the most frequent cause of undesirable incidents. Incidents in infrastructure systems often have a wide impact, and it is therefore important to carry out thorough assessments of both operational risk related to the operation and maintenance of services and security risk related, for example, to unauthorised use of the services.

The transition to the modernised online transaction exchange system Baltus²¹, a flexible, secure infrastructure for the routing and transport of transaction-related financial enquiries between banks, was completed in 2016.

A working group comprising representatives from the financial industry and Norges Bank was established in 2016 to create a shared infrastructure for faster settlement of payments, including making modifications to Norges Bank's settlement system. This infrastructure is intended to facilitate the continuous execution of real-time payments. Payments between the customers of different banks can then be executed virtually instantly at the same time as the inter-bank settlement risk is controlled. The working group is expected to submit its report in April 2017.

Through 2016, in accordance with section 9 (3) of the Financial Contracts Act, Bits monitored the banks' and financial institutions' switch to ISO 20022 message formats for file-based euro payments; see section 3.2.7. Work is also in progress to establish a common messaging standard, based on ISO 20022, for all file-based payment instructions issued by financial institutions to banks. The banks have based their work on the principle that ISO 20022 formats are also to be used for transmitting file-based payment instructions for currencies other than euro.

In 2016, BankAxept modernised its services, including its contactless card payment system, and will continue this work in 2017; see further details in 3.1.5.

Under PSD 2, banks are required to allow the participation of new payment service providers. A working group, headed by Bits, is to consider how the banks should establish access to payment

²¹ Banks' online transaction exchange system, which is the network used by banks for transaction exchange and to check the balance of accounts in each other's account systems.

accounts for service providers, both existing and new, who wish to offer the new payment initiation and account information services. Bank ID is also taking a closer look at how to adapt authentication systems to comply with PSD 2's provisions on the use of strong customer authentication.

In the battle for the mobile payment market, a number of new, technologically different payment terminal systems for use in physical stores have been established, in addition to the existing card-based payment terminals. This has resulted in the establishment of Retail Payment, the aim of which is to establish a single shared infrastructure with one terminal system²². Under the auspices of Bits, the banking industry has initiated a project aimed at facilitating the adoption of one technical device per merchant, which accepts the different payment systems offered in the market.

Through digital collaboration, the financial industry and public sector will seek to exploit the possibilities offered by technology to increase the efficiency of a range of processes across the sectors. So far three projects have been established with the following objectives:

- **Consent-based loan applications**
To enable information to be obtained from public sector agencies so that the credit score of loan applicants can be transmitted digitally and directly between the data owner and the bank.
- **Control information**
To enable the tax authorities to ask banks, as part of an investigation, to disclose relevant control information.
- **Bankruptcy proceedings**
To ensure that when bankruptcy proceedings are initiated, a digital notification is immediately sent to banks, causing bank accounts to be frozen.

Through Bits, the financial industry has drawn up requirements for improved customer identity authentication and BankID customer identity verification. In the first half of 2017, Posten Norge will launch a new personal delivery confirmation service, enabling banks to fulfil the new authentication requirements. Banks are expected to comply with these requirements once they become applicable.

Banks in the other Nordic countries have seen a need to establish a financial sector cybercrime unit (FinansCERT), like the one in Norway, and the creation of a common Nordic FinansCERT was therefore discussed. This process has resulted in the establishment of a Nordic Financial CERT, based on the Norwegian FinansCERT.²³

²² <http://shifter.no/index.php/2016/10/25/norske-retail-payment-inngar-partnerskap-globale-teknologigiganter/>

²³ <https://www.finansnorge.no/aktuelt/nyheter/2017/04/nordisk-finansnaring-etablerer-digitalt-forsvarssenter-i-oslo/>

3.8 Changes in outsourcing

Since 1 July 2014, Finanstilsynet has received outsourcing notifications in compliance with section 4 c of the Financial Supervision Act, which have given the supervisory authority a good overview of the outsourcing market. Finanstilsynet monitors the institutions that outsource services and systems to ensure that they still have management and control of these functions. It also checks that agreements and contingency preparedness are in compliance with applicable laws and regulations.

3.8.1 Notifications received

The notifications received in 2016 reveal a trend for more financial sector services to be performed outside Norway's borders. Major service providers used by the financial industry are consolidating their services in fewer centres. This largely applies to operational and monitoring services.

Outsourcing notifications have primarily been submitted by banks and insurance undertakings. These notifications can be broken down into three categories:

- Changes that are made in companies operating parts of the technological infrastructure, such as EVRY and Nets.
- New agreements or major changes in existing agreements between banks and insurance undertakings and their core system providers.
- Notifications of outsourcing of ICT services to service providers which have traditionally not included development or operating services for the financial industry in their service portfolio. These are service providers such as Microsoft, Google, Amazon, Salesforce and Facebook. The biggest challenge that Finanstilsynet found in connection with these notifications was that the agreements were not fully in compliance with applicable laws and regulations. After pressure from regulatory authorities and the financial industry, the service providers have modified the contracts they offer to the financial industry. Finanstilsynet assesses whether the contract fulfils the provisions on a case-by-case basis.

3.8.2 The duty of notification as an important tool

The outsourcing market is moving towards more globalised models and new laws and regulations are expanding financial institutions' outsourcing options. The duty of notification is necessary to enable the supervisory authorities to maintain an adequate overview of the financial infrastructure.

The duty of notification under section 4 c of the Financial Supervision Act also applies when the service provider outsources a service or system to a subcontractor. Finanstilsynet checks that financial institutions ensure through their agreement with the service provider that they will be informed when the service provider plans to change or enter into agreements on the use of subcontractors.

It may be difficult for institutions to have adequate knowledge about new delivery models, such as cloud services. Institutions must have sufficient ICT expertise to place orders and verify that the ICT services provided are in accordance with the orders. This also applies when there are multiple layers of subcontractors. If Finanstilsynet deems that the expertise and resources remaining in the institution are

insufficient, it may be necessary to ask the institution to implement and document measures to remedy the situation.

When ICT services are sourced from outside Norway, Finanstilsynet will ensure that the country risk is included in the institution's decision-making basis, which should take account of international ranking lists and analyses. Country risk may vary within a country, and the area to which the service is outsourced must be assessed in addition to the country as a whole. If Finanstilsynet deems that the residual risk after implementation of mitigating measures is not satisfactory, the institution may be ordered to take further action commensurate with the significance of the outsourcing for the financial system.

3.8.3 Revision of the circular on the outsourcing of ICT functions

In 2016, Finanstilsynet headed a working group that examined the outsourcing of functions by payment service providers and other financial infrastructure providers. The Ministry of Finance and Norges Bank participated in this work. The working group attached particular importance to offshore outsourcing. The working group presented recommendations as to how current laws and regulations should be applied and which factors institutions should consider when outsourcing a function. The group also made recommendations on risk-mitigating measures, including whether some functions are of such significance that they should be operated from Norway.

In light of the working group's recommendations, Finanstilsynet will revise its circular 14/2010 on the outsourcing of banks' ICT functions. Among other things, the following points will be inserted in the revised circular:

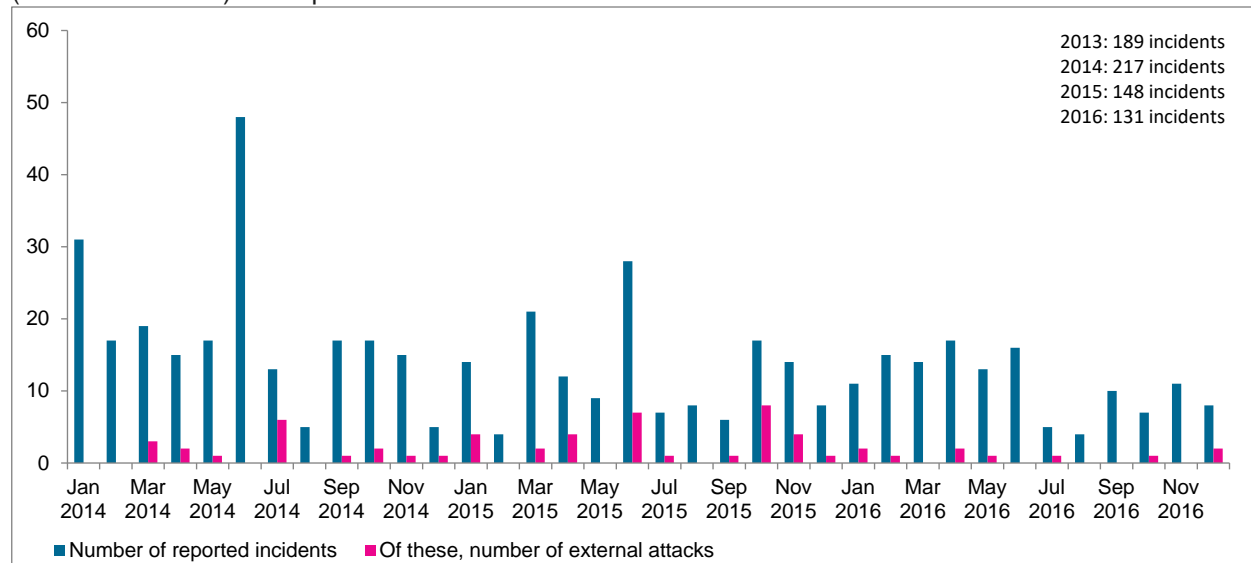
- Make it clear that the obligation to notify Finanstilsynet of the outsourcing of a function also applies to outsourcing by a service provider to subcontractors.
- Specify the information that must be provided in an outsourcing notification.
- Make it clear that country risk may vary within a country, and that the area to which a function is outsourced must be assessed, in addition to the country as such.
- Reference to updated international ranking lists and analyses.

Account will also be taken of the EBA's upcoming guidelines on outsourcing and cloud services; see 5.1.5.

3.9 Incidents reported in 2016

Financial institutions report to Finanstilsynet in accordance with the requirements in section 9 of the ICT Regulations on deviation and change management in connection with serious and critical ICT-related incidents. The 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 individual customers are not as a rule subject to reporting. A better overview of the level of intentional incidents emerges from status reports from FinansCERT and from the loss statistics; see 3.1.9.

Figure 3: Total number of reported incidents and number of reported external attacks (malicious attacks) in the period 2014–2016



Source: Finanstilsynet

3.9.1 Incident statistics

Finanstilsynet's incidence reporting indicates that operational stability was greater overall in 2016 than in 2015. Of 131 reported incidents, ten were reports of external attacks (intentional, malicious incidents). Both in actual numbers and as percentages this was lower than in 2015.

Alongside the provision of more payment services for mobile devices, not least BankID, telecommunications suppliers have also assumed greater importance for the availability of the services.

Serious incidents that resulted in long disruptions of mobile payment services were also reported in 2016.

Finanstilsynet likewise received more reports of faults and operating problems associated with banks' electronic anti-money laundering and terror financing monitoring systems. Finanstilsynet regards incidents that result in loss of AML controls as serious and reportable.

On three occasions, banks reported delays in delivery of SWIFT transactions. These were operational incidents, and were unrelated to the attacks (security incidents) that affected some global participants in the SWIFT network.

Finanstilsynet has noted that errors in capacity monitoring and/or planning are repeatedly the cause of incidents. Overruns of fill ratios and threshold values in technical components such as database servers, message queues etc. result in serious service disruptions.

Each year, Finanstilsynet receives incident reports from undertakings of involuntary exposure of customer data or other confidential data due to errors in applications or operations. This exposure may increase vulnerability and can be exploited for malicious purposes.

The majority of incidents reported by investment firms were linked to failure to record telephone conversations.

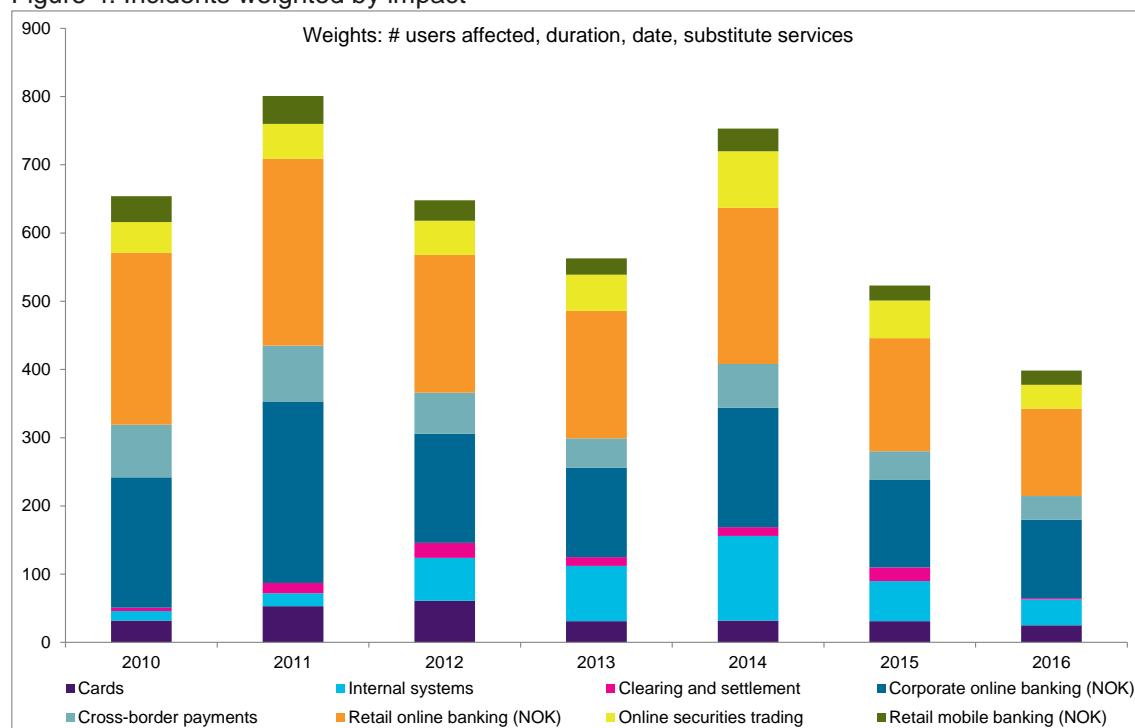
In December 2015, collection companies were made subject to a requirement to report incidents. Finanstilsynet received three reports from collection companies in 2016, all about operating problems that resulted in errors in mailings to debtors.

Finanstilsynet received two reports from insurance undertakings in 2016: one about an inaccessible website and one about an error in mailings to customers.

Reports were received from both banks and investment firms about DDoS attacks, encryption viruses and phishing, but somewhat fewer than the previous year.

3.9.2 Analysis of incidents as a measure of availability

Figure 4: Incidents weighted by impact



Source: Finanstilsynet

For each incident that has impacted availability, Finanstilsynet has considered the duration of the disruption, the number of undertakings affected, the estimated number of customers affected and whether there are substitute services customers can use. The data are weighted and compiled into time series, so that developments can be followed over time.

Figure 4 shows that the payment system and customer-facing solutions were more readily available to customers in 2016 than in 2015, despite the fact that several undertakings changed operations site and supplier in 2016, which entails a certain risk of downtime in the transitional phase.

The banks are spread among more operations service providers than they were a few years ago, and most incidents therefore impact a smaller number of customers than previously, when operations were concentrated among fewer suppliers. All else being equal, this reduces the risk of many undertakings being unavailable at the same time.

3.10 Observations of digital crime (cybercrime)

Cybercrime against financial institutions may consist of attacks on availability, confidentiality, through unauthorised retrieval of information, and integrity, through unauthorised payment transactions.

Digital attacks may affect several dimensions, and it may be difficult to determine the purpose of the attack.

3.10.1 Phishing and social engineering

Employees are often the weakest link in cyber defences. Phishing and social engineering are the most widely used methods for subjecting undertakings to malware. Undertakings must prevent undesirable incidents by providing internal training and raising awareness of this threat. Finanstilsynet has noted that some banks have programmes of this kind for their employees.

3.10.2 DDoS attacks and encryption viruses

The level of DDoS attacks was the same in 2016 as in recent years. DDoS attacks now seldom result in long disruptions to availability compared with previous years, thanks to the strengthening of the undertakings' defence against DDoS attacks. The spread of encryption viruses through various phishing attacks continued in 2016, and various types of financial institution were successfully infected. The undertakings' file systems were encrypted, and considerable extra work was involved in retrieving data backups and re-establishing systems. In some cases in 2016, both DDoS attacks and attacks with encryption viruses were followed by demands for ransom (ransomware) in order for the attack to stop or the file systems to be decrypted. Finanstilsynet does not know of any financial institution that has paid a ransom.

3.10.3 Attacks in the international SWIFT network

Digital attacks targeting SWIFT received a great deal of attention in 2016. The SWIFT network itself was not attacked, and no vulnerabilities have been detected in it, but the attacks were channelled through banks and targeted payment transactions due to be conducted through the SWIFT network. Countries in Central Europe and several countries outside Europe experienced such attacks, among

them Bangladesh. The attacks were a combination of social engineering and technical fraud. The attackers used various types of manipulation to acquire information about the users and user interface and user accesses to the undertakings' applications. The access could be used for fraud by setting up payment transactions to be conducted through the SWIFT network. The fraudsters also inserted codes that partially eliminated traces of the attack. The access control security measures for Norwegian users of the SWIFT network and applications that create transactions for transfers through the SWIFT network are more stringent than those of the countries that experienced these attacks. Since the incident, SWIFT has implemented a comprehensive security programme with new, mandatory security requirements. These include know-your-customer activities and controls against sanctioned customers and countries. The security requirements will apply to all users of the SWIFT network.

3.10.4 "Waterhole" attacks

In 2016, malware known as "waterhole malware" was disseminated, presumably through types of phishing, to various types of financial institution in different parts of the world. The malware contained lists of websites of other, often more central, financial institutions. The PCs of financial institutions on these lists became infected when they visited the infected websites. In Norway, too, financial institutions were discovered in 2016 to be "waterholes" for this type of targeted distribution of malware. In those cases where dissemination of the malware did occur, the virus failed to penetrate the financial institutions' systems, prevented from doing so by the institutions' surveillance and anti-virus software. It is unclear whether the purpose of the attack was pure data retrieval or whether the information obtained was to provide a basis for unauthorised transactions.

3.10.5 Other observed vulnerabilities

Finanstilsynet observes that there are vulnerabilities in servers and services that are available on the Internet, including older versions of software, which contain a number of security flaws. Attackers may attempt to exploit the vulnerabilities to crash or damage the service, or for other criminal purposes.

Finanstilsynet also observes other inappropriate software configuration, due to which the control mechanisms against hacking did not register all communication links, and hence did not control them.

These matters are taken up with the institutions in question, which are requested to remedy the weaknesses.

3.11 Developments in financial technology

The use of technology has made the Norwegian financial industry one of the most modern, efficient and forward-looking in the world. As new technology has become available, the financial industry has been quick to implement it and create services that ensure greater efficiency and user friendliness.

FinTech is a new term that has been used in recent years. Finanstilsynet's view of the term, a collective designation for various ways of changing and/or influencing traditional financial services through the use of technology, hence the term FinTech, is that the Norwegian financial industry and financial

services have long been absorbing technological innovations. Finanstilsynet therefore does not see FinTech as something new and unknown. Examples are several of the major initiatives in payment services that have been implemented through the years by the banks acting jointly.

Finanstilsynet sees that this technological trend, together with changes in the regulatory framework, particularly the introduction of PSD 2, may create challenges. One challenge, for example, may be how to secure equal competitive conditions for all operators for the same type of payment service.

3.11.1 Regulatory sandbox

The word “sandbox” often turns up in connection with FinTech. The Financial Conduct Authority (FCA) in the UK and the Monetary Authority of Singapore (MAS) are examples of supervisory authorities that provide sandboxes for companies with ideas for new financial services. The supervisory authorities have undertaken to help new service providers enter the financial services industry by relaxing some of the regulatory requirements for a limited period. Examples of requirements that are relaxed are the composition of the board of directors, the credit rating of the enterprise, the qualifications of the institution's management and capital requirements. There is no relaxation of regulatory requirements such as confidentiality surrounding customer information, treatment of funds belonging to customers or requirements regarding money laundering procedures. After the trial period, it is required that all relevant conditions for licensing be met.

Finanstilsynet engages in dialogues with IT supervisory colleagues in both the FCA and the MAS, with a view to following developments and drawing on their experiences.

Although no regulatory sandbox has been established in Norway, Finanstilsynet provides FinTech businesses with considerable guidance with respect to both rules and regulations and the planned services. The Ministry of Finance has asked Finanstilsynet to consider how a low-threshold contact point for guidance of innovative activities can be established in an appropriate manner.²⁴

3.11.2 "Distributed Ledger Technology" (DLT)

DLT²⁵ is one of the technologies that is expected to contribute most to further digitalisation and rationalisation of financial sector processes. DLT is a distributed database that is shared across nodes in a network. The technology is the focus of much attention in connection with the standardisation of regulations and infrastructure and removal of trade barriers in Europe.

As a consequence of these changes, operators see opportunities for developing solutions that are based on structural changes (disruptive) rather than creating solutions based on the existing infrastructure.

Like other technologies, DLT will undergo development and standardisation. Uses for the technology can be expected to be found in more areas. In due course, the areas of application and their

²⁴ <https://www.regjeringen.no/no/dokumenter/etablering-av-kontaktpunkt-i-finanstilsynet-for-veiledning-av-fintech-virksomheter/id2548606/>

²⁵ <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>

requirements will influence the speed and direction of development more than the current situation, where new areas of use are considered in the light of available technology. This kind of technological change typically takes longer than expected to be put into use, but the consequences of the changes are often greater than anticipated.

DLT functions as a self-regulating accounting system and lends itself to tasks that may be based on account maintenance, ownership registration, transactions and historical records. Although today's solutions are neither many nor visible, DLT systems have attracted attention as a foundation for the development of new solutions, for example for interbank money transfers. A number of major international banks are involved in this development, and some systems are operating in the pilot phase.

Several central banks have established projects to examine the possibility of issuing a national digital currency; Norges Bank, for example, is studying the possibility of introducing electronic central bank money. Solutions based on DLT technology may be relevant.

Projects in Norway include the Norwegian Central Securities Depository's collaboration project with Deutsche Börse aimed at developing a cross-border system for furnishing collateral and established R&D projects for using DLT in several banks and IT companies. The Norwegian banks' infrastructure company Bits AS has established a forum for sharing experience of using DLT.

Although there are as yet few established systems based on DLT, substantial research and testing is taking place. There are great expectations regarding future areas of use.

4 The participants' risk assessment

This chapter considers the principal threats brought up by the institutions themselves in interviews and in their responses to Finanstilsynet's questionnaire. Major threats revealed through interviews with key providers of security systems are also discussed.

4.1 Interviews

4.1.1 BankID – particularly on mobile devices – caused problems

BankID is a central part of banks' authentication and signing mechanism and it is therefore crucial that this function be operational and available to users. Several institutions indicated in interviews that there had been availability problems with the BankID system on mobile devices in 2016. A number of the incidents were due to faults with the telecommunication providers. Many service providers contribute to the technical infrastructure of financial markets. If the quality of service deliveries is to be increased, it is important that all these providers be monitored and followed up.

4.1.2 Inadequate focus on security in the design of systems

One topic that was often mentioned in interviews was challenges associated with integrating security in the design phase. This applies particularly to new development projects, but also to some extent to changes in existing solutions. It was found that if security architecture was not included in the design phase of new development projects, it was often both expensive and difficult to add security systems to a fully programmed system. Security systems that were added afterwards also resulted in poorer security than if they had been an integral part of the system.

4.1.3 Resources – shortage of qualified resources for mainframes, traditional programming and security expertise alike

As mentioned in the RAV analyses of previous years, a number of the solutions used in the banking and financial services industry in Norway were developed in a different IT architecture (e.g. operating system), and in other programming languages than those used in development today. The institutions agree that it is difficult to get hold of expertise to manage and operate the older portion of the application portfolio, since newly qualified ICT personnel tend not to be interested in working with legacy technologies. The trend is for a growing number of companies to outsource these services to countries where this type of personnel is more readily available than in Norway. This may mean a risk that company-internal knowledge is compromised. However, the institutions will be dependent on the old systems for several years to come. Outsourcing development, management and operations to enterprises that possess this expertise reduces the risk somewhat, but at the same time is very demanding in terms of agreements and management and control of the outsourced systems.

4.1.4 Knowledge of the use, architecture and monitoring of cloud-based solutions

The financial services industry wishes increasingly to use services delivered as cloud-based solutions (outsourcing). The services they want to use are often offered by big service suppliers such as Amazon, Google and Microsoft. Several of the institutions admit to inadequate knowledge of technical infrastructure, operating procedures and how management and control are performed by the service providers. Since institutions subject to supervision have full responsibility for their own infrastructure, it is a challenge for them to have sufficient expertise on the outsourced services to be able to manage and control them satisfactorily; see 3.8.

4.1.5 Security and access control – protection of corporate information

Corporate information is sensitive data, and access control and data security systems for infrastructure where this type of information is stored must accordingly be subject to stringent requirements. Institutions that were interviewed pointed out that particularly where information is stored in systems that are outsourced, follow-up of access control is crucial to maintenance and control of, for example, inside lists. Sensitive corporate information was viewed by those who were interviewed as readily marketable and hence of particular interest to criminal organisations. It is therefore important that all those who store corporate information, both owner and operators, place great emphasis on management and control to ensure that the quality of the security systems is appropriate and that they function as intended.

4.1.6 Time to market

The participants emphasise the importance of putting new or improved solutions into operation rapidly. Competition for customers is intense, and it is those who are fastest to reach the market with new solutions who win market share. This may result in systems being put into operation before they have been properly tested. This, coupled with inadequate integration of security architecture into the system, may imply a strong risk that the systems do not have the necessary level of security. This applies both to authentication systems and to how data are processed and shared.

4.1.7 Criminal organisations use artificial intelligence

The use of increasingly sophisticated and expensive methods is one of many indications that cybercrime has moved out of the garage and into organised crime. Artificial intelligence (AI) is one of several services used by criminals to obtain information as to how customers perform their transactions, or how the defences on the internet react to attacks. With the aid of artificial intelligence, they acquire large quantities of information that can be used in targeted attacks. The acquisition of information is not limited to equipment used in online or mobile bank solutions; it also includes a steadily increasing number of consumer articles or vehicles that can send and receive information via the Internet. The institutions that were interviewed saw it as vital that cyber security systems use systems as advanced as those represented by artificial intelligence.

4.1.8 Phishing

Large-scale phishing attacks have become simpler to carry out in recent years because technical solutions for carrying out such attacks are sold on the Internet. The solutions can often be purchased for from USD 2 to 10, and their use does not demand any particular technical expertise. Attacks have become increasingly sophisticated, and the phishing often targets particular departments in institutions and the employees in these departments rather than the whole institution, so that the hacking attempt attracts less attention. There is a potential for criminals to succeed in fraud based on phishing.

Institutions indicate that they place great emphasis on training and informing their employees about phishing and the use of e-mail to reduce this risk.

4.2 Questionnaire on vulnerability

In December 2016, Finanstilsynet conducted a questionnaire survey of 23 institutions. In the questionnaire, Finanstilsynet asked the institutions to rate themselves with respect to their vulnerability to potential threats. The results are shown in tables 5–10 below. Green expresses low vulnerability for the institution, yellow medium vulnerability and red high vulnerability. No colour indicates that the institution did not reply.

The institutions were also asked to rate their vulnerabilities going forward, i.e. as increasing, stable or decreasing. The trend that emerges in the column on the far right in the tables below is an expression of the average of the assessments given, where 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 that point down indicate that vulnerability is regarded as decreasing (the interval -0.2 to -1).

The size of the institutions is not reflected in the table below.

4.2.1 Support for strategic decisions

Table 5: Support for strategic decisions

	Vulnerability	The institutions' responses	Trend 2016	Trend 2015
1	The ability of systems to retrieve relevant information from external and internal sources and compile and synchronise the information into a picture of the enterprise's risk for the purpose of management and reporting to authorities		→	→
2	The ability of systems to automatically provide an overall risk picture, so that if a cornerstone enterprise goes bankrupt, for example, the system automatically issues an alert about loans to enterprise employees and suppliers, so that we can consider writing these off as losses		→	→
3	The ability of the systems to reflect customers' ability to service debt		→	→
4	The quality of data in our systems and registers		→	→
5	Integration and synchronisation of systems		→	↘
6	When new IT systems are to be developed, do we take into account the needs and systems of all relevant departments? We do this to avoid the challenges associated with "silo solutions", such as extensive software maintenance, complicated operations and challenges associated with data synchronisation		→	→
7	Complexity of IT systems		↗	→
8	Scope of and faults and deficiencies in systems		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed				

Source: Finanstilsynet

The table shows the risk of ICT not always functioning satisfactorily as support for strategic decisions, customer services or case processing. One example is that ICT systems do not give sufficient warning, for example of financial problems, that affect a cornerstone enterprise or a whole industry. Institutions therefore do not receive information from the ICT systems that enables them to take the necessary steps.

The complexity of the IT systems is regarded as a growing risk. New services combined with partially old architecture results in complexity and risk.

4.2.2 Operational irregularities

Table 6: Operational irregularities

	Vulnerability	The institutions' responses	Trend 2016	Trend 2015
1	Organisation, procedures, job description, reporting and controls		↘	↘
2	Agreements with suppliers give us the right to scrutinise all aspects of the delivery?		→	→
3	The test systems are "production-like", i.e. test data, applications, software, control systems and hardware are the same for testing as for production?		→	→
4	We make changes in the infrastructure ("non-functional" changes) during periods with little traffic, and can quickly reverse the change and roll back if necessary?		→	→
5	Our ability to detect all weaknesses		→	→
6	The controls for ensuring that all hardware and software are included in IDS/IDP, firewall and antivirus and other measures for ensuring stable operations		→	→
7	Logs and our ability to react to the contents of the logs		→	↘
8	"Ticking bombs", i.e. components that are gradually wearing out, or assets that gradually reach levels requiring intervention without our noticing it, such as memory leakage, certificate dates, worn out electronic components, an energy supply that is running down (batteries etc.)		→	↘
9	Our ability to detect irregularities in data traffic (abnormal load, abnormal ports / protocols, irregular response times) in the operating pattern and take action before damage occurs		→	→
10	Our protection against data attacks (advanced persistence threat, Trojans, ransomware, DDoS)		→	→
11	The quality of our business continuity and disaster recovery systems; see section 1 of the ICT Regulations		↘	→
12	Procedures for cooperation with suppliers		→	→
13	The pressure to deliver we are exposed to in the market		↗	↗
14	Access to expertise, including the expertise to stipulate requirements for suppliers and to monitor deliveries		↗	→
15	Scope of changes		↗	→
16	New regulatory requirements that make it necessary to change our systems		↗	↗
17	Our knowledge of where data transmission lines go and line redundancy		→	→
18	Access control, access control and segregation of duties		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed				

Source: Finanstilsynet

Major operators have tested business continuity solutions with positive results – risk has gone from stable to decreasing.

Pressure to deliver, changes as a result of new regulations and a shortage of expertise constitute a growing threat.

Inadequate logging and surveillance have changed from being a decreasing threat in 2015 to a stable threat in 2016, i.e. the threat has increased compared with 2015. The growing threat associated with the Internet of Things may be a contributory factor.

4.2.3 Data are not adequately protected

Table 7: Data are not adequately protected

	Vulnerability	The institutions' responses	Trend 2016	Trend 2015
1	Our guidelines for classification of structured (databases) and unstructured (text documents, e-mails) information and protection of the information		→	→
2	Access controls – employees, consultants, suppliers, applications, software		→	→
3	Our logging systems and our ability to react to log contents		↘	→
4	Possible penetration of our systems		→	→
5	Protection of data on portable devices		→	→
6	On termination of data storage agreements, the supplier must document that data have been completely deleted?		→	→
7	Unstructured data (i.e. data that users themselves evaluate the need to protect) such as e-mails, presentations, text documents, are reviewed regularly with a view to protection or alternatively deletion.		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed				

Source: Finanstilsynet

Access controls continue to represent a challenge. Outsourcing, offshoring and temporary, contracted expertise create challenges.

There was an increase in ransomware in 2016, as revealed by the institutions' comments.

Vulnerability associated with logging and the ability to react to the contents of the logs is decreasing.

4.2.4 ID theft

Table 8: ID theft






	Vulnerability	The institutions' responses	Trend 2016	Trend 2015
1	Our protection against malware that infects a user in the institution and misuses the rights of the infected user		→	→
2	Controls on the issue and use of log-on IDs and passwords to customers and employees (BankID, employee ID, system users, admin users)		→	→
3	Controls that prevent skimming and card-not-present fraud		→	↗
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed				

Source: Finanstilsynet

Malware and fraudulent use of rights in connection with ID theft are still regarded as a considerable risk.

4.2.5 Misuse of access to IT systems

Table 9: Misuse of access to IT systems




	Vulnerability	The institutions' responses	Trend 2016	Trend 2015
1	Access control		→	→
2	Our policy on segregation of duties		→	→
3	Logging		→	→
4	Analysis of "suspicious" transactions such as retroactive value dating, movements in internal accounts, transfers from customer to employee and back		→	→
5	Monitoring of employees' own-account trading		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed				

Source: Finanstilsynet

The threat picture is unchanged from previous years.

4.2.6 Money laundering

Table 10: Money laundering

	Vulnerability	The institutions' responses	Trend 2016	Trend 2015
1	Market surveillance		→	→
2	The ability of the IT systems to compile information about customers, customer relations and customer behaviour (KYC – Know Your Customer)		→	→
3	Electronic surveillance of transactions and transaction patterns – precision in flagging suspicious transactions		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability White: Not assessed				

Source: Finanstilsynet

Several institutions still consider it a challenge to develop systems that flag suspicious transactions with high precision. A substantial number report active efforts to improve collecting, flagging, analysis and reporting in this area.

4.3 National assessments of the threat picture

In its publication *Helhetlig IKT-risikobilde 2016* [Overall ICT risk picture 2016] the Norwegian National Security Authority (NSM) has a description of agents presenting a threat of digital espionage which points out that foreign governments represent a high risk because they have the resources to engage in methodical activity for extended periods. In its Annual Threat Assessment for 2017, the Norwegian Police Security Service (PST) states:

“Intelligence operations against targets in Norway will include computer network operations. Foreign intelligence services will also actively attempt to gain access to individuals in organisations that deal with sensitive information and technology.”

Focus 2017, the analysis of the military intelligence service, points out that the most serious threats are cyber-based, and that Norwegian economic and technological assets are targeted by foreign government agencies.

The sensitive information referred to in the reports concerns information on the strategy, technology and financial situation of Norwegian financial institutions. Finanstilsynet therefore concludes that the bulk of the information affected by these threats will be in the area of securities, and investment firms in particular, but that information of this kind is also to be found in other places such as banks' corporate functions and in the economic units of the institutions. Finanstilsynet is of the view that greater attention should therefore be paid to these areas in institutions' risk assessments.

5 Regulatory changes

In 2016 there was once again a series of EU processes associated with proposals for new, or amendments to existing directives, regulations, regulatory technical standards and guidelines, which will have a bearing on Norwegian conditions as and when they are transposed into Norwegian legislation. There were also amendments to laws, regulations and guidelines at national level.

In some areas, the changes may entail a need for extensive modifications in financial institutions' system design or ICT-related processes. Changes in the system portfolio are generally a significant source of error.

5.1 Coordination within the EU and changes in EU rules and regulations

5.1.1 Payment services – new Payment Systems Directive

The new Payment Systems Directive (PSD 2)²⁶ enters into force on 13 January 2018, and is intended to promote innovation by creating greater competition between existing and new operators. Pursuant to PSD 2, the EBA, in cooperation with the ECB, has been authorised to submit ten recommendations or regulatory technical standards, among other things on strong customer authentication and common and secure communication, recommendations concerning incident reporting and recommendations concerning control of operational and security risk. The ECB and EBA will also draw up recommendations on reporting of fraud statistics.

Proposals for regulatory technical standards for strong customer authentication and secure communication²⁷ have been sent by the EBA to the European Commission, and will enter into force 18 months after they are adopted. The draft specifies the requirements for use of strong authentication. It also specifies a number of rules for exemptions based on factors such as payment risk profile, payment channel, type of payment, payment recipient and amount. There are extensive requirements for protecting the confidentiality and integrity of payers' personal security credentials, with regard to both use and delivery. Requirements are also made for authentication and communication between existing operators/providers of payment accounts and new/existing operators wanting to provide the new payment initiation services (PIS) and account information services (AIS). The proposal is therefore

²⁶ <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2013/okt/revidert-betalingstjenestedirektiv---psd-2.-/id2434721/>

²⁷ <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2>

key to achieving the objectives of PSD 2. Payment account providers are required to make available at least one interface that offers the same availability, performance, support and emergency response measures as the interfaces made available for payment service users' direct access to their payment accounts. There are also requirements regarding data exchanges, including that the information made available through the interfaces by payment account providers must be at least the same as that made available to the payment service user through direct online access.

The EBA has circulated for comment a consultation paper on incident reporting. The recommendations encompass both operational and security incidents, and contain requirements regarding the classification of incidents and the process of notifying the supervisory authorities. The recommendations open the way for both delegated and consolidated reporting and stipulate requirements for the supervisory authorities' follow-up of reported incidents and cooperation with the authorities of other countries where relevant. The recommendations also include proposals for forms to be used in reporting. Final recommendations will be adopted in 2017. The recommendations are broadly in line with existing provisions in the ICT Regulations, but changes must be expected when the recommendations are implemented in Norway.

Recommendations on management of the operational and security risk of payment system providers will be circulated for comment in the first half of 2017. The recommendations include requirements for risk management and a number of requirements regarding identification of risk areas, policies and measures, surveillance, robustness testing and management of security incidents. Final recommendations are expected to be adopted in 2017.

PSD 2 stipulates requirements for reporting of loss figures associated with the use of payment services. In Norway, these loss figures have been reported since 2011. A work programme has been established by the EBA and ECB to ensure consistent reporting across countries and simplified consolidation at EEA level. The categories for fraud involving payment cards, credit transfer and direct debit will be specified. The total number of transactions in the same category must be reported along with the fraud figures. Fraud with payment transactions is often cross-border. Harmonised loss figures will provide a picture of how the fraud develops and moves across countries. Finanstilsynet has no such statistics at present. Reporting according to the new rules is scheduled to start in 2018, with publication in 2019 for the first time. It is assumed that the rules will make it necessary to change existing loss reporting rules in Norway.

5.1.2 New privacy legislation²⁸

The new EU General Data Protection Regulation will enter into force in May 2018. The rules apply to all organisations that compile or use personal data about EU/EEA citizens. They imply, among other things, that organisations must have a privacy statement, and conduct risk and privacy impact assessments. Many enterprises will have to establish a data protection officer. The Regulation will require that privacy be integrated into ICT systems that encompass personal data. The option that

²⁸ <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/>

makes the least incursion into privacy is to be the default system. Examples of possible factors for which default settings will be required are:

- quantity of information to be compiled
- scope of the processing
- data storage time
- who is to have access to the data

Enterprises that do not comply with the rules risk substantial financial sanctions.

Finanstilsynet's assessment is that the changes will require the institutions to make quite substantial modifications to their IT systems. Finanstilsynet further assumes that institutions will make active efforts to put procedures and systems in place.

5.1.3 Network security

Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016²⁹ (the NIS Directive) defines measures designed to ensure a high common level of security for network and information systems in the EU.

The Directive requires member states to ensure that operators of important services, including banks, financial market infrastructure and digital infrastructure, implement security measures and report incidents. This is already regulated in the financial sector through the ICT Regulations, and therefore does not entail major changes in the institutions' obligations.

5.1.4 Transmission of data between the EU/EEA and the USA – Privacy Shield

On 12 July 2016, the European Commission adopted the new regulatory framework on the transmission of personal data from Europe to the USA, called the EU-US Privacy Shield. The decision also applies to Norway, through the EEA Agreement.

The European Commission has concluded that the new agreement, which replaces the Safe Harbour agreement that was ruled invalid in October 2015, ensures an adequate level of protection for the transmission of personal data from Europe to the USA.

Personal data can now be transmitted to American companies that are certified by the US Department of Trade pursuant to the Privacy Shield agreement, and that have thereby undertaken to abide by special rules for the protection of personal data.

²⁹ <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/okt/revidert-betalingstjenestedirektiv---psd-2.-/id2434721/>

5.1.5 Taskforce on IT Risk Supervision

In 2016, Finanstilsynet took part in the EBA's Task Force on IT Risk Supervision (TFIT) and was represented on two working groups. One working group has prepared draft guidelines for assessing IT risk in connection with the SREP³⁰ process. The other working group has prepared a draft recommendation for supervisory review of banks' use of cloud services. According to plan, the results of these working groups will be completed in the first half of 2017.

5.2 Changes in the Norwegian regulatory framework

5.2.1 MiFID II / MiFIR

The Markets in Financial Instruments Directive (MiFID I) has been transposed into the Norwegian Securities Trading Act and Stock Exchange Act. With effect from 3 January 2018, MiFID I will be replaced in the EU by MiFID II and MiFIR (Markets in Financial Instruments Regulation). MiFID I regulates the activities of trading venues and investment firms, including market transparency requirements. The purpose of the revision of MiFID I is to achieve more transparent, smoothly functioning markets and to increase investor protection. MiFID II and MiFIR are supplemented by legislation in the form of around 40 Commission Regulations and one Commission Directive.

The Securities Act Committee's proposal for the transposing of MiFID II and MiFIR into Norwegian law is presented in Norwegian Official Report NOU 2017:1. The Ministry of Finance has circulated the proposal for comment, with a deadline of 15 May 2017.

A number of the new requirements in MiFID II and MiFIR relate to the investment firms' and trading venues' systems for trading financial instruments. New system requirements are set for investment firms and trading venues that use algorithms and for order record keeping and synchronisation of events, such as trades and price changes, in trading venues. New formats are to be used for transaction reporting (TRS reporting), and Legal Entity Identifiers (LEI) are to be used for identifying issuers, marketplaces and investors, if these are legal entities. Trading venues, their members, and investment firms that trade in commodity derivatives are also required to report positions in commodity derivatives. This will also imply requirements for the institutions' system design.

5.2.2 The European Market Infrastructure Regulation

The European Market Infrastructure Regulation (EMIR) introduces an obligation for the parties to a derivative transaction to report some standardised information about any derivative contract entered into and changes made to it, to a trade repository (TR). This reporting duty will apply to all institutions that are involved in these transactions, as opposed to TRS reporting, which is a duty applying only to investment firms. The duty of reporting pursuant to the EMIR entered into force in the EU on 12 February 2014. As of mid-April 2017, the EMIR has not been transposed into Norwegian law, and Norwegian institutions are therefore not obliged to report any derivative contracts that have been concluded to trade repositories. The EMIR is expected to be transposed into Norwegian law in the

³⁰ The Supervisory Review and Evaluation Process (SREP) is Finanstilsynet's evaluation of banks' own risk, capital requirements (ICAAP) and liquidity requirements (ILAAP).

second quarter of 2017, so that Norwegian institutions will be required to report from that time. However, the date when the actual duty to report takes effect has not been fixed, as this will depend on the transposing of supplementary legislation to the EMIR into the Norwegian regulatory framework.

The regulatory technical standards containing more detailed reporting requirements (including the reporting form) will be changed in the EU with effect from 1 November 2017. This should be borne in mind when developing the reporting form.

In order to provide services in the EEA, trade repositories must be registered with the European Securities and Markets Authority (ESMA). A list of registered trade repositories the institutions can choose to use for reporting is available on ESMA's website.

5.2.3 Anti-money laundering measures

In December 2016, the committee that has drawn up the new Act and regulations on anti-money laundering measures delivered its second interim report to the Ministry of Finance. The draft Act was circulated for comment, with a deadline of 1 April 2017. The committee's mandate was to draw up a draft act and regulations that transpose the fourth EU anti-money laundering directive, and to take account of the recommendations of the Financial Action Task Force on Money Laundering (FATF). The Anti-Money Laundering Directive is a full harmonisation directive that limits possibilities for national choices. It has been proposed that much of the contents of the current money-laundering regulations be included in the Act. In the first interim report, which was published in November 2015, the committee proposed some adjustments to the scope of the Act. The interim report also contained an evaluation of whether a cap should be introduced for cash purchases.

In December 2016, Finanstilsynet published circular 24/2016, Guidelines on Anti-Money Laundering Rules. The guidelines will be adapted to new rules after these enter into force.

5.2.4 Regulations relating to interchange fees in card schemes

Regulations relating to interchange fees for card-based payment transactions entered into force on 1 September 2016. The regulations place a cap on interchange fees for card-based consumer payments. They regulate merchants' right to encourage consumers to pay with the cards the merchants' prefer, but consumers are free to choose the one they want to use. This means that merchants must establish technical solutions that support users' right to make their own choice of payment card.

The regulations also set a requirement of separation between the owner of the card scheme and the company that processes the cards. Recommendations for regulatory technical standards with respect to the separation requirement have been submitted by the EBA to the European Commission.

5.2.5 Draft new Security Act

In 2016, a draft new Act relating to Protective Security Services was submitted. The Act will apply to all activities that are crucial to fundamental national functions. The report refers to the fact that the banking and monetary system is a fundamental national function.

It is proposed that the scope of the Security Act be expanded to cover any institution that is crucial to fundamental national functions. Banks and infrastructure institutions may be covered. It is proposed that the terms 'sensitive object' and 'sensitive infrastructure' be used for objects and infrastructure defined by the sector authority as being crucial to fundamental national functions.

The draft Act proposes provisions relating to general requirements for preventive security. A sectoral regulatory framework that largely covers the provisions of the new Security Act has already been established for the financial sector. Similarly, an extensive sectoral regulatory framework that largely covers many of the proposed provisions on classified procurements has already been established for outsourcing.

6 Risk areas

Finanstilsynet's primary objective is to contribute to financial stability and smoothly functioning markets. Financial services cannot be delivered without well-functioning ICT systems. New digital solutions increase efficiency and help to lower costs. However, the trend also implies increased vulnerability.

6.1 Financial infrastructure

If payments cannot be made, important societal functions will no longer function satisfactorily after a short while.

In 2016 Finanstilsynet noted that the leading systems for logging onto payments services (Bank ID and Mobile BankID, both dependent on shared operational infrastructure) were unavailable on several occasions. These systems are the only means of logging onto the services of several large financial institutions. Especially stringent requirements must therefore be set for the quality of the log-on system.

In recent years, new and alternative methods for making transfers and payments have appeared. In 2016, several payment systems appeared in which customers use their mobile phone to approve payments. E-invoice, direct debit and standing orders are known from previous years, as is payment by means of online banking. The services can be accessed by online banking or mobile banking. The many options make the payment system less vulnerable; mobile banking may be available even if online banking is not functioning, and payment can be made by direct debit even if online banking is not functioning.

In 2016, several institutions were subjected to a type of attack in which attackers succeeded in making the institutions' data illegible for them. If attackers should be successful in accessing large quantities of customer and account data, and making them unavailable, this could create major challenges for the institution. Institutions that operate on behalf of all or several financial institutions are particularly vulnerable. They should conduct exercises in reconstructing and reverse-engineering data.

Rules for treatment of inside information are intended to contribute to smoothly functioning securities markets. Breach of the rules may lead to loss of confidence in marketplaces and to investors withdrawing from the market. In 2016, Finanstilsynet observed considerable weaknesses in management and control of access to systems that may contain market-sensitive information.

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

In 2016 the stability of the financial infrastructure was good, and on a par with that in 2015. The regularity of clearing and settlement systems and communication with the international payment system SWIFT and the international settlement system CLS was also good.

Although there were incidents that made payment systems unavailable for short periods, Finanstilsynet regards the Norwegian financial infrastructure as sound and stable.

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 areas of vulnerability 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 institutions' ICT governance and security work, including their measures to counteract cybercrime, the robustness of their operations and contingency preparedness 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. 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.

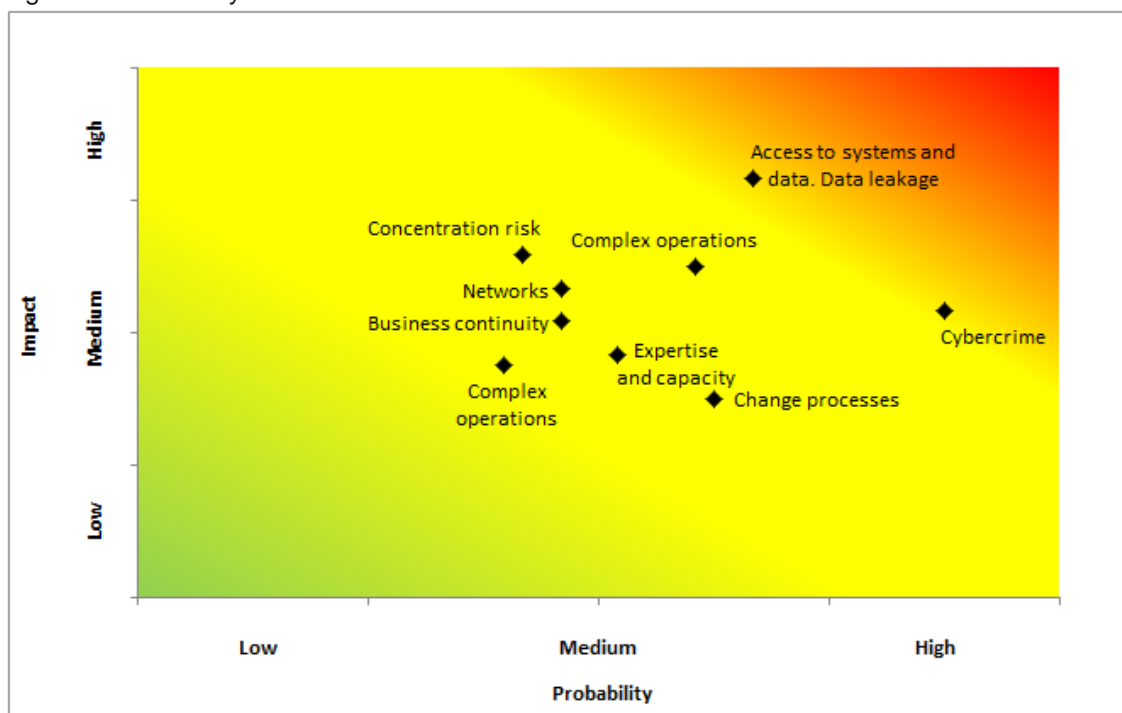
Interbank/settlement systems that are offered by banks are generally part of the banks' ordinary systems as far as operations are concerned. Observations and feedback from Finanstilsynet's ICT supervision of these banks will thus provide important information of benefit to Norges Bank in its oversight of the interbank systems.

Finanstilsynet can attend the supervisory and surveillance meetings that Norges Bank has with FMIs in the capacity of observer, and Norges Bank can take part as observer at Finanstilsynet's inspections of banks and data centres of importance to financial infrastructure.

6.2 The institutions

The figure 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 (low, medium, high) and the consequences if the incident occurs (low, medium, high).

Figure 5: Finanstilsynet' risk assessment



Source: Finanstilsynet

Finanstilsynet regards access to systems and data, data leakage and cybercrime as the most central threats to and vulnerabilities in the institutions systems. Inspections in 2016 reveal substantial deficiencies in control of access to systems and data, and Finanstilsynet regards the risk as higher than in 2015. Cybercrime is increasing in scope and complexity, making the risk higher than in 2015.

Complex operations, concentration risk and network faults are also major threats and vulnerabilities. Other risk areas are inadequate business continuity design, inadequate expertise and capacity, complex system portfolios and faults arising from changes in systems.

Networks

Financial services are based on services from a number of suppliers and are dependent on the quality and security of the suppliers' networks. The interaction is extremely complex, with a high risk of faults

and deficiencies in the service. One relevant example is that the dominant log-on system depends on an SMS service, which is a “best effort” service; in other words, no guarantees are given concerning the availability of the service.

The Internet of Things (IOT) expanded in 2016, meaning that an increasing number of devices are connected up to the institutions’ networks. Examples are surveillance, access control, process control and video systems. These systems are not well protected against hacking and other attacks. They typically have firmware and software that have not been changed for a long time, and that have vulnerabilities. Moreover, the supplier’s standard log-on user ID is often still active.

In theory, all data should be classified in accordance with the sensitivity and vulnerability of the data, and a unique security policy ascribed accordingly. However, administrative and equipment costs impose limits here. Microsegmenting of networks, a topic that was much discussed in security circles in 2016, is an attempt to come closer to this goal. Microsegmenting is a sort of virtualisation of the network stack – a parallel to virtualisation of memory, hard disk and CPU. In other words, the institution has defined several security levels for each layer in the stack. Subsequent to an analysis of the data with respect to sensitivity and vulnerability, the data are attributed the correct security in each layer of the stack. A practical example is highly sensitive data, which will be given the highest security level. In the transport layer, this means encryption – data are transported through an encrypted channel (virtual private network). In the application layer, it means strong authentication – users are linked to a strong authentication procedure. In practice, institutions restrict themselves to three or four security zones (admin and crypto, internal, DMZ, Internet). Data must to some extent be adapted to policy, and not the reverse. This makes heavy demands in terms of monitoring, and ensuring that data are placed in the right zone.

Some institutions regard this as so complicated that they allow others to manage everything, including administering firewalls. External administration of firewalls and network segments and zones means opportunities for undesirable and illicit access to data and systems.

Access to systems and data. Data leakage

In 2016 it was found that some institutions associated with the securities market should improve their controls with respect to access to inside information. If inside information is used to achieve financial gains, it may lead to investors avoiding the Norwegian securities market.

Finanstilsynet has observed that one institution’s e-mail server is operated together with other e-mail servers. Encryption of e-mails takes place at transaction level between servers; i.e., as a rule, e-mails lie on the servers in clear text. If a number of institutions share infrastructure, there is a risk of information becoming available to unauthorised persons.

Finanstilsynet notes that the institutions lack procedures to ensure that the e-mail configuration is set up in a manner that supports encryption, and that the configuration is set up in such a way that

transfers do not take place if the configuration of the recipient does not support encryption or does not support encryption that is regarded as adequately secure today.

Administration (registration and deregistration of users and rights) currently tends to take place by means of appropriate user interfaces in the form of one or more applications that are built onto the access control system. It used to be more common to administer users directly in the access control system, i.e. by means of registration functions that are an integral part of the access control system. The systems may still be such that it is possible to administer users by registering them directly in the access control system. This constitutes a risk.

As from May 2018, institutions must satisfy the requirements of the new EU Privacy Regulation. The Regulation will set stringent requirements for the institutions, with major repercussions in the event of failure to comply with the requirements.

Cybercrime

The frequency and diversity of network attacks is on the increase. At the same time, institutions have built up solid defences, which reduce the probability of the attacks causing major damage.

In 2016 there were several cases where hackers made data inaccessible to an institution and demanded a ransom. Finanstilsynet does not know of cases where ransom money was paid. Finanstilsynet is aware that the situation has caused quite considerable costs for restoring data from backups and lost time due to lack of access to systems and data.

It will be a very serious matter if attackers succeed in making large quantities of customer and card data inaccessible.

Complex system portfolio

Systems are built over a long period of time on the basis of technology and platforms that prevailed at the time when they were developed. The result is complex systems featuring several copies of production data and system linkages that have been developed in-house. Substantial resources are spent on maintaining an overview, synchronising data and maintaining software, resulting in complexity and risk.

It is difficult to set up test environments that simulate production, and to achieve full end-to-end testing in a complex infrastructure. Finanstilsynet's inspections have also revealed that test programmes and test procedures do not necessarily offer full certainty that changes will function quite according to plan when they are put into operation.

Complex operations

Operating multi-layer architecture with systems and applications on different technical platforms that have to interact is challenging. The different layers of the architecture often have different operators. The daily running cycle of major financial institutions consists of a large number of individual tasks

which are interdependent and have to be synchronised with external deliveries from other institutions and partners. When changes are made, including purely technical changes, some dependencies may not be taken into account. Dependencies between systems are not always adequately documented. Agreements on and procedures for cooperation among the various operators in the event of faults are not always good enough.

Operating error of this type may be difficult to pinpoint. Re-runs and corrections may be necessary, possibly resulting in service unavailability that may impact both institution and customers.

A number of reported incidents in 2016 were due to shortages of resources such as hard disk space, memory or network capacity, or too few threads in a process. Monitoring and traffic analysis appear to be inadequate. It should be possible to remedy these inadequacies with a reasonable application of resources.

Testing changes in the production set-up is challenging, partly because it is not feasible, financially or practically, to establish and maintain a complete test environment with applications, systems, data and traffic corresponding to a full production set-up.

Change processes

Change implies a large inherent risk of error.

In 2016 there was a decline in the number of incidents that can be attributed to errors in change processes, even though there were substantial system changes during the year.

New methods of executing financial services may result in large-scale restructuring of the market. Banks and suppliers of payment services may have to change substantially as a result of further automation in credit and payment systems. The new Payment Systems Directive (PSD 2) paves the way for the entry of new types of operators into the market for payment services and account information.

As a result of new regulatory requirements, institutions will have to make extensive system changes and innovations in 2016 and 2017.

Concentration risk

The core systems of the banks are operated in different places. Nordea and DNB operate their own core systems, the systems of the Eika banks and some small banks are operated by SDC, and those of the other savings banks are operated by Evry. Branches of foreign banks in Norway also have different systems, mostly operated by their parent bank. The concentration used to be greater, and an incident would then put large parts of the financial industry out of operation. There is less probability now of one incident affecting several institutions at the same time.

However, the payment systems infrastructure is largely concentrated within Nets, which means high vulnerability.

The insurance and securities industries tend to have operations located at multiple sites.

Business continuity

The incidents reported in 2016 show that business continuity systems do not function as they are supposed to in many instances. This may be due to set-up complications, to back-up systems not being updated in step with changes in the environment, or to back-up solutions not being tested after changes in the environment.

Some major operators tested their business continuity systems in 2016. Since then, Finanstilsynet has been more confident that these systems will function according to expectations in an unplanned situation.

Smoothly functioning business-continuity solutions have been established for payment card infrastructure.

Expertise and capacity

There is great demand for IT expertise generally, not least in the public sector. There is currently great competition to get first to the market with new financial services. The inherent risk of faults and deficiencies is growing. Discipline with respect to quality and control is being tested.

6.3 Users and consumers

Risk associated with use of e-trading systems for securities trading

Access to correct information and the possibility of conducting trades on the basis of this information are critical success factors for all users of electronic securities trading systems.

Electronic securities trading is conducted by different types or categories of users with different needs and different appetites for risk. Users who trade shares intermittently (weekly, monthly or annually) use their e-trading system mainly to monitor developments in their portfolio. Trading usually takes place with security in the customer's bank account and the settlement is an internal exchange between cash in a bank account and securities in a custodian account. This category of users is rarely exposed to such a high level of risk that they need to make acute changes in their positions.

More active users who want high exposure use credits and derivatives, and prefer to use systems with built-in granting of credit without a bank connection. This means that users of these systems are not dependent on banking systems to conduct transactions, and thus have a considerably lower risk of disruptions in their access to the system. The same investment firms often offer several types of solutions geared to different user groups.

User groups are excluded

The industry has reported that Norway has an efficient payment system because payment system providers are innovative and quick to eliminate old systems. One well-known way to eliminate old systems is to increase prices for these services and to discard manual solutions, whether they be paper-based payments, ATMs or offices. This impacts users who are not as well placed to use digital solutions, including many older consumers.

Users incur risk

Payment systems should not impose more risk than necessary on customers. Large customer groups, for example elderly consumers, only use cards in physical shops and ATMs. At the same time, we know that the amount of fraud associated with unauthorised³¹ use of cards on the Internet is substantial and increasing. Guidelines for Internet payment security stipulated by the EBA require that consumers must be able to lock their cards for use online. Some payment system providers have still not introduced this safeguard for their cards.

³¹ Unauthorised means that the customer has not consented to the use.

7 Monitoring by Finanstilsynet

7.1 Key areas for Finanstilsynet's ICT supervision

Supervisory activities are risk-based.

Finanstilsynet will be focusing on the supervisory agencies and suppliers that have the greatest influence on financial stability and smoothly functioning markets. Financial institutions that make major changes in their ICT function, thereby potentially increasing their operational risk, will be particularly subject to scrutiny. Other topics calling for monitoring are the institutions' control of all types of access to systems that contain sensitive information, contingency preparedness in connection with business continuity and response to crises, risk assessments, recording of telephone conversations and the development of new solutions entailing the use of new technology. Priority will be given to cyber security in the institutions' ICT systems and the organisation of surveillance.

Supervisory activities will also extend to the institutions' risk assessments with respect to outsourcing of ICT and the quality of agreements and follow-up of agreements between institutions and suppliers. Money laundering and systems for financing terrorism will be monitored.

7.2 Work with payment systems

Finanstilsynet will monitor the institutions' payment services with respect to new regulations³² to the Payment Systems Act and compliance with the notification requirement.

Compliance with guidelines for secure internet payments will be monitored through spot testing and penetration testing of Internet-based systems.

Collaboration with Norges Bank will continue.

7.3 Follow-up of incidents

Finanstilsynet will closely monitor developments in serious incidents, and place emphasis on finding the cause(s) and taking steps to prevent recurrence.

In serious cases of non-compliance, follow-up meetings will be held as needed.

³² Regulations relating to payment service systems (Norwegian text)

7.4 Contingency preparedness

The work of the Contingency Committee for Financial infrastructure (BFI) will continue. This includes reviewing incident scenarios and determining whether the responsibilities associated with crisis situations are sufficiently clear. Exercises are being planned for 2017 as well.

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

7.5 Monitoring of the threat picture associated with cybercrime

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

- contingency preparedness work targeting digital vulnerability and security
- changes in payment mediation, both through the use of new technology (FinTech) and through extensive cross-border activities.

7.6 Consumer protection

Finanstilsynet will place emphasis on institutions taking customer security seriously and protecting customer data against sharing without consent or falling illegally into the possession of third parties.

Copying of the magnetic strip on cards is the most common method of acquiring information in Internet fraud; see 3.1.7. Going forward, Finanstilsynet will follow up card providers' compliance with the rules concerning use of magnetic strip terminals.

8 Glossary

Term/abbreviation	Meaning
AML	Anti-Money Laundering
Baltus	Banks' online transaction exchange system. The network used by banks for transaction exchange and to check the balance of accounts in each other's accounting systems.
BFI	Contingency Committee for Financial Infrastructure Committee to coordinate action in the event of financial sector crises. Chaired by Finanstilsynet.
Bits	Bits AS is the banking and finance industry's infrastructure company
Botnet	A term compiled from the words 'robot' and 'network'. A network of programs on various servers linked together via the internet. The programs work together on a given task
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. Team of experts who deal with cyber security breaches
CLS	Continuous Linked Settlement
CNP	Card Not Present. Fraud with the aid of stolen card data, mainly in connection with online trading
DDoS attacks	An Internet attack that overloads a server by directing a huge amount of traffic at the server, usually by means of a botnet. The purpose is to prevent normal access by ordinary users
DLT	Distributed Ledger Technology. A distributed general ledger can be regarded as a type of database that is shared across nodes in a network
DNS	Domain Name System
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
EMIR	The European Market Infrastructure Regulation
ESMA	European Securities and Markets Authority.
FATF	Financial Action Task Force. Membership organisation for countries, of which Norway is a member. Established to set standards for AML and anti-terror financing
FCA	Financial Conduct Authority, UK

FinansCERT	Norwegian financial sector cybercrime unit
FinTech	Financial technology, used for technological innovation in the finance sector and also about institutions in the sector that employ modern technology
Internet of Things (IoT)	Technological devices linked to the Internet. Examples are surveillance, access control, process control and video systems. The concept also includes sensors deployed to gather data. Many devices have built-in computers and can communicate with other devices and services. The technology enables services to be performed anywhere, anytime
ISO 20022	ISO standard for financial messaging
ISP	Internet Service Provider - supplier of internet access and domain names
MAS	Monetary Authority of Singapore
NBO	Norges Bank's Settlement System.
NICS	Norwegian Interbank Clearing System
NFC	Near Field Communication. Used in payment cards and mobile phones for contactless payment
NSM	Norwegian National Security Authority
Offshoring	Procurement of services from outside the country. Sometimes used to refer to procurement outside the Nordic/Baltic regions
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
Privacy Shield	Agreement between the EU and the USA. Security in connection with transmission of information between the parties. Entered into force on 12 June 2017
PSD 2	New payment services directive from the EU
PUM service	Personal delivery with confirmation of receipt. Secure delivery service for small dispatches delivered by Bring, a Nordic delivery service
QR Code	Quick Response Code is a mosaic code for commercial and personal use. It can store a large number of alphanumerical characters and can be read quickly. It is therefore highly suitable for optical reading of data such as an address
Ransomware	Malware that restricts or prevents access to ICT systems and demands a ransom
SecuRe Pay	European Forum on the Security of Retail Payments – forum under the ECB
Strong authentication	Authentication employing several methods, e.g. pin code + password
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TFIT	Taskforce on IT Risk Supervision – EBA working group
TFPS	Taskforce on Payment Services – EBA working group
TR	Trade repository
Trojans	Viruses that pretend to be ordinary programs, but that contain malware
TRS	Transaction reporting (securities)
Waterholes	A digital attack strategy where the victim is a group of organisations or type of industry (in this case financial). The attackers infect websites the selected group is assumed to visit often with malware that is transmitted to guests

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