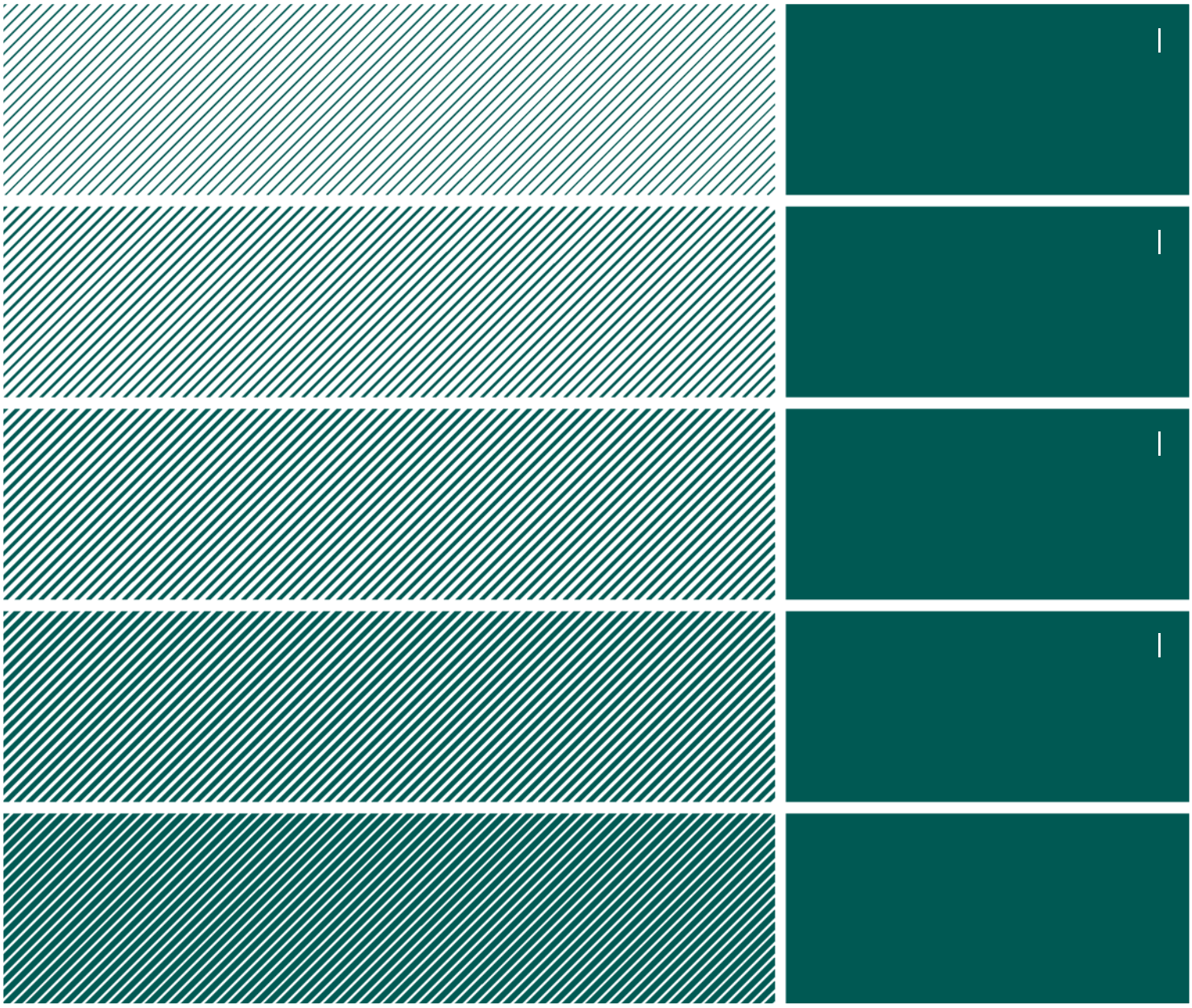
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Report

Risk and Vulnerability Analysis 2013

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



Risk and Vulnerability Analysis (RAV) 2013

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

Finanstilsynet, April 2014

Contents

1 Introduction

The Financial Supervisory Authority of Norway (Finanstilsynet) performs an annual risk and vulnerability analysis (RAV analysis) of the financial sector's use of ICT and solutions for the provision of payment services. The RAV report is based on data from a variety of sources, and contains assessments of the potential impacts of identified risks on the financial sector in Norway.

Technological advances take place rapidly in the financial sector, giving rise to new services. However, new technology often contains unknown vulnerabilities. Enterprises face demands to improve the quality of their services and solutions, rationalise their operations and cut costs. These demands are made by shareholders, management, customers and public authorities, and call for change management and risk management.

Although use of the Internet offers a multitude of possibilities, it also paves the way for global electronic crime. So far, this issue has been adequately addressed by individual institutions and the financial sector as a whole in Norway. The threat will remain global, and Norway may be the subject of attacks that are both unexpected and involve the use of unknown methods. It is imperative that we continue to give priority to preventive efforts and take swift action to deal with vulnerabilities and risks in an appropriate manner.

The aim of Finanstilsynet’s annual RAV report is to describe changes in the risks related to the financial sector’s use of ICT and payment services. The glossary at the end of the report explains key terms and institutions.

2 Summary

Developments

Technological advances in the financial sector bring a need for changes in regulatory frameworks, services and infrastructure. The combination of these changes represents an increased risk. New technology can introduce new and unknown vulnerabilities, creating greater risk. Change also takes place at the organisational level in financial institutions, infrastructure institutions and major ICT service providers, which can heighten vulnerability.

Digital marketplaces for trade in and distribution of electronic services offer the financial sector a wide range of possibilities, but also attract organised criminal groups which largely attack payment services. This form of crime is international and unobstructed by national borders. New operators which are not subject to Norwegian law and which operate in a borderless Internet community, create challenges for customers, Norwegian financial institutions and public authorities alike.

Through the EEA Agreement, new EU rules are being introduced with a view to ensuring a safer financial sector. However, the totality of these changes could pose challenges for both financial institutions and authorities. Implementing the changes, including systemic changes, could entail a risk.

Use of smart telephones and tablets is rising sharply, and financial institutions are launching numerous new services that can be accessed using these devices. These changes could lead to higher risk that is not adequately identified or managed, and financial institutions must adapt to these developments.

Finanstilsynet's findings and observations

Finanstilsynet largely uses its own data sources for the RAV analysis. The primary source is the results of inspections that have been carried out, followed by financial institutions' reporting of IT-related incidents. Finanstilsynet has built up a comprehensive database containing information on registered incidents, and analyses this information to obtain insight into current areas of risk. Every year, Finanstilsynet conducts interviews with major financial institutions and important service providers and infrastructure operators. Finanstilsynet also carries out targeted surveys in areas involving use of new technology and services which could present unknown risk.

Current areas of risk identified in the 2013 analyses

1) **Extensive changes in the financial sector's IT-related activities**

Several of the large financial institutions are implementing, or plan to implement, extensive changes in their ICT activities, in term of both systems and operations. Examples of changes include replacement of service providers and operating facilities, changes in operational procedures and operations architecture, insourcing and increased use of offshoring. Several of the changes entail personnel changes, such as restructuring and downsizing.

Generally speaking, changes lead to increased operational risk. It is evident from the interviews that change management is considered to be one of the greatest risks. In Finanstilsynet's experience, the majority of and the most significant incidents reported have occurred in connection with changes. It is essential that institutions control and manage the

risks related to the ongoing, wide-ranging changes.

Although individual institutions might believe that their changes and risks are under control, it is Finanstilsynet's opinion that the sum total of the changes poses a substantial risk to Norwegian financial infrastructure and stability. It is important that this risk is understood and that every attempt is made to mitigate it.

2) Interaction between several service providers

Many changes entail the involvement of a variety of service providers in the value chain of one and the same institution. Where there was previously a single main IT service provider, services and deliveries are now divided between several suppliers (multisourcing).

Such a model can present certain advantages. However, Finanstilsynet is of the opinion that the model may lead to unclear distribution of responsibility and inadequate interaction and coordination, which may in turn create greater risk, particularly in a critical situation. Finanstilsynet refers to the "Easter incident" in 2011, when precisely the lack of interaction was a key problem. Multisourcing may make it difficult for the institution to gain an adequate overview and control of the risk in the totality of its outsourced IT activities. Risk management and clearly worded contracts are therefore absolutely essential.

3) Inadequate risk assessments

In earlier RAV analyses, Finanstilsynet has pointed out that risk assessments and risk management are clearly an area of potential improvement in financial institutions. This area still appears to present a challenge. Most financial institutions prepare annual risk assessments in accordance with the provisions of the Norwegian Risk Management and Internal Control Regulations and the Norwegian Regulations on the Use of Information and Communication Technology (ICT Regulations), but the quality of this work varies. In Finanstilsynet's general experience, risk assessments and risk-mitigating actions are not followed up systematically. It is not always apparent that the actions have been carried out or that they have had the anticipated impact on the risk.

4) Attacks on payment services

Payment services are still under criminal attack. This applies to most electronic channels through which the payment services are digitally distributed all the way to the customers. In several areas, bank losses showed a marked decline in 2013. However, there was a marked increase in losses related to the use of payment cards in online stores, i.e. "card-not-present" transactions. This may be linked to the large-scale hacking of the databases of international operators which contain payment card numbers.

5) Risk due to outdated design

In previous years' RAV analyses, Finanstilsynet has pointed to the increasingly urgent need to replace older legacy systems with new ones. One of the reasons is the need for flexibility and data collation. Another reason is the challenges inherent in maintaining up-to-date copies of basic data so as to be able to provide an accurate picture of the overall customer base.

Modern systems, on the other hand, consist of layers of homogeneous functions that are linked to the services by means of program calls (enterprise service bus). These program calls are reused across services.

Furthermore, knowledge of legacy systems is gradually fading, making maintenance and

operation of such systems increasingly challenging.

Finanstilsynet's further efforts to monitor developments

Finanstilsynet will continue to give priority to close collaboration with key players in the financial sector, to ensure that the sector understands both the level of risk and the challenges that institutions must meet. There will be emphasis on securing insight into institutions' contingency systems and on making sure that institutions take necessary action to ensure that they are effective.

Payment systems and trends

The report assesses risk related to individual payment system services, change processes and new products and services that may represent a risk. This risk consists chiefly of planned malicious attacks, but also of unplanned incidents that might threaten the stability and quality of services. In Finanstilsynet's opinion, the payment services are generally stable and of satisfactory quality. Nonetheless, serious non-conformities do occur.

Efforts to promote higher quality in both financial institutions and their service providers will continue. Although attacks on payment services do occur, losses are still moderate. This is largely due to measures put in place by individual institutions and the sector as a whole, such as the establishment of FinansCERT. Had the sector not taken relevant preventive action, estimates show that the losses would have been extremely high. The crucial process of implementing preventive and other measures must continue. Payment systems in Norway are dependent on the close collaboration of a variety of players, shared solutions and engaged service providers. It is therefore essential that management and control be made a priority and that concerted efforts to establish shared systems and infrastructure continue. Furthermore, it is important that accurate, candid information is provided on losses related to payment services, and that developments are monitored over time. This also ensures that consumers and financial industry operators are kept informed.

The securities area

Particular attention is focused on the topic of securities in the report since wide-ranging changes are taking place in this sector, the collective impact of which could constitute a risk. The changes now being seen are also affecting possibilities for revenue generation and may reduce the funding available for necessary measures to renew and assure quality. Legacy systems may pose a challenge, while replacing them may also entail risk. Significant changes in regulatory frameworks will affect infrastructure and securities institutions in the EU. New electronic marketplaces for cross-border securities trading are also affecting the volume and revenues of the traditional operators. Hence there is a great need for changes in this area.

3 General trends

This chapter describes changes in regulatory frameworks, technology and service trends in Norway and worldwide.

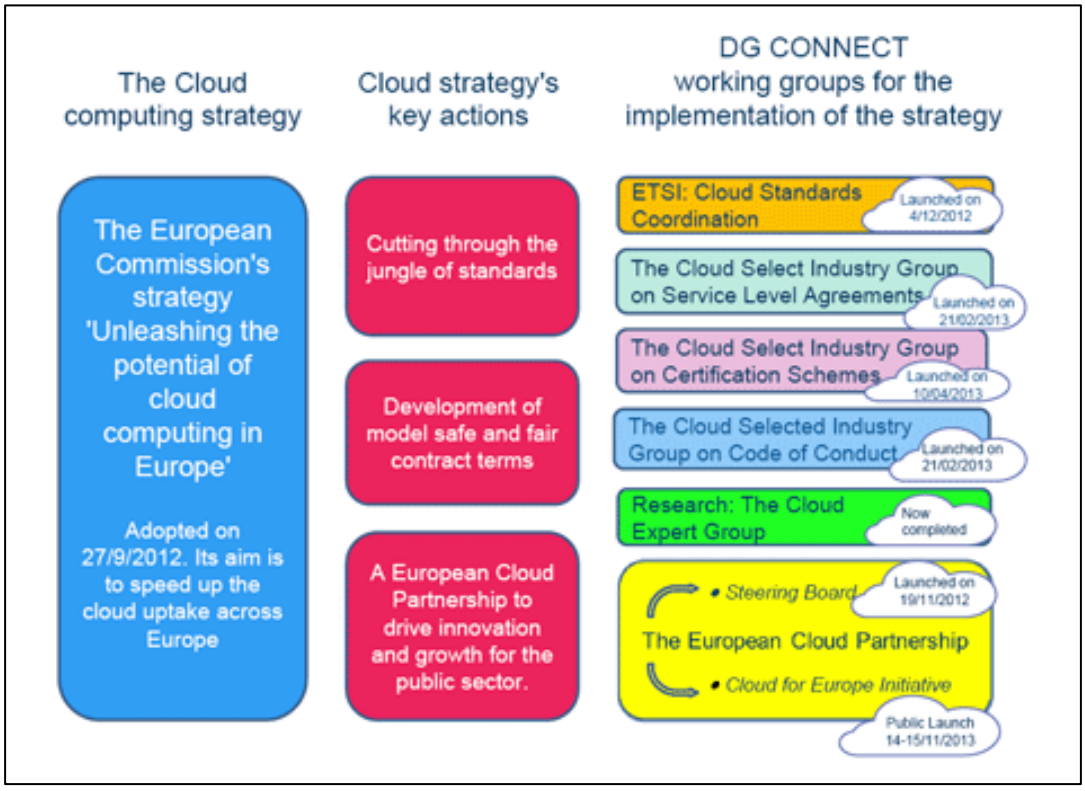
3.1 Cloud computing trends in the EU

In September 2012, the European Commission launched its cloud computing strategy: "Unleashing the Potential of Cloud Computing in Europe",[1] aimed at increasing the number of jobs and generating higher GDP in Europe. The strategy is designed to promote cloud computing in all economic sectors, and working groups have been established to implement a range of identified measures.

The strategy consists of three key actions:

1. Simplifying standards
2. Recommending model contracts that ensure safe and fair contract terms
3. Fostering partnership, innovation and growth in the public sector in the EEA

Figure 1: Cloud Computing Strategy and Actions



Source: European Commission[2]

[1] Digital Agenda for Europe – European Commission http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

[2] http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

The most important working groups whose activity could impact on electronic financial services are:

- The European Telecommunications Standards Institute (ETSI) coordinates standards for cloud computing and electronic signatures and works with stakeholders to establish standards designed to support EU strategy in this field.
- The Cloud Select Industry Group on Service Level Agreements, which targets consumers and SMBs.
- The Cloud Select Industry Group on Certification Schemes. With the help of the European Network and Information Security Agency (ENISA) and other institutions, the group seeks to assist the development of a voluntary certification scheme for cloud computing.
- The Cloud Select Industry Group on Code of Conduct aims to promote the uniform application of data protection and processing rules.
- The Cloud Computing Expert Group on Research. The work of the Group has informed the EU's Strategy, and provided guiding principles for research areas.
- The European Cloud Partnership, which advises the EU Commission on opportunities for new growth in this area. The aim is to bring together industry and the public sector to create a uniform market for cloud computing in Europe.

Work on compiling a list of standards has been completed, and the final report, Cloud Standards Coordination,[3] was published in November 2013. The report provides a full overview of standards and specifications for cloud computing. The report targets cloud service providers, cloud service purchasers and regulating authorities.

Although cloud computing has been standardised to a certain degree, further developments are expected in this domain.

One of the areas that the report identifies as a challenge is establishing standards for agreements regulating the relationship between service providers and purchasers of cloud computing services. In its outline of the life cycle of a cloud service agreement, the report refers to relevant reports and standards relating to the various phases of the agreement period. The report has sought to identify all initiatives related to cloud computing standardisation and specifications. Since the infrastructure on which cloud computing is based is complex and comprises numerous components, there are many different organisations in the fields of security, telecommunications, power supply and other sectors that have established or are in the process of drawing up cloud computing standards, specifications and overviews.

3.2 Coordination of and changes in the EU regulatory framework

In 2013, the EU proposed a number of amendments to existing directives and also proposed directives, regulations, technical standards and guidances relating to payment services and systems. These proposals have been circulated for consultative comment. In their present form, some of the proposals will probably result in changes in the IT systems used by the financial sector and payment service providers. The proposed amendments may also bring

[3] http://ec.europa.eu/digital-agenda/en/news/cloud-standards-coordination-final-report

changes in the distribution of responsibility and risk among the players in the payment service value chain, and they may introduce new risks. A possible undesirable consequence is that customers find it less safe to use payment services, which would in turn reduce trust in such services.

The proposed amendments are comprehensive and thus represent a potential compliance risk. In general, changes in a system portfolio are one of the primary causes of system error. Wide-ranging changes in the regulatory framework which are implemented over a short period of time could entail a risk.

3.2.1 Regulation on electronic ID and trust services for electronic transactions

A Regulation governing electronic ID and electronic signatures has been proposed. Although it mainly concerns electronic interaction with public administrations, the security technology and other aspects, for instance in connection with identification and levels of security in payment systems, will have repercussions in every area of society. It is proposed that the European Commission should be able to decide the highest security level in areas where neither individual states nor Norway have regulatory influence. The Norwegian Ministry of Justice and Public Security[4] has expressed concern about potential serious consequences for the crime situation and public security in Norway if the level of security prescribed in the Regulation is too low and Norway is unable to determine its own level.

3.2.2 New Payment Services Directive (PSD2)

The EU has proposed a new Payment Services Directive (PSD2).[5] One of the main objectives is to expand the regulatory scope of the existing directive to cover Third Party Payment Service Providers (TPP). TPPs do not provide account services themselves, but offer customers payment services by acting as an intermediary between the customer and the customer's bank. Customers thereby commission the TPP to initiate payments on their behalf. The TPPs base their services on customers' existing bank accounts. Facilitating such activities through regulation creates new, complex operational and legal interactions in payment service value chains (between TPPs, banks and customers). These interactions will introduce new interfaces and may entail new risks and vulnerabilities. As a result, customers may experience reduced security when using payment services and their confidence in the system may be undermined.

Under the proposal for a revised Payment Services Directive, a TPP would have access to account information in the customer accounts of the account-holding bank or payment institution, and would be able to effectuate payment transactions in the same way as if the customer made the payment order directly to his own bank. Such access, which entails a separation of account-holding and payment services, could result in diminished interest in the

[4] http://www.regjeringen.no/nb/sub/europaportalen/eos/eos-notatbasen/notatene/2012/okt/forslag-til-forordning-om-eid-og-esignat.html?id=728989

[5] Payment Services Directive:
Norway is otherwise well prepared in this area through the existing regulatory framework, the Norwegian National Security Authority's Norwegian Computer Emergency Response Team (NorCERT) and the establishment of a separate Financial Computer Emergency Response Team (FinansCERT)

maintenance and development of underlying, effective payment infrastructures. If third parties are also given the right to access private and confidential log information which the customer has received from his bank, a number of security and liability issues arise. Giving TPPs access to customer account information could raise privacy issues. If, in addition, provisions are adopted that prohibit contractual relationships between banks and TPPs, the question of liability in the event of loss or misuse becomes unclear.

Another key area covered by the proposal is the requirements relating to payment service providers' management and control of risk and incident reporting. Many of the requirements for risk management and incident reporting[6] have already been implemented in the Norwegian ICT Regulations, but there are other requirements that could necessitate more stringent reporting requirements in Norway.

3.2.3 Proposal for revised guidelines on Payment Services Directive Passport Notifications for payment institutions[7] and e-money institutions[8]

In connection with the revision of the Payment Services Directive, a number of improvements and changes have been proposed in the guidelines for notification by one EEA country (home Member State) to another regarding permission for an institution to engage in activity in the other EEA country based on consent granted in the home Member State. The aim is to standardise and simplify the process of establishing a branch for institutions operating within the EEA. This includes institutions offering payment services and e-money.

3.2.4 Regulation on interchange fees for card-based payment transactions – the Multilateral Interchange Fees (MIF) Regulation[9]

The EU has proposed a Regulation on interchange fees for card-based payment transactions. The purpose of the Regulation is to increase market competition by regulating interchange fees, organising processing procedures and regulating business models. Provisions have also been proposed which could have an impact on the current "priority rule"[10] in the Norwegian national payment card system (BankAxept), which could in turn reduce the efficiency of the Norwegian payment system and lead to increased use of international cards with the higher costs that such use would entail for consumers. This Regulation may lead to changes that will introduce new areas of risk and vulnerability. The proposal may also lead to a reluctance to invest in developing payment infrastructures that are crucial to trade.

---

[6] http://www.finanstilsynet.no/no/Artikkelarkiv/Rundskriv/2009/4-kvartal/Rapportering-av-IKT-hendelser-til-Kredittilsynet/

[7] http://ec.europa.eu/internal_market/payments/docs/framework/transposition/passporting_guidelines_en.pdf

[8] http://ec.europa.eu/internal_market/payments/docs/emoney/passporting_guidelines_en.pdf

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0550:FIN:EN:PDF

[10] Under the priority rule, BankAxept is given highest processing priority when combined cards are used in payment terminals.

3.2.5 Directive concerning measures to ensure a high common level of network and information security (the NIS Directive[11])

The aim of the directive is to ensure a high common level of network and information security (NIS) for EU member states. It is proposed that the directive also apply to the financial sector and its players.

The goal of the proposed directive is three-pronged:

1. Establish national NIS authorities, set up Computer Emergency Response Teams (CERTs) and adopt national NIS strategies.
2. Ensure cooperation between national NIS authorities within the EU/EEA.
3. Ensure the development of a culture of risk management and information-sharing between institutions in the private and public sectors. The institutions will be required to adopt necessary security measures and to report any serious incidents in their network and information systems.

Norway is otherwise well prepared in this area through the existing regulatory framework, the Norwegian National Security Authority's Norwegian Computer Emergency Response Team (NorCERT) and the establishment of a separate Financial Computer Emergency Response Team (FinansCERT).

3.2.6 Changes in anti-money laundering rules

The European Parliament has presented a proposal regarding requirements that information concerning the payer must follow the entire payment chain. A proposal for a new Anti-Money Laundering Directive has also been put forward. This proposal maintains the principal rules, but includes a number of clarifications, elaborations and changes.

3.3 Norwegian financial institutions and cloud computing

Norwegian banks have outsourced their banking solutions ever since the banks began to use IT in their banking operations. Services are extensively outsourced in the insurance sector as well. New technology is now available which makes it easier for service providers to offer both increased storage and processing capacity, which can be spread between multiple data centres in different locations.

As a rule, the solutions offered by most of the major players are general and can be used by several different sectors without requiring special adaptation. This creates economies of scale and ensures effective control of processes such as problem and change management. The international service providers that offer cloud computing services have largely drawn up agreements that are the same for all their customers. The agreements are often formulated in such a way that it may be difficult for the purchaser of the service to have control of his own data and knowledge of the risk inherent in the infrastructure. This is the case in particular if the agreement limits the customer's insight into the part of the service providers' infrastructure that is used by the customer's solutions.

[11] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

Use of cloud computing is to be regarded as outsourcing, and section 12, Outsourcing, of the ICT Regulations, which sets clearly defined requirements for outsourcing contracts, therefore applies without exception. Institutions must be aware of and have control of all risk relating to their own use of ICT. Even where all or parts of the ICT activities are outsourced, the institution is responsible for the service provided. Agreements must give the institution the right to inspect and control the activities of the ICT service provider that are covered by the agreement. The agreement must further ensure that Finanstilsynet has access to information held by the service provider if Finanstilsynet deems this to be necessary as part of its supervision of the institution.

In the past few years, there has been growing focus on contingency preparedness and institutions' business continuity and disaster recovery plans. The Regulations' provisions on contingency preparedness lay down specific requirements which must be complied with even when the task is outsourced.

3.4 Organisation and ownership

In November 2012, Nets Norway AS (Nets) announced changes in the organisation of the Nets Group. In the light of a possible spin-off of Nets' Norwegian operations, Finanstilsynet pointed out to Nets that it would need to clarify the banks' right to use the solutions for the banks' shared payment services and shared infrastructure. Many of the shared solutions that Nets administers and runs as a service provider for Finance Norway and the banks, such as key elements of BankAxept and BankID, are necessary components of the banks' payment systems. Finanstilsynet has also pointed out the importance of managing and maintaining control of shared operational infrastructure, particularly in a contingency situation, and the challenge that this may present if some of the activities take place outside Norway. Finanstilsynet pointed out to the banks that they are responsible for delivery of Nets' solutions in key areas of the payment systems in Norway, and that it is the banks' responsibility to ensure necessary management and control in order to keep risk at an acceptable level.

3.5 Changes in the sourcing landscape

Several international service providers are of interest to Norwegian financial institutions. For the financial institutions, profitability is a driving force in the search for new opportunities, but stability, quality and flexibility are also emphasised as being important factors. Service providers have their strengths and weaknesses, often in different products in the view of the purchasers. As a result, some institutions use several different service providers. In 2013, several large financial institutions and some service providers announced that they were changing system suppliers and systems in important areas, or that they were in the process of considering a new supplier.

This trend is giving rise to problematic changes for the players involved, and comprehensive agreements must be put in place. Experience has shown that changes are the greatest source of ICT error for financial institutions. A change of service provider therefore calls for thorough risk analyses. Managing fault situations in value chains involving several service providers will be particularly challenging. The payment card incident at Easter in 2011 showed that it is difficult to take swift collective action to control damage when there are several service providers in the value chain.

In the long term, loss of local technical know-how and experience may also weaken financial institutions' purchasing expertise where these services are concerned.

3.6 Collective action by the financial industry

Banks, other important financial sector players and Finance Norway work together to promote security, the development of shared infrastructure, services and common standards. The results of incidents, surveillance, analyses and statistics are exchanged and discussed, and measures are adopted.

The Norwegian Banks' Standardisation Office (BSK) has begun work on modernising the Banks' On-line Transaction Exchange System (BALTUS), which is the network for the routing and transport of transaction-related financial information and inquiries among banks in the common payment system infrastructure in Norway. "Baltus 2.0" is intended to be a modern network in which message content and header information will be separated to accommodate more levels and paths in the system. This change is scheduled to be carried out by the end of 2015. BSK has also commenced work on a "road map" for the transition from current national and international payment system standards to ISO 20022. EU regulations require that ISO 20022 be made the mandatory format for customers' submission of payment orders. Both of these measures will lead to changes in shared infrastructure and changes in the systems adopted by the various financial institutions. The ISO 20022 requirement will also necessitate changes in companies' ERP systems for exchange of payments and payment information with financial institutions. In the long term, this will lay the basis for standardising and simplifying corporate customers' procedures.

In 2013, Finance Norway established shared operational infrastructure for fast payments,[12] and launched a limited pilot project. The fast payment system makes it possible for customers to make a payment that is perceived as taking place in real time at any time of the day or night. The transferred funds are immediately made available in the payee's account, while the inter-bank settlement takes place afterwards through the ordinary settlement cycles. Each bank must develop its own customer systems, using either online banking or mobile banking. In order for the payer to be able to use this service, both the payer's and the payee's banks must be linked to the operational infrastructure.

BankID Norge is preparing to launch BankID version 2.0, which will be a Java-free BankID.[13] The new version will use a browser, requiring no installation of any other software or downloading of apps, and will be available on a broad range of devices. The new system, which is to be introduced in the autumn of 2014, will eliminate vulnerabilities and do away with problems experienced by users in connection with Java. The Java-based BankID is expected to be phased out relatively quickly, although no deadline has been set for the phase-out.

In 2013, Finance Norway and relevant financial institutions established FinansCERT Norge, a Norwegian financial sector cybercrime unit. The purpose of this unit is to maintain and strengthen monitoring, response and information exchange with regard to IT security incidents in the financial sector.

[12] http://www.sparebankforeningen.no/id/17811.0

[13] https://www.bankid.no/Presse-og-nyheter/Nyhetsarkiv/2013/BankID-20-uten-Java-lanseres-hosten-2014/

Through Finance Norway, institutions are adopting a business orientation by establishing dedicated companies for shared services such as BankAxept and BankID. These shared services also include a shared infrastructure and are a key component of the banks' range of payment and Public Key Infrastructure (PKI) services. BankAxept's business orientation is aimed at meeting tougher price competition in the market, ensuring the sustainable development of services and meeting market demand for new payment systems. The goal is still to deliver a stable, efficient and competitive payment system. By giving the banks' PKI system a business orientation, the aim is to ensure the continued sustainable development of BankID, develop additional services and promote wider use.

3.7 Technical developments and risks/threats

3.7.1 Mobile banking

The use of mobile banking has increased at a rate unequalled by any other banking service. Mobile banking has a number of "old" and "new" vulnerabilities, which may in time pose a significant risk to payment systems.

The most common sources for obtaining applications are Apples App Store for iOS and Google Play for Android. In addition to these, Android offers the possibility of installing apps from any source that contains an Android application. In the case of iOS, the telephone must be "jailbroken"[14] to enable the user to install applications from other sources. Many unofficial app stores offer both pirate versions and infected versions of well-known applications. Using bank apps that have been digitally signed by the bank ensures higher security. The bank should actively encourage customers to increase security by checking the signature and the app certificate. The bank should also enable the user to download apps via a link on the bank's website to App Store or Google Play.

The principle that an app runs in a self-contained area (sandboxing) applies to both operative systems. The security provided by sandboxing is naturally dependent on the developer utilising this technology, keeping code and data inside the "sandbox". However, studies show that apps can "leak" data, such as when sensitive information is sent to open logs. The fact that some development communities are not mature enough to make sure that all security norms are followed constitutes a risk.

Mobile devices have security features and secure storage areas designed to protect keys and programs against unauthorised use. Some users remove this protection by "jailbreaking" (Apple) or "rooting" (Android). Attackers are then able to gain access to codes, keys, log-in details and data capsules, and can install malware that steals log-in codes and other sensitive information.

Studies indicate that mobile device users have a tendency to click on malicious links, partly because the short URLs on the mobile device do not reveal the attacker. Attackers have succeeded in stealing both the user's log-in codes, which were texted to the user as SMS codes, and codes sent online. In this way they appropriate the customer's money, as in the case of Eurograbber, a "two-pronged" attack.

[14] Change in the telephone's security settings

With the help of the MAC address on the user's PC, the bank can link a user to his PC. The bank can thus stop an attacker who logs in from his PC using stolen codes. Mobile devices do not have an identifier of this type and cannot be controlled effectively in this way. However, functions can be incorporated into the app which build an identifier that can be used for this type of verification. The principle of mutual authentication should be applied, so that the customer can authenticate the bank and vice versa.

One way of reducing risk is to place each bank session in a context that generates a risk score. The bank should assess the telephone's location (if the user permits this), IP address, security updates, break-ins, system configuration, infections and use of unsecured wireless networks before allowing the user to access the bank. The information should be cross-checked with the customer's use pattern. The user, for his part, should only download apps via the bank's website and keep his mobile device up-to-date and virus-free.

Use of data capsules may, in time, pose a risk. They are more and more common in apps, the use of which is also escalating, thereby expanding the proliferation of such capsules. Data capsules that are stored on a bank customer's PC may be read, stolen and possibly changed. This also applies to capsules used in HTTPS sessions. Online banks use data capsules on both PCs and mobile phones. This situation calls for vigilance on the part of both banks and users. Trojan attacks remain a challenge, often occurring in connection with phishing and DDoS attacks. Tablets and smartphones have seen a rise in the number of virus infections, the Android system being particularly vulnerable. Since there are no real anti-virus programs or firewall solutions for this type of device, virus infections are a risk given the growing number of telephone services now being offered. The development of malware for mobile devices lies many years behind malware targeting PCs. Although the risk is low at present, it can be expected to increase in the years to come.

A further risk is posed by weak encryption in parts of the mobile network.

3.7.2 Big Data

"Big Data"[15] is not a standard product, and potential users must therefore have a clear idea of what they want to achieve in order to obtain the expected benefit of a Big Data investment. Many start out with what they have, such as a data warehouse, and use business intelligence tools, often in combination with data visualisation tools. Good solutions are gradually becoming available in this domain. Data capture from new sources, such as public registers and social media, is used when needed in specific applications and for business processes. Data volumes are growing rapidly, which may create a data management problem rather than a support for business processes. There is a need for swift processing of fresh data, requiring powerful tools. Several operators are already on the market, and powerful Big Data search engines are expected to become available in the near future.

Big Data can be used in many connections, such as to gain better insight into a company's existing customer base, identify trends and needs for new products and, not least, for cross-selling. Another area emphasised is the use of Big Data to support decision-making by

[15] "Big Data" is an IT term used to describe the collection, storage, analysis, processing and interpretation of large amounts of data. The data may be both structured and unstructured. Big Data is often used for marketing purposes.

drawing on data from outside a company's own business activities. It can also be used to compare similar situations, reveal anomalies and identify any systematic deviations relating to individuals or groups. Analyses of customer data may also be shared with the customer, providing him with added value transcending that of traditional data. A typical example could be an analysis of buying patterns and spending habits (stores, travel, restaurants, experiences and the like), beyond the data provided in simple bank account statements. Some banks already offer such services.

Big Data can provide businesses with useful information, but it may also entail a risk in some areas. Information can attain a saturation point at which additional information generates no added value. Some warn against the danger of relying too heavily on analyses of large amounts of data. If the data administration is poor, systematic errors may occur in the basic data, or the data may become outdated. Mistakes may also be made in the analyses themselves. There may be too much smoothing for deviations and anomalies to be detectable, or too little, so that the results are mainly "noise". If an institution then believes it is in possession of all the knowledge, it may make seriously erroneous decisions. Decisions made by the institution may have significant, wide-ranging consequences for many customers, while mistakes made by individuals seldom affect anyone but themselves. This type of knowledge can only be built up over time, and effective procedures are required for the use of Big Data analyses.

Big Data may involve the use of personal data, which is regulated by law. The EU is currently preparing a new directive on the protection of personal data which will both improve coordination of European legal frameworks and change the requirements governing the processing of personal data. An important principle for the collection of personal data is that of processing for specified, explicit and legitimate purposes. When a customer consents to the collection of personal data, he or she must be informed of the purpose of collecting such data. A new EU regulation may change this requirement to permit the data owner (the institution) to also use collected data for other purposes. Another important principle is the individual customer's right of access to data registered about the customer himself. Extracting such data for use in a Big Data context may be a demanding process, due to numerous indirect dependencies. In the autumn of 2013, the Norwegian Data Protection Authority published a report entitled *Big Data – personvernprinsipper under press* [Big Data – personal data protection principles under pressure].[16] The issue of personal data protection is considered in depth in this report.

Big Data also have an intrinsic value. Since such data also contain internal data that are not accessible outside the institution, they may have significant value for other parties who can use them to expand their database. Such data may not be disclosed, exchanged or sold unless they have been anonymised. They should therefore be well protected and secured against misuse. Disloyal employees may be tempted to sell this kind of data to third parties, including criminal networks.

In the financial sector, Big Data analytics are used by the major international financial groups, especially US corporations. Many of the areas of application discussed in the media are at the interface between financial services and retail chains, for instance. These areas of application

[16] http://www.datatilsynet.no/Global/04_planer_rapporter/Big%20Data_web.pdf

may be precluded by current European personal data protection legislation that is more restrictive concerning such uses.

3.7.3 Disaster preparedness (data centre and quality)

Finanstilsynet lays down requirements for institutions' disaster recovery plans through the ICT Regulations' section 10 on business continuity requirements and section 11 on disruption of operations and disaster preparedness. The various institutions under Finanstilsynet's supervision have different risk profiles and have therefore also adopted different disaster recovery plans. In the next few years, a growing number of the existing data centres in Norway will be moving into new data centre halls which provide infrastructure such as electricity, telecommunications, cooling and physical protection of the building. These halls will be similar to a data centre hotel, where service providers purchase space for their own technical infrastructure. Each buyer must weigh the standards and best practices incorporated in this type of data centre hotel against its own risk assessment.

Up until now, it has not been common practice in the Nordic region to certify data centres, but when establishing their facilities many centres have nonetheless adopted the certification requirements applied to the different tier levels[17] by institutions such as the Uptime Institute. In Northern Europe no data centres have been certified, but in Spain, for example, the two largest banks, Santander and BBVA, and the insurance company Mapfre, have certified their data centres to Tier 4 standards. To compare the quality of the data centre certification with the operational sustainability of the solutions located in the data centre hall, the Uptime Institute has established a three-tier system for certification of operational sustainability, which indicates whether the infrastructure solutions installed in the data centre are designed to exploit the full quality potential of the data centre.

Finanstilsynet will take a closer look at this issue in 2014 in connection with its work on further developing its supervisory tools.

3.7.4 Malware

Malicious software (malware) that is spread by individuals and small hacker groups may harm those affected, but seldom leads to any far-reaching societal problems. Malware used by criminal groups poses a greater risk. These groups are increasingly professional, preparing their attacks in an expert manner. The attacks are usually mounted in several phases, which may include a reconnaissance/mapping stage, a development stage in which malware is adapted for its intended purpose, and testing of the malware on a similar smaller enterprise so as not to reveal the target, before the actual attack is launched. The attack may also be accompanied by a variety of diversionary tactics.

The reconnaissance stage usually involves the use of "phishing". This method may also be used during the development and testing of malware in order to customise websites, for example, to give them a credible layout, and in order to lure the user into "false" websites so

[17] Tier levels and requirements: A variety of industrial standards have been established to define the requirements for a data centre. These are divided into tier levels, of which 1 is the lowest and 4 the highest. Level 4 contains all the requirements in the lower tiers, in addition to requiring solutions to be duplicated to ensure their robustness.

as to deploy various other viruses to be used in the attack. During the actual attack, the hacker can then divert the victim's attention by targeting some servers with DDoS attacks, thereby keeping the security department busy.

The phishing phenomenon has evolved both qualitatively and quantitatively. Phishing increased in 2013, and a multitude of new approaches were tried out. It is increasingly difficult to distinguish between a phishing e-mail and an ordinary e-mail. A number of incidents show that the attacks are now more targeted – spear phishing – in an attempt to gain unauthorised access to confidential data. Phishing can also be carried out through telephone calls, text messages and web dialogues.

Phishing is an effective method in an era when people disclose large amounts of information about themselves on social media such as LinkedIn, Facebook and Twitter. Phishing was one of the tactics used in the serious hacker attack on senior Telenor executives in 2013.

In 2013 Norway experienced a wave of phishing attacks against Norwegian financial institutions. Large quantities of false e-mails were sent out, ostensibly by a financial institution. However, the e-mails are still not written in good enough Norwegian to be credible. The language in e-mails written in English, seemingly sent by international enterprises such as VISA, PayPal, etc., is better.

The false e-mails are attempts to fish for payment information, but they can also infect computers with malware if the recipient clicks on a link or an attachment in the e-mail. The same is attempted in telephone phishing, which also increased dramatically in 2012 and 2013. The recipient of the telephone call is given instructions directing him to a website where he is asked to click on a link. This link then uploads malware to the computer.

An indication of the extent of phishing activity is the number of false websites that are shut down. In the United Kingdom, phishing in the financial sector is quantified in this way; see chapter 7.5 (loss figures).

DDoS attacks have proliferated worldwide. Effective countermeasures have been established in Norway, which may explain the decline in such attacks towards the end of 2013. Internationally, the trend is that these attacks are becoming more sophisticated, with the correct log-in syntax, so that the attacks breach the first barriers and must be stopped deeper inside the systems, for instance at application level. Several Norwegian operators anticipate a similar trend in Norway.

Despite wide-ranging attacks in Norway, reports indicate that the number of infected PCs in Norway is relatively small. In any event, institutions must continue to give priority to protecting themselves against malware.

3.8 Challenges for consumers

The proposed EU directives referred to under chapter 3.2 will redistribute responsibility between banks and their customers. Among other things, provisions are proposed that could deprive member states of the possibility of limiting the deductible charged to customers in the event of misuse ascribable to gross negligence. A limit of this type currently applies under Norwegian, Swedish and Danish law. Abolishing or significantly reducing these limits will shift the distribution of risk between bank and customer. This could be unfortunate if it results

in a mismatch between those who are responsible for security and those who incur the risk. The consequence could be higher losses and lower incentives to maintain good security. Financial institutions determine the level of technical security for their services, while organisations and individuals may experience problems if information regarding customer relationships or payment information becomes accessible to unauthorised parties.

Protection of the customer's interests is governed by the customer agreement, as well as by currently applicable rules and regulations. These may be changed at any time, and not always to the customer's advantage. In Norway, the current rules and regulations assure a high level of consumer protection. This may have to be changed if proposals for EEA-wide harmonised rules are adopted.

Payment cards that enable the holder to make contactless payments may create a vulnerability because customers do not know enough about secure use. Payment cards will function in the same way as NSB's and Ruter's travel cards. If a customer places his whole wallet on the scanner, instead of taking out and scanning the travel card itself, the scanner will be able to register all the other cards in the wallet that are based on the same payment technology. In the event of fraud, the cardholder will not be notified about the payment transaction until he checks his account. All cards containing a RFID chip are ready for scanning and cannot be switched off.[18] A growing number of new cards now offer this functionality.

Many payment cards have protocols for using a PIN for contactless payments, even though it is not used in the actual services. An unlimited number of attempts may be made to find a PIN in this connection. The PIN may be tested for several days without exceeding the number of valid attempts. The PIN for contactless payments and for ordinary payments turns out to be the same.[19]

Consequences for customers may include:

- Increased use of contactless payments will make bank statements very long, and many consumers will never notice rogue payments of small amounts.
- When consumers discover a suspect transaction, they must go through a relatively lengthy process to recover their money, in addition to which customers are often given little information on which to base their claim for a refund. They may also have to deal with time limits and cumbersome claim processing procedures.

To be able to check their bank statements, they must have something with which to reconcile them, such as receipts.

As a result, relatively few fraudulent transactions involving small amounts are likely to be discovered and followed up.

[18] http://www.rogerclarke.com/EC/CPS-12.html

[19] http://fc13.ifca.ai/proc/9-2.pdf

3.9 Virtual currencies

In the past year, virtual currencies, or "cryptocurrencies", have attracted considerable attention. Bitcoin[20] is the most widely used and discussed virtual currency, but other well-known cryptocurrencies include LiteCoin, ZeroCoin and Linden Dollars. Virtual currencies exist in many forms, and at present there are more than 100 different varieties.[21] A virtual currency is a type of unregulated, digital currency which is not issued and guaranteed by a central bank, and which can function as a means of payment because it is perceived to have value as long as others accept the digital currency as payment in trade.

Virtual currencies are exchanged and accepted in more and more places, both on the Internet and outside the web in the "real economy". In addition to its extensive use in gambling forums, social media and criminal forums, a growing number of retail merchants, restaurants and places of entertainment have begun to accept virtual currencies (incl. Bitcoins) as a means of payment, since they usually do not involve a bank and therefore leave no "traces" to be found by the authorities. Moreover, they entail low or no transaction costs.

Since the virtual currencies are neither issued nor guaranteed by a central bank, and so far have been subject to no oversight, consumers have no legal protection. This means that there are significant risks attached to the currencies. In December 2013, the European Banking Authority (EBA) warned consumers of the possible risks associated with buying, holding or trading virtual currencies. Finanstilsynet helped to draft the warning.[22]

Points mentioned in the warning:

- You can lose your money on exchange platforms.
- Your money may be stolen from your digital wallet.
- You are not protected when you use Bitcoins as a means of payment.
- The value of your Bitcoins may change rapidly, and may even fall to zero.

The lack of regulation also creates opportunities for fraud. It is often impossible to trace virtual currencies, and users enjoy a high degree of anonymity. This makes the use of virtual currencies attractive for criminal activity and money laundering.

The Swedish Financial Supervisory Authority (Finansinspektionen – (FI)) considers Bitcoin to be a means of payment, which means that payment services institutions that offer Bitcoin as a means of payment must report their activities to FI.

The EBA is now considering whether virtual currencies can and should be regulated.

[20] http://bitcoin.org

[21] http://coinmarketcap.com/

[22] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2013/4_kvartal/Advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/

4 Finanstilsynet's findings and observations

Finanstilsynet's main sources of information on financial institutions' IT activities are inspections, interviews and incident reports. Finanstilsynet also stays updated on major development projects and changes by meeting regularly with the largest institutions and service providers, and is notified by institutions of any new or changed payment services.

In connection with its work on this RVA analysis, Finanstilsynet interviewed a number of security companies and internet service providers (ISPs)[23], and conducted a survey on relevant areas of IT development.

4.1 Some findings from IT inspections in 2013

Challenges arising from new outsourcing strategies
Finanstilsynet sees a trend whereby major financial institutions are seeking to consolidate their operations in large organisations and entering into agreements with global partners. It is often difficult to see where the Norwegian branch is placed in the organisation or conglomerate, and to understand how the Norwegian branch is managed and run. It appears to Finanstilsynet to be more challenging for institutions to ensure management and control of their operations with this type of "globalised" outsourcing.

Inadequate agreements
Establishing good agreements seems to be increasingly important. Finanstilsynet is seeing a tendency for financial institutions to split up the provision of ICT services into several parts. This means entering into agreements with more contracting parties. The agreements must cover every aspect of the outsourced activity and describe the interaction between parties. Furthermore, it is important for financial institutions to establish contractual rights to the use and ownership of solutions and source code. If an ICT service provider has financial or other types of problem, it is crucial to have agreements that specifically cover these circumstances so that it is technically possible to choose another supplier.

Contingency solutions for payment services
In 2013, Finanstilsynet and Norges Bank conducted a joint thematic inspection of contingency solutions for domestic payment services. To map the banks' contingency measures to ensure customers of access to means of payment and the role played by cash, inspections were carried out at three selected banks and a clearing house.

The preliminary assessment is that a contingency situation involving a lack of access to shared infrastructure is easier to deal with using back-up solutions than a contingency situation where there is a lack of access to the bank's core system. On the other hand, more users are affected, all in all, when shared infrastructure cannot be accessed. Norwegian banks' core system operations are relatively dispersed, both technologically and geographically, so that there will probably always be access to the core systems of some banks. This inspection has not been completed, and the results will be reviewed in a summary report.

[23] ISP: Internet Service Provider

Inadequate risk assessments of ICT activities
In the inspections carried out in 2013, Finanstilsynet found that the risk assessment of ICT activities is inadequate in a number of cases. Assessments are often carried out at a general level, based on a "top-down" approach. Unless the observations of the operational staff are systematically documented and incorporated in the basic structure underlying risk prevention efforts, they may not be included in the risk assessment. It is important that the persons participating in risk assessments have sufficient knowledge of the areas being analysed.

Finanstilsynet has also noted a lack of a structured review to determine whether ICT activities are run in compliance with the regulatory framework. This applies to operations in compliance both with institutions' own internal rules and with applicable laws and regulations, such as the ICT Regulations.

Use of ISAE 3402 reports
The results of a review of the ICT activities of an ICT services provider, documented by means of an ISAE 3402 report,[24] may be a helpful tool for customers who purchase ICT services from the service provider. However, ISAE 3402 reports are designed for audits relating to internal control over financial reporting. Under section 12 of the ICT Regulations, which deals with outsourcing, the financial institution is responsible for meeting all the requirements of the Regulations, even where all or parts of its ICT activities are outsourced. The institution's right to inspect the service provider's activities covered by the agreement must be set out in contractual form. The ISAE 3402 report provides a general overview of the risk situation, based on the results of selected audits, but normally does not cover all aspects of the ICT activities and thus does not cover the issue of whether the services provider is operating in compliance with the provisions of the ICT Regulations.

4.2 Institutions' own assessments

4.2.1 Interviews

In November and December of 2013, Finanstilsynet held interviews with 14 institutions and two interest groups about their views on risk in 2013 and beyond. The 14 institutions focused on risk associated with IT services, while the two advocacy groups emphasised risks related to the role of security service providers. In the following paragraphs, both groups are referred to as institutions.

In short, the combination of cost pressure and pressure to deliver and challenges related to change management, coupled with extremely high demands for quality and security in services, appears to be the greatest risk.

Most of the institutions report that various forms of fraud are made possible by phishing or card-not-present transactions and will constitute a risk (see also the loss figures in chapter 7.5). Several institutions report a decline in Trojan attacks in 2013.

The institutions also point out that ID theft is still a risk.

[24] International Standard on Assurance Engagements (ISAE) 3402: Assurance Reports on Controls at a Service Organization http://www.revisorforeningen.no/arch/_img/9605549.pdf /

Ten of the institutions emphasised that change management posed a particular risk for them. Six of these institutions reported that the change management risk is associated with the introduction of new regulatory requirements. Two of the institutions reported especially high risk in connection with other major system changes.

Three institutions consider use of social media to be a great risk. Two of them regarded use of customer services in the form of chatting to be a significant risk.

"Poor workmanship" in the development of new services was deemed to be a major risk by four institutions. OWASP's[25] Top Ten Project shows examples of threats in services.

Network failure is seen as a vulnerability and a risk by five institutions. One of the institutions also pointed to the risk of eavesdropping and fraudulent transactions conducted over public networks.

Two of the institutions view Advanced Persistence Threats (APT)[26] as a substantial risk.

Six of the institutions consider the administration and control of data to pose a major risk. "What data do we own and where are they?", as one of the institutions put it.

Two institutions see a risk in the provisions of the Payment Services Directive (PSD 2) and the recommendations of the European Forum on the Security of Retail Payments (SecuRe Pay), on issues such as overlay services[27].

In the view of five institutions, DDoS are and will remain a threat. Considerable action has been taken, substantially reducing the risk of adverse impacts.

Three institutions report that the value chains are long, creating a significant risk with regard to testing, monitoring, liability and control.

Nine institutions consider cost pressure and pressure to deliver to be a great risk.

Two institutions point to the risk of insider fraud.
Four of the institutions refer to risk associated with legacy core systems (accounts receivable).

None of the institutions consider mobile banking to be a major risk, and two institutions see little risk associated with mobile banking.

4.2.2 Questionnaire survey

As a means of mapping some areas in which rapid advances are being made and which could therefore constitute an operational risk, Finanstilsynet conducted a questionnaire survey. Banks and insurance companies were asked to answer questions on the following topics:

[25] The Open Web Application Security Project (OWASP) – a world-wide not-for-profit organisation that seeks to promote IT security: https://www.owasp.org/index.php/Main_Page

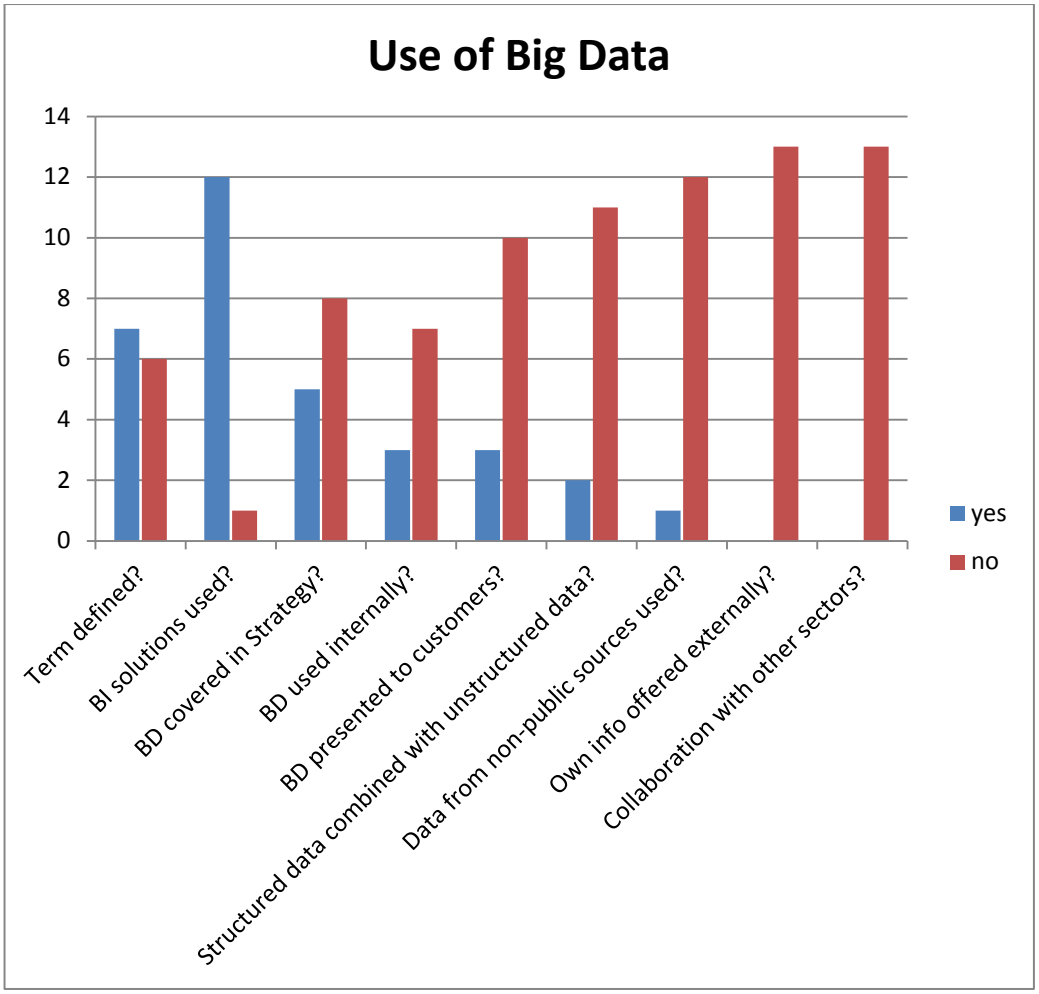
[26] Malware in the institution's systems. The code goes unnoticed for a long period of time.

[27] Third-party services at the customer-bank interface.

- Use of Big Data
- Use and development of apps
- Use of or plans to use cloud computing

Use of Big Data (BD)
Many banks in Norway have begun to use Big Data in certain areas. Most of the banks use business intelligence tools to analyse data in their data warehouses, and on the whole it is this type of information that is shared with customers. Some banks have started to collect data from other sources as well, but none share information with third parties, or collaborate on such services.

Figure 2: Use of Big Data



Source: Finanstilsynet

Use and development of applications (apps)
The institutions reply that apps are treated in the same way as other channel services, and that they are developed using standard methodology. Most of the institutions buy application development services from external service providers, but the institutions' own development and testing requirements are applied in the development process. The apps are designed to

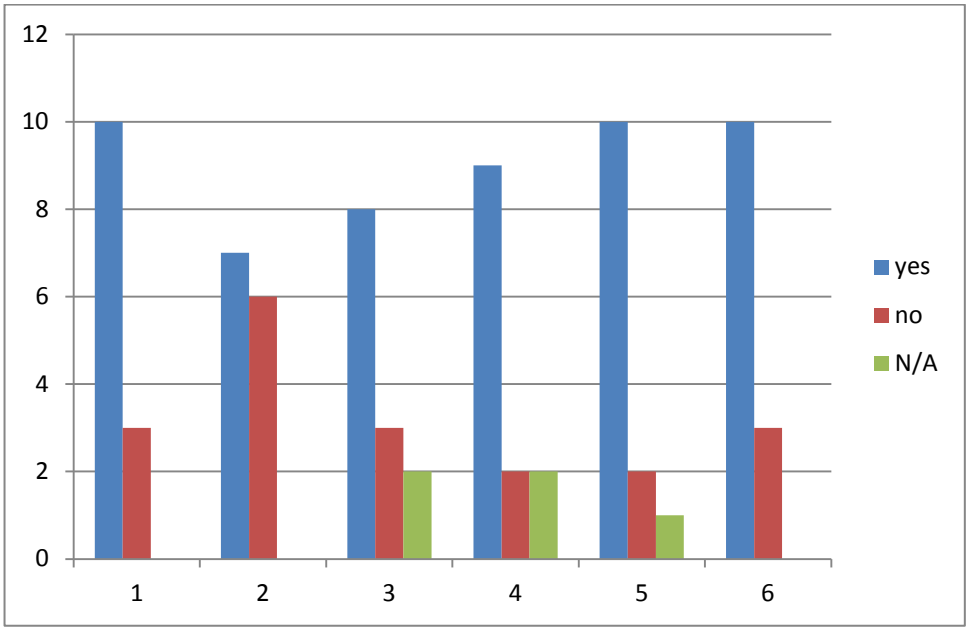
meet the same security and quality requirements as other web-based channel services.

Several institutions have developed apps that use GPS, cameras and contact lists for "where are we" functions, but the function only logs data locally on the device.

Use or plans to use cloud computing
The institutions were asked the following questions:

1. Has the institution begun to use or is it considering using cloud computing services?
2. Has the institution made a strategic decision to use cloud computing?
3. Before use of cloud computing was included in the strategy, were risk assessments carried out?
4. Did the risk assessments include the issue of compliance with laws and regulations?
5. Are there areas of the institution's portfolio that are particularly appropriate for use of cloud computing?
6. Has the institution considered how compliance with confidentiality, integrity and accessibility requirements is to be assured in connection with use of cloud computing?

Figure 3: Breakdown of responses regarding use of or plans to use cloud computing



Source: Finanstilsynet

The survey responses show that the institutions are addressing issues associated with use of cloud computing at a strategic level, have carried out risk assessments and have considered the use of cloud computing in relation to legislation and other rules.

The areas considered by the institutions to be the most relevant for use of cloud computing are open anonymous data that may be published externally, office support services for internal interaction and anonymised personal data for customer services. Judging from the responses, the use of cloud computing is not an option for the institutions' core activities. Institutions consider control of their own customer data to be important.

The institutions were asked to rank the following topics relating to the choice of cloud computing services by order of importance:

1. Accessibility
2. Cost
3. Security
4. Simplicity
5. Stability
6. Access to (personnel) resources/expertise

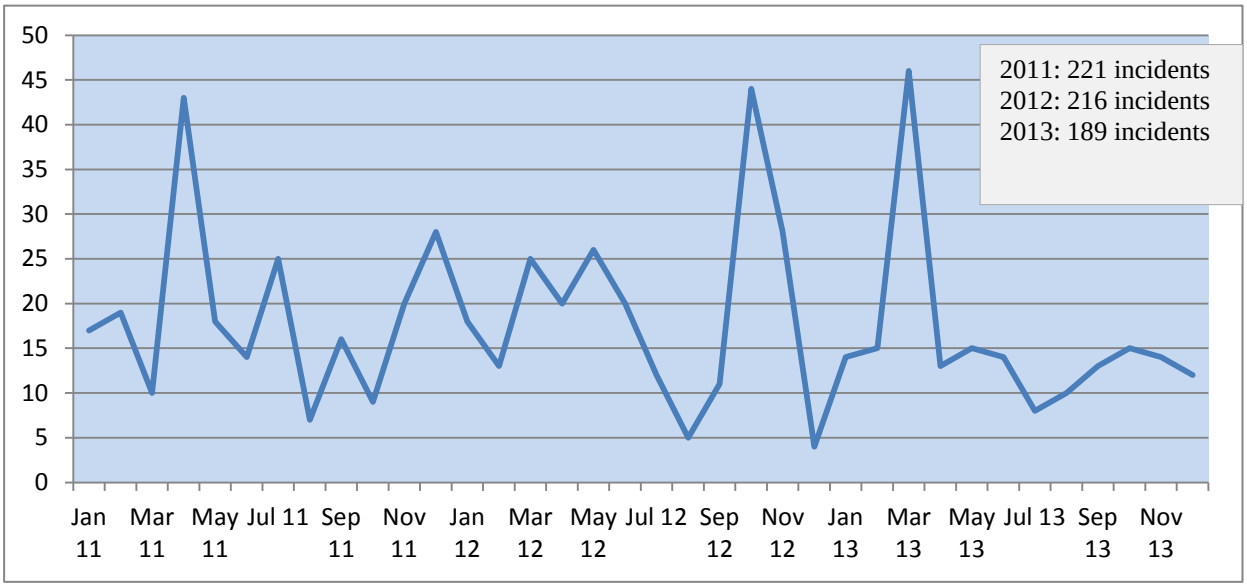
The security of the service was ranked highest, followed by cost. Access to resources/expertise was deemed to be the least important, according to this survey.

4.3 Incidents reported in 2013

Any operational failures, unintended incidents or intentional attacks on payment services must be reported to Finanstilsynet.

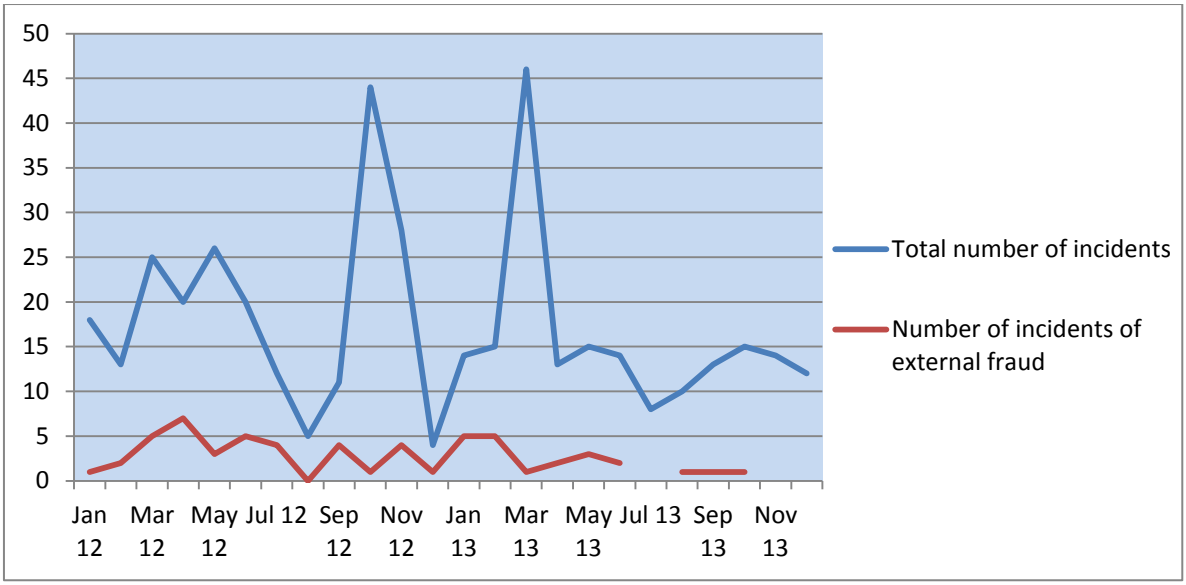
Somewhat fewer incidents were reported in 2013 than in the two preceding years. Operational stability has generally been better, but serious service outages occurred at most banks in 2013. The number of Trojan attacks fell significantly in 2013, compared with 2012. Phishing attacks, on the other hand, increased in both scope and variety.

Figure 4: Number of incidents reported in the period 2011–2013



Source: Finanstilsynet

Figure 5: Number of incidents of external fraud (malicious attacks) in relation to total number of incidents reported in the period 2012–2013



Source: Finanstilsynet

4.3.1 Operational incidents in vulnerable infrastructure

In the spring of 2013, there were two serious incidents that demonstrated the vulnerability generated by failure of shared infrastructure. On 4 March there was a network outage in Evry that lasted around four hours, and on 18 March there was a network outage in Nets that lasted around two hours. In both incidents, a network component failed, and the secondary system did not function as it should.

The network component was the door to a large number of payment services. Finanstilsynet considers that there is reason to review the service providers' network architecture to prevent the failure of one component from impacting many critical services simultaneously, and has taken this issue up formally with the service providers.

4.3.2 Inadequate testing

Many incidents in 2013 were caused by errors in applications, implementation or operational design and resulted in an erroneous response to the user/customer. This led to many unfortunate consequences, such as customers being sent bank statements containing incorrect account information. Many of these incidents could have been avoided by means of better testing. An acceptance test must be carried out by the institution itself as a final guarantee that the product or service meets the specifications. If a non-conformity has not been discovered earlier in the testing process, it should be detected by the institution's acceptance test.

4.3.3 Increase in phishing attacks

In 2013 there was an increase in fraudulent phishing attempts to deceive people into disclosing sensitive information. People received a great many e-mails, purportedly from

financial institutions like VISA, Teller, Western Union, Nets, DNB, SpareBank 1 and other banks, or from telecommunications service providers such as Telenor and Netcom. New scenarios were constantly presented. Often, it was a question of security updates accompanied by a request for payment card details or account numbers. Most of these e-mails were written in poor Norwegian, while e-mails purporting to be sent by international financial institutions like Western Union, VISA, etc. were written in English and were better formulated. If the recipient clicked on a link in these e-mails, his computer could become infected and thus vulnerable to more serious Trojan attacks. It is possible that 2013 was a year in which data and information were collected in preparation for attacks.

4.3.4 DDoS attacks in 2013

The rise in the number of DDoS attacks in 2012 continued through 2013. The countermeasures taken by both the institutions themselves and by the internet service providers have been reinforced, with the result that although the attacks have increased, they had little impact on accessibility. In 2013, a new type of targeted DDoS attack was seen, and in September a major insurance company was subjected to a DDoS attack in which the attackers made concrete threats.

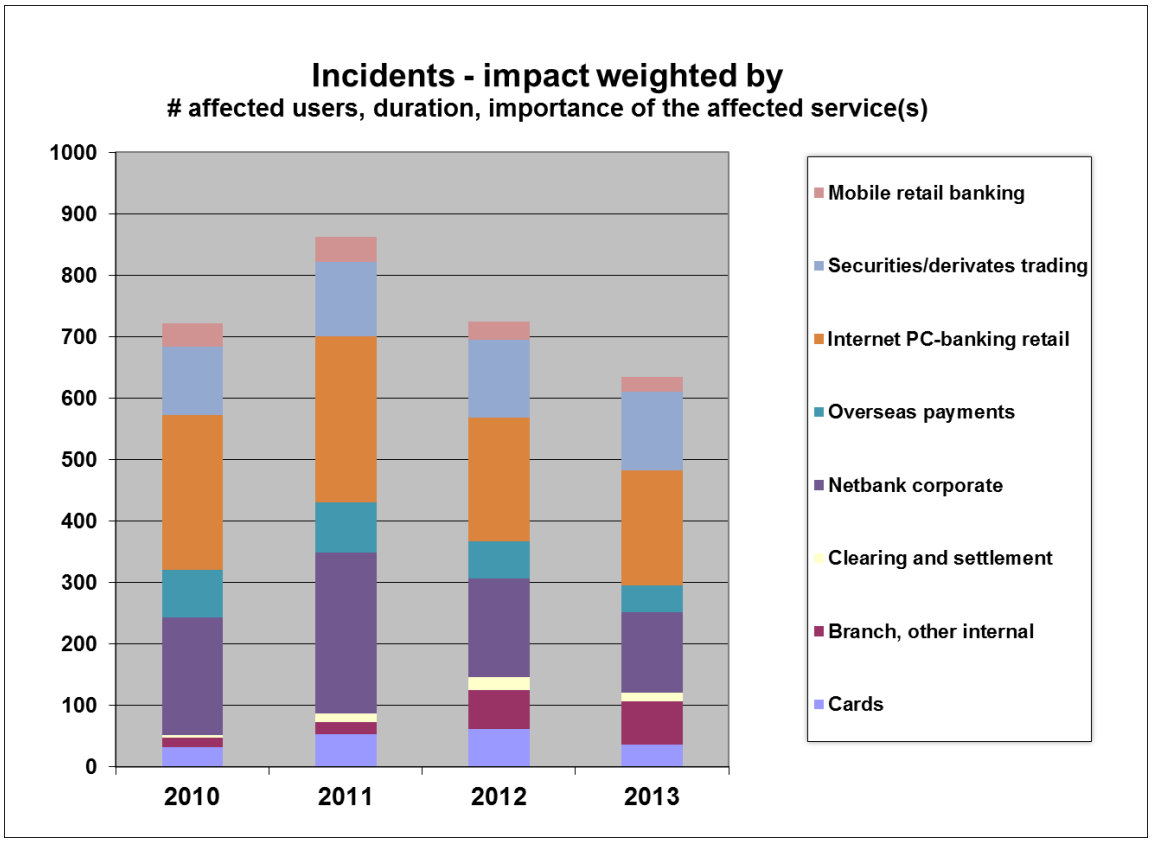
4.3.5 Analysis of incidents as a measurement of accessibility

For each incident that affected the accessibility of services, Finanstilsynet has assessed the duration of the outage, the number of institutions affected, approximately how many customers were affected and whether there are replacement services that customers could use. This provides Finanstilsynet with a year-by-year index for payment system inaccessibility, enabling it to monitor developments.

The figure shows that the payment system was less inaccessible to the general public than in previous years. This may be because the quality improvement efforts of key service providers have produced results. If fewer new services were established in 2013 than in earlier years, this may also be a contributory factor. In previous years, institutions have implemented measures to prevent identity theft, DDoS and Advanced Persistent Threats (APT), which may have contributed to the reduction.[28]

[28] This is an overall assessment, and individual institutions may therefore differ from the general picture.

Figure 6: Incidents weighted by impact



Source: Finanstilsynet

4.4 Risk areas identified from other sources

4.4.1 Interviews with security companies and internet service providers

In the autumn of 2013, Finanstilsynet held discussions with some key players in the field of security systems and surveillance in Norway.

Finanstilsynet noted a number of points during these discussions.

Following the revelations concerning the attacks on Telenor in 2013 and improved documentation of what appears to be a rising international trend of digital industrial espionage, higher priority has been given to detecting and taking steps against industrial espionage. The hidden statistics on attacks of this kind have been high, probably owing to fear that publishing information may result in negative publicity.

The number of DDoS attacks is rising, possibly because these attacks can now easily be bought as a service in "dodgy" marketplaces. However, the impact is less because of better surveillance, tools and counter-attack procedures on the part of both the ISPs and the individual companies.

Governments and IT users in the Nordic countries are among the most IT-security conscious

in the world, and have the lowest rate of infection with viruses and malware.

Concerted action involving government authorities, internet service providers, the police, and now also the various CERTs have resulted in steadily improving protection against the undesirable consequences of cyber attacks. It is considered important to continue this cooperation.

4.4.2 Reports from international security organisations

In its 2013 Threat Landscape Report,[29] the European Union Agency for Network and Information Security (ENISA) views the following threats as the most serious:

1. The attackers are becoming increasingly sophisticated in their attacks, and using ever more sophisticated tools.
2. Tools that used to be used against PC platforms have now been converted for use against mobile devices.
3. Not just a handful, but quite a large number of national states now have the capacity to conduct targeted attacks, for example of the type Advanced Persistent Threat (APT), against the government and against private and public enterprises.

Two new areas that are growing strongly may present a challenge to security:

4. Internet of Things (IoT) and Big Data.

ENISA also points to positive trends in 2013:

5. The police have succeeded in closing down a number of major criminal websites and arresting key persons associated with these circles.
6. The number of reports and data on cyber attacks has risen, as has the quality of the information available. This makes better threat analyses and targeted security work possible.
7. System suppliers have reduced the time of response to new threats by providing faster access to security upgrades.
8. Cooperation among a number of relevant security organisations has commenced and will be intensified in the time ahead.

In "Cybercrime Report 2013", international security products company Fortinet[30] describes how modern cybercrime resembles normal, legal IT activities. Well organised operators deliver tools "as a service", with a complete price list. It is possible to purchase consulting services, rent a botnet, obtain customised Direct Denial of Service (DDoS) attacks and purchase code that exploits weaknesses in order to infect computers.

---

[29] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[30] http://www.fortinet.com/resource_center/whitepapers/cybercrime_report_on_botnets_network_security_strategies.html

On the positive side, Fortinet mentions that authorities, software providers and security firms are cooperating on Computer Emergency Response Teams (CERTs). This has made it possible to stop the biggest botnets.[31] However, they also point out the necessity of international cooperation as a critical success factor.

[31] A botnet (bot is the second syllable of the word 'robot') is a network of computers, connected to the internet, the owners of which are not aware themselves that their computers have been taken over by unauthorised parties with the aid of trojans, computer viruses or in some other manner.

5 Risk areas

This chapter describes the risks that Finanstilsynet regards as the most serious for the financial sector.

5.1 Extensive changes in the financial sector's IT activities

As described in chapter 3.6, Finanstilsynet is aware that several of the large financial institutions are making, or intending to make, extensive changes in both their IT systems and their IT operations. Examples of change include replacement of suppliers and operating sites, changes in operating systems and architecture, insourcing and increased use of outsourcing and offshoring. Some of the changes also affect human resources, such as restructuring and cutbacks. A number of key IT suppliers are also introducing or planning significant changes. This applies in particular in cases where suppliers are affected by the choices of the financial institutions.

The scope of and reasons for the changes vary. Some of the main reasons are cost savings, quality improvements and stricter efficiency and flexibility requirements. Once completed, the changes are intended to reduce vulnerability and risk.

The institutions appear to agree that, as a general rule, the changes entail greater operational risk. The interviews (see chapter 4.2.1) reveal that the actual handling of the change is regarded as one of the greatest risks. Finanstilsynet has found that the majority and the most serious of the reported incidents have actually occurred in connection with changes. It is essential that enterprises monitor and manage the risks associated with the extensive ongoing changes.

5.2 Interoperation between several operators

Many of the changes mentioned above imply that a number of suppliers are involved in the value chain of one and the same enterprise. Where there was formerly one main IT supplier, services and deliveries are now split up among several suppliers (multisourcing).

Such a model may offer many advantages. However, Finanstilsynet believes that the model may result in a lack of clarity regarding responsibilities, and inadequate interoperation and coordination, which can increase risk, particularly in a crisis situation. Finanstilsynet refers to the "Easter incident" in 2011, where it was precisely inadequate interoperation that made it difficult to reduce the scope and consequences of the triggering event. Multisourcing may also make it a challenge for the enterprise to acquire sufficient insight into the internal control of and risk associated with all the outsourced IT activities. Risk management and extensive agreements are necessary.

5.3 Inadequate risk assessment

In previous RAV reports, Finanstilsynet has pointed out that risk assessment and management represent an area in need of improvement. The area still seems to present challenges. As a general rule, annual risk assessments are in fact carried out in accordance with the provisions of the Norwegian Risk Management Regulation and ICT Regulations, but the work is of

uneven and often inadequate quality. In Finanstilsynet's experience, too many risk assessments and risk-reducing measures are not followed up sufficiently systematically. It is often not clear whether the measures have been implemented, or whether they have had the expected effect on risk. It may be difficult to see whether risk analyses actually are being used well enough as a means of managing risk and helping the institution to achieve its goals.

Finanstilsynet has the impression that institutions' risk analyses too often have a general perspective and that institutions do not go to sufficient lengths to secure expertise in the areas to be analysed. Personnel involved in day-to-day operations and development are often best placed to identify risk. Systematic work on risk and adequate documentation must be incorporated as a part of day-to-day operations. Risk analysis is a vital means of ensuring that the introduction of new systems or changes in existing ones take place in a prudent manner and with acceptable risk.

5.4 Attacks on payment services

Payment services are still under attack by criminals. This applies to the majority of electronic channels where payment services are made available all the way to the customer, directly through online banking, or via public sales outlets, ATMs for dispensing cash, shopping at retail outlets or via online shopping. Banks' losses in a number of areas do show a clear decline in 2013, while there was a clear increase in losses connected with the use of cards in card-not-present online shopping. The possibility of a connection with the large-scale hacking of international credit card number databases cannot be excluded.

Information from various sources gives Finanstilsynet reason to believe that criminal groups are continuing work to develop methods for attacking online banks, ATMs and EFT/POS terminals, and that attacks on systems in the individual countries will come in waves and possibly unexpectedly. There is therefore every reason to persist in the important work of building defences and plugging vulnerable spots. A great deal of phishing occurred in 2013, and this may be viewed as a preliminary to attacks. Whether attacks occur will depend on the criminals' assessment of their chances of success in light of the information they have about the defence capability. Although there was no general increase in losses in 2013, large amounts were lost nonetheless, and there is every reason to set one's sights on further reducing losses.

5.5 Risk due to outdated design

In RAV reports of previous years, Finanstilsynet has pointed out an increasingly urgent need to replace old legacy systems. In time, expertise on old systems will cease to exist, and maintenance and operation will become more of a challenge.

Each service was built as an isolated vertical silo, with the user interface at the top and the legacy data at the bottom. New services must to a large extent be built from scratch from the bottom up.

This earlier lack of built-in flexibility in the systems makes it difficult to meet the present-day requirements of the growing number of new services and customer channels. This has been compensated for by extracting legacy data in the form of copies. The result after a while was that customer and account data increasingly lay in several copy registers, and keeping them

updated is a demanding process.

In modern systems, however, there are functions that are coupled to services via a "service bus". The reuse principle results in a reduction in time to market, and there is less risk of errors.

6 Monitoring by Finanstilsynet

6.1 IT supervision and other contact with institutions

Monitoring of institutions' IT risk primarily takes the form of inspections. In 2014, Finanstilsynet will be focusing on the entities under supervision and suppliers that have the greatest influence on financial stability and smoothly functioning markets.

Particular attention will be paid to operational risk in the banking sector, with the focus on the supervised entities' central ICT systems and outsourcing. Financial institutions that make major changes in their ICT function, including outsourcing, and that may thereby increase their risk, will be subject to special scrutiny. Finanstilsynet will continue its monitoring of contingency and disaster-recovery systems, risk assessments, implementation of measures associated with legacy core systems and operating stability and structural changes in suppliers to the supervised entities.

On the basis of risk assessments, both general IT monitoring and IT monitoring focused on particular topics will take place. The most important basis for monitoring is verification of compliance with the ICT Regulations and use of various supervisory modules (self-evaluation forms) based on best practice. The most common self-evaluation forms are available on Finanstilsynet's website.

Finanstilsynet has regular contact with the large institutions in connection with the general IT risk situation, development and change projects and incidents.

6.2 Work with payment systems

The legal basis for Finanstilsynet's general supervisory responsibility is the Financial Supervision Act and the regulations on risk management and internal control and on the use of ICT. Responsibilities relating primarily to payment service systems are also regulated by chapter 3 of the Payment Systems Act.

Verification of compliance with the regulatory framework is an important responsibility, while development of legislation is important in such a dynamic area. Finanstilsynet is working on proposed separate regulations for payment service systems with legal basis in the Payment Systems Act and proposed amendments to the ICT Regulations. Amended rules and regulations will be followed up and incorporated in the supervisory system as relevant.

When it comes to work with payment systems, Finanstilsynet is focusing attention here too on the supervisory entities and suppliers that have the greatest influence on financial stability and smoothly functioning markets, with particular emphasis on operational risk. When major changes are made in payment systems, either through the development of new systems or by outsourcing, Finanstilsynet will focus on this factor in its work, as the changes may involve greater operational risk.

6.3 Development of the regulatory framework in Norway

On the basis of Finanstilsynet's information about development trends and the risk picture, the authority is drafting regulatory amendments in areas related to outsourcing and risk in payment systems.

To the Financial Supervision Act:

- a general obligation to report any outsourcing to Finanstilsynet.
- a stronger legal basis for closer consideration of outsourcing that is deemed to entail too high a risk.

To the Regulations on the Use of Information and Communication Technology (the ICT Regulations):

- a special obligation to report any outsourcing of ICT systems to Finanstilsynet.
- outsourcing of ICT that is of significance for the institution's operations must be approved by the institution's Board of Directors.
- new rules on security and risk associated with the establishment of and changes in payment systems.

To the Payment Systems Act:

- Requirements regarding the security level in connection with the use of electronic payment systems. The duty of notification described in the circular must be included in the regulations. The proposed new regulations may contribute to more secure payment services for users and stipulate concrete design requirements, to provide consumers with better protection against fraud.

Proposed amendments to the Financial Supervision Act and the Payments Systems Act have been forwarded to the Ministry of Finance.

Duty of notification of the establishment and operation of payment systems
Institutions shall notify Finanstilsynet of the establishment and operation of systems for payment services without undue delay; see section 3-2 of the Norwegian Payments Systems Act. The duty of notification is described in more detail in circular 17/2004 (Norwegian text) with appurtenant self-reporting form. The notifications are important for enabling Finanstilsynet to monitor changes in payment services, learn of the use of new technology and the choice of new suppliers of services and, not least, to monitor the operational risk related to these services.

Finanstilsynet generally receives few notifications. Supervisory inspections provide support for the assumption that there is under-reporting, and that institutions are not complying adequately with their duty of notification. Finanstilsynet will submit a proposal that the Payment Systems Act be used as the legal basis for regulations to replace Finanstilsynet's circular of 17/2004.

6.4 Reporting of incidents

Financial institutions are required to report significant incidents to Finanstilsynet; see Section 9 of the ICT Regulation. Reported incidents are collected in Finanstilsynet's incident database, where they are analysed and used as a basis for possible future measures. The incident database is a valuable source of data for analysing trends and relationships; it provides good

insight into institutions' operational risk and highlights topics that Finanstilsynet may need to monitor.

Finanstilsynet is generally satisfied with institutions' reporting, but sees that there is still room for improvement. Further work will be devoted to securing correct and timely information to form a basis for any reaction and/or measures.

To ensure reporting at the correct level by financial institutions other than banks, Finanstilsynet plans to arrange a mini-seminar on incident reporting for insurance companies in 2014. The annual incident reporting seminar for officers in charge of reporting, and bilateral follow-up meetings with individual institutions, will continue.

6.5 Contingency preparedness

Through cooperation with the financial industry, Norges Bank, other authorities and central service providers, emphasis is placed on contingency preparedness, whether for the industry as a whole, the institutions themselves or the institutions' subcontractors. This is work that will remain in focus, through inspections, further follow-up of contingency and disaster-recovery systems and appropriate exercises.

Finanstilsynet is also involved in Nordic, European and international collaboration on oversight work, which will continue. To address the issue of online incidents, Finanstilsynet also participates in European collaboration on internet security.

The establishment of FinansCERT Norge, under the auspices of Finance Norway, is regarded as an appropriate step in the process of safeguarding electronic payment systems. Similarly, the establishment of special business units for important shared payment services and infrastructure is an appropriate move.

The Contingency Committee for Financial Infrastructure (BFI)
Finanstilsynet is responsible for chairing and functioning as a secretariat for the committee, and will continue the work of developing the role of the BFI on behalf of the authorities, the financial industry and the individual financial institutions.

The BFI constitutes an important meeting place for various operators in Norway who have responsibilities within the Norwegian payment system. The committee has a particular focus on contingency work, and is therefore concerned with following up on incident trends. One of the initiatives is the planning and conducting of annual exercises involving the authorities, financial institutions and service providers as participants, in order to be optimally prepared in the event of a serious incident.

6.6 Further development of supervisory tools

International best practice such as Cobit, ITIL and ISO form the basis for the self-evaluation methods used by Finanstilsynet in its oversight of IT and payment systems. These provide a basis for resource-effective oversight. It is essential that supervisory tools are on a par with best practice, and Finanstilsynet will constantly upgrade its supervisory methods and tools in the light of experience gained from conducting inspections and knowledge of best practice in the area. A major review of methodology based on the most recent best practice frameworks

at procedural level, such as Cobit, is planned for 2014. The development of a tool for targeted inward reporting will also be considered.

7 Payment systems and development

7.1 General information on payment systems

Payment systems are central to all economic activity. In Norway, payment systems are governed by laws and regulations and through the financial industry's self-regulatory system, administered by Finance Norway (FNO).

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

Reliability, speed and efficiency are the cornerstones of the economy, where bank payment systems employing the "Square model" have held a central place. Technological developments have substantially influenced payment systems, with the result that more and more of the payment process takes place entirely electronically, including value chains both leading up to and following the payment value chain itself.

Technological developments coupled with deregulation and new legislation, with the EU as prime mover, coupled with consumers' and institutions' expectations and demands for simplicity and freedom of choice, present a challenge to traditional payment system models.

New and more efficient payment methods, new kinds of electronic "wallets", operators who establish themselves in various "man in the middle" roles, virtual currencies, new "settlement mechanisms" and increased cost effectiveness are some of the factors creating change in the payment mediation landscape.

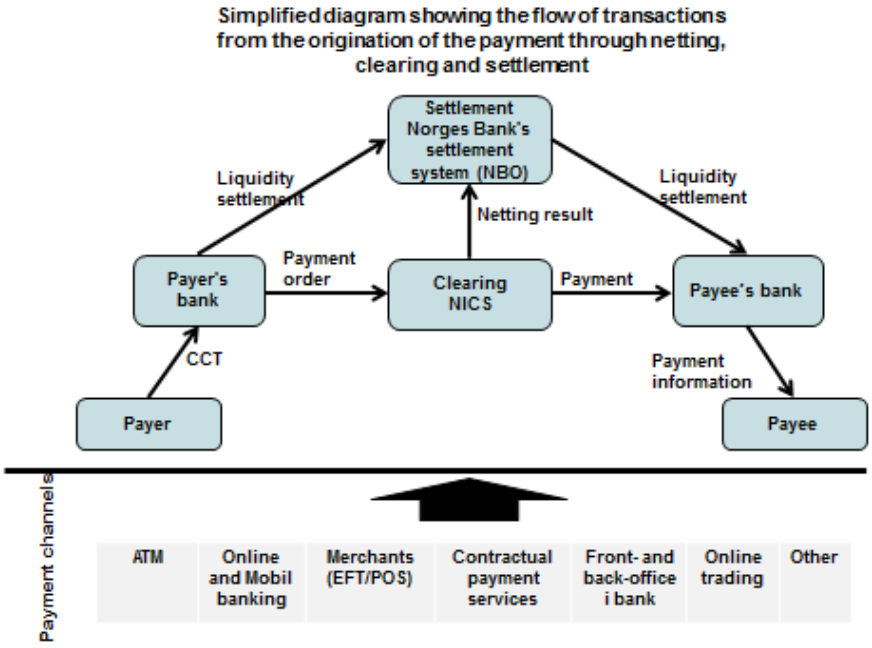
The market expects faster, more efficient, more user-friendly systems for paying for goods and services where striking a balance between competition and cooperation affects market efficiency and availability, and where user-friendliness has to be balanced against security requirements. This may result in payment value chains lengthening, requirements regarding sharing of responsibility among players becoming important, and new security solutions having to be introduced. This may lead to an increase in risk.

The Financial Contracts Act[32] and the EU Payment Services Directive are key defences established to safeguard consumer interests and to provide the best possible protection for consumer security and rights.

Figure 7 shows the flow of transactions in the Norwegian payments system. The lowermost portion of the figure illustrates the various payment channels used by customers.

[32] http://lovdata.no/dokument/NL/lov/1999-06-25-46

Figure 7: Flow of transactions in the Norwegian payment system



Source: Finanstilsynet

With the Norges Bank Act and the Payment Systems Act providing the legal basis, Norges Bank and Finanstilsynet together discharge important responsibilities in the area of payment systems, and collaboration on and sharing of responsibility have been established to achieve optimal interaction in the area.

7.2 Risk and vulnerability in payment systems

New technology will be accompanied by new and sometimes unknown applications and possibilities, but also new risks and vulnerabilities.

The participants change due to market dynamics, government regulations, emphasis on cost cuts and strategic moves by individual participants.

User-friendliness and speed appear to be the dominant factors in the battle for the payment services market. The situation changes fast, so what appears to be a market leader today may prove to be yesterday's news tomorrow. In this race, security may be a competitive parameter, but it may also suffer as a result of the excessive emphasis on user-friendliness, cost savings and time to market.

At any given time, payment systems will therefore offer risk and vulnerability challenges that call for awareness regarding security, monitoring and the implementation of measures where necessary.

7.2.1 Use of malicious software (malware) against payment services

Phishing, where swindlers pretend to be well known financial institutions or payment service providers, has become a very common means of illegally acquiring or stealing data. Phishing increased in 2013, overall, despite a decline in the fourth quarter. This type of crime targets payment cards in particular, and the fraud is often associated with payment in online shops that do not require security solutions like BankID and 3-D Secure, or where the fraudsters exploit weaknesses they have detected in payment service providers. Finanstilsynet's experience is that the institutions are well prepared and implement effective measures that curb losses by keeping customers informed, rapidly shutting down false websites, picking up responses to inquiries and monitoring transactions.

Even though Trojans are becoming increasingly sophisticated and accordingly more difficult to detect by means of traditional anti-virus software, there was a pronounced decline in activity in Norway in 2013. This can be attributed largely to active preparedness and good defences combined with modest returns. As this type of attack has come in waves, and there is still considerable activity internationally, we must assume that Norway may again be hit by targeted attacks.

7.2.2 Credit card fraud and data theft

Although the financial industry in Norway takes many initiatives and is well to the fore globally in terms of reducing vulnerability, credit card fraud is one of the highest technology risks facing the financial industry. Norwegian cards are used physically abroad, and not least in virtual online shopping.

Theft of credit card data has become big business, and the most vulnerable sites are those where large quantities of card-related data are stored or mediated.[33] Failure to secure credit card data may allow hackers to acquire confidential information that can be misused. The stolen information is often sufficient to enable fraudulent use in payment mediation, either directly or indirectly, by providing access or rights that make fraud possible.

The threat of cyber attacks on online shopping websites has increasingly become a reality. This became very evident when credit card and/or contact data were stolen from about 96 000 Norwegian card-users,[34] plus some hundred thousand card-users from other countries, in a concerted hacker attack.[35] Banks have subsequently detected card fraud that may be linked to the hacking. Another fear is that stolen information may be used for targeted phishing for more sensitive data.

Finanstilsynet notes that losses from card-not-present transactions are rising. These losses are mainly a result of fraudulent use of stolen card information on online shopping websites that do not require 3-D Secure authentication, either nationally or globally.

Failure to require 3-D Secure authentication from the online shopping website, while requiring use of the CVC code, constitutes a risk in payment mediation. When card information is stolen, it is easy to use it fraudulently on online shopping websites that do not require 3-D Secure authentication.

[33] http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/
[34] http://coop-norge.mynewsdesk.com/pressreleases/hotellbestillingstjeneste-beroert-av-datainnbrudd-929230
[35] http://news.sky.com/story/1167656/loyaltybuild-hackers-steal-card-details

The continued use of magnetic strips in many places makes fraudulent use of stolen card information easy for criminals. Although data encrypted on microchips are now being used in many places, like Norway and Europe, other countries lag far behind and this leaves openings for fraud with the aid of stolen information. One of the world's largest and best known data attacks[36] took place during last year's Christmas shopping in the USA. Information was stolen from over 110 million customers.[37, 38 and 39] It included magnetic strip information from at least 40 million customers obtained by tapping data from merchants' terminals.

Millions of encrypted PIN codes were also stolen, although there are no known cases of PIN codes being cracked. Laboratory tests[40] show that PIN codes can be cracked, but it is still uncertain whether this can be done in practice because there will normally be more security measures implemented than are taken into account in laboratory tests.

Banks maintain close surveillance in order to detect fraud, and card-holders are held harmless. Nevertheless, this type of data theft entails a great deal of extra work for card acquirer, card issuer and card owner. It is important that banks continue to implement relevant measures that can be used by both individual banks and the industry as a whole.

One measure that might be effective is for banks and international payment card companies to demand that online shopping websites implement 3-D Secure authentication. This will make theft of card information less attractive and reduce card-not-present losses. Merchants that operate only with magnetic strips also constitute a vulnerability. This occurs to only a limited extent in Norway. It is important that magnetic strips be replaced by microchips, but this also requires that all relevant countries do so.

Diversification of cards, i.e. cards with and without magnetic strips, one-time cards and one-time passwords via mobile telephones are measures that should be considered.

Failure to comply with the PCI standard (PCIDSS)[41] may create vulnerabilities that hackers are on the look-out for, not least where it is probable that large quantities of data are stored. In addition, it is important that compliance with the standard is enough in itself, and as an element in reducing vulnerabilities together with other risk-reducing measures. Closer monitoring of compliance with the PCI standard will be a good initiative.

Finanstilsynet finds that a number of banks have established the option of regional blocks. This may provide greater protection against fraudulent use of stolen card information, and is something that all banks should consider implementing. It is true that regional blocks only apply to the use of bank cards in physical terminals, and not to credit cards and online shopping, but this would nonetheless be one means of reducing opportunities for fraud.

[36] http://www.bostonglobe.com/business/2014/01/11/information-million-taken-target-data-breach/J7kRpDwXaxkPk5amUgVdXI/igraphic.html
[37] http://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337/
[38] http://www.bostonglobe.com/business/2014/01/11/information-million-taken-target-data-breach/J7kRpDwXaxkPk5amUgVdXI/story.html
[39] http://www.digi.no/926377/datavirus-i-kassa-rappet-id-er

[40] http://www.jbonneau.com/doc/BPA12-FC-banking_pin_security.pdf
[41] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

7.2.3 Mobile payment systems

The development and use of mobile systems continued to grow rapidly in 2013, to the extent that use of these systems now exceeds traditional online banking.[42 and 43] This means that mobile devices are also acquiring a significant role in payment services, as a medium for making payments, as a new kind of electronic wallet [44] and as a medium for security systems such as BankID.

There is tough competition in the Norwegian market among operators who want to ensure that their technology becomes the standard. Mobile systems must be user-friendly, and new systems are constantly being introduced. The small surfaces of mobile devices make user error a real possibility, and there is a risk that the requirements of simplicity, speed and user-friendliness may be met at the expense of security.

Mobile applications are increasingly exposed to the same risks as the traditional online banks. The Open Web Application Security Project 's (OWASP) top ten risk overviews for mobile and traditional web applications show that mobile applications are five years behind with respect to vulnerability.[45] The same vulnerabilities that manifested themselves during the development of web applications turn up in mobile applications, not necessary in the applications themselves, but on the server side.

Developments in mobile applications very largely employ new technology, and there is a risk of immature expertise. There are examples where the development of mobile applications has not been satisfactorily quality assured with respect to security. This has revealed a lack of awareness and/or poor coding in the development of applications, with the result that false information enters and information leaks out of apps.[46]

One risk aspect of mobile devices is that they are constantly being required to meet more needs, and that payment mediation is just one of these. When many functions and data are collected in one place, it creates a vulnerability that payment service providers must be aware of when they develop apps.

Although there have been no known attacks on mobile apps in Norway, it is important that the institutions make at least the same security requirements of mobile payment applications as of traditional online banking applications; i.e. that they perform thorough security and vulnerability analyses and implement measures, take action to quality assure their development processes and ensure that sensitive information is not transferred over the internet.

7.2.4 Vulnerabilities in shared infrastructure

A number of financial services are linked together and share technical resources. A fault in one service may cause one or more other services to fail as well.

[42] https://pressesenter.sparebank1.no/2013/04/paskerush-i-mobilbanken/
[43] http://www.dagensit.no/article2582872.ece
[44] http://www.dinepenger.no/bruke/disse-slaass-om-din-mobile-lommebok/22599383
[45] https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks
[46] http://www.dinside.no/923295/nettbank-appene-er-saarbare

Incidents that arise in, or affect the payments infrastructure have a broad impact and can rapidly have major consequences. It is therefore important to regularly review the risk and vulnerability of the network architecture and to take steps to prevent incidents that could affect many critical services at the same time.

7.2.5 Risk associated with changes in payment services

In addition to the development of new systems, there will be a constant need to make changes in existing payment systems, which means a high rate of change. The changes are made in applications, technology and communication systems alike, and are generated by a multiplicity of change drivers. The drivers include functional upgrading, use of new technology, replacement of sub-systems, compliance with regulatory requirements and self-imposed industry requirements, cost cuts and satisfying market demand for efficient, simpler and more user-friendly services.

Changes are a frequent cause of faults and non-conformities developing in payment systems, and there is therefore considerable risk attached to them. It is therefore essential that risk assessment and management, in addition to good end-to-end test processes and the establishment of a sound security culture at all levels, form a central part of institutions' development and change processes.

Payment systems are constantly evolving, and new operators become established. Changes in or longer value chains generate a need for clear distribution of responsibilities, whether it be among applications, stages in the value chain or different operators in the value chain. It is therefore important to perform regular risk and vulnerability analyses in connection with changes.

7.2.6 DDoS can affect payment systems and prevent access to payment and security services

DDoS attacks are not necessarily the most important in terms of vulnerabilities that can affect payment systems, although attacks continued to increase in 2013. Massive targeted attacks can make customer payment systems completely or partially unavailable for a period of time. Gartner Research describes how "low-powered" DDoS attacks are also used to disguise other attacks on payment systems.[47, 48 and 49]

In Finanstilsynet's experience, the institutions themselves and the internet service providers (ISPs) have intensified measures to minimise the impact of the attacks on availability. It is important nonetheless to continue to be vigilant and maintain defences against DDoS attacks, since they both paralyse customer services and may be a sign of other potential fraud.

[47] http://www.itavisen.no/nyheter/bruker-ddos-til-%C3%A5-kamuflere-banksvindel-90002
[48] http://www.scmagazine.com/fraudsters-target-wire-payment-switch-at-banks-to-steal-millions/article/307755/
[49] http://blogs.gartner.com/avivah-litan/2013/08/12/ddos-diverts-attention-during-payment-switch-takeover/

7.3 Management and control of payment systems

It is a management responsibility to ensure that the individual institution has an established framework for management and control of the entire payment service system and fixed procedures for important functions. Control systems must be established that ensure compliance with rules and regulations and with an established quality level. Regular value chain-based risk and vulnerability analyses are necessary, especially in connection with the development of new services and systems, to reduce vulnerability and risk to an acceptable level, put in place measures against criminal attacks and prevent serious incidents. This includes establishing a business continuity and contingency system and regular exercises in order to be in a position to act effectively when incidents occur.

It is important to ensure that all elements and players in the transaction chain between payer and payee are included in the management of operational risk. This is particularly important in light of the fact that payment systems are constantly changing, with new operators and business models, longer value chains and changes in responsibility limits. All operators in the value chain have an independent responsibility to ensure that they have the expertise and time necessary for managing and controlling operations in their own systems, those of the ICT providers and not least any subcontractors.

Much of the electronic infrastructure used by the payment systems is outsourced to ICT providers, but the institutions' responsibility for management and control remains the same and cannot be outsourced. As a general rule, security is an integral part of the service package, and in recent years has become an increasingly costly component for service providers. It is difficult for service providers to obtain compensation for this component through amendments to agreements, and there may therefore be a risk that proper provision is not made for security.

7.4 Notification requirement – payment service systems

The Payment Systems Act requires that institutions notify Finanstilsynet without undue delay of the establishment and operation of payment services. The notification shall provide information about agreements between participating institutions and service providers, whether rules governing the use of the services have been complied with, and other risk associated with payment service systems. The main objective of the duty of notification is to ensure that necessary risk assessments are made, that necessary measures to ensure safe and secure operations are implemented, and that any agreements between the parties involved are established before a new payment system is implemented.

In 2013, Finanstilsynet received 38 notifications, 23 of them concerning BankID on mobile devices, four concerning offers for services for hand-held devices, four concerning changes associated with foreign payments, two about substantial changes in the use of payment services and two about other payment-related services. Finanstilsynet also received three retrospective notifications concerning previous years. There was no need in 2013 to follow up institutions on the basis of the notifications received.

Even given a substantial increase in the number of notifications, there is still assumed to be under-reporting of changes in payment systems, and Finanstilsynet will take steps to ensure that the duty of notification is observed.

7.5 Overview of annual losses related to payment services

7.5.1 Losses in Norway

The tables below present figures for the last three years for losses due to credit card and internet banking fraud in Norway. The losses represent all banks in Norway, and have been obtained from Finance Norway and the Norwegian Banks' Standardisation Office (BSK) in collaboration with Finanstilsynet.

Table 1: Losses related to use of payment cards (figures in NOK 1000s)

Type of payment card fraud	2011	2012	2013
Fraudulent use of card information, card not present (CNP) (online transaction)	24,190	35,701	51,954
Stolen card information (including skimming), fraudulently used with counterfeit cards in Norway	468	2,308	762
Stolen card information (including skimming), fraudulently used with counterfeit cards outside Norway	57,340	55,869	51,534
Original cards lost or stolen, fraudulently used with PIN in Norway	32,224	28,128	21,274
Original cards lost or stolen, fraudulently used with PIN outside Norway	7,008	8,544	9,570
Original cards lost or stolen, fraudulently used without PIN	4,488	4,603	4 949
TOTAL	**125,718**	**135,153**	**140,043**

Source: Finanstilsynet

Table 2: Number of payment cards affected by fraud

Type of payment card fraud	2011	2012	2013
Number of cards affected by fraud	16,784	20,332	22,531

Source: Finanstilsynet

Total card fraud losses increased somewhat in 2013. There was a considerable increase in card-not-present (CNP) fraud, but a reduction in losses associated with other types of card fraud. CNP is online shopping using payment cards via the internet, by telephone or by e-mail. The card information may have been illicitly acquired through phishing or hacking of merchants' or card payment service providers. As mentioned in chapter 4.3.1, there was a strong increase in 2013 in phishing designed to dupe people into disclosing payment card information. Finanstilsynet is not aware of any hacking of Norwegian merchants or service providers in 2013, but is aware of major hacking in Ireland and the USA.

Of the total volume of card payment transactions in Norway, fraud accounted for about 0.018 per cent. This is lower than in the euro countries (SEPA), where the share in 2011 was 0.036 per cent.[50] However, if online shopping with cards issued in Norway is considered (NOK 53 billion in 2012),[51] the fraud figure is close to 0.1 per cent.

[50] http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf?1b8fb7a7abcf9c9f5a0dd8e6eada19e2

[51] Norges Bank's Annual Report on Payment Systems 2012
http://www.norges-bank.no/pages/94894/Betalingssystem_2012_o.pdf

3-D Secure (Verified by Visa / MasterCard SecureCode)
3-D Secure is a security system offered by VISA and MasterCard to make online shopping more secure and to reduce card issuers' losses in the event of unauthorised use of cards on the internet. The system also offers the merchant improved settlement rights.

Two conditions must be fulfilled for 3-D Secure to be applicable.
- Issuing bank must have installed 3-D Secure on the card.
- Merchant must have implemented 3-D Secure at the merchant (transaction) site.
If both conditions are fulfilled, extra authentication information is required from the user through 3-D Secure before the online transaction can be completed. The extra authentication information may take the form of a fixed password, use of BankID, a code received by SMS from the card issuer or similar.

If either the issuing bank or the merchant has not implemented 3-D Secure, the transaction is completed without this extra security. A card acquirer who enters into an agreement with the merchant on the use of the payment card may refuse to enter into agreements with merchants that do not establish 3-D Secure.

A special models has been established for handling losses in order to encourage the establishment of 3-D Secure systems. If neither of the parties has 3-D Secure, or both have it, it is the issuing bank that incurs the loss. Otherwise, it is the party with the poorest security that incurs the loss.

Table 3: Losses related to use of online banking (figures in NOK 1000s)

Type of online banking fraud	2011	2012	2013
Attacks using malicious software on customer's PC (Trojans)	664	5,064	1,327
Lost/stolen security device	3321	3,367	1,321
TOTAL	**3,985**	**8,431**	**2,648**

Source: Finanstilsynet

Online banking losses declined in 2013. In order to provide an accurate picture of the fraud level, banks reported on two other parameters in addition to losses:

- fraudulent transactions that are registered in an online bank with a valid account number and an amount, but where completion was prevented.
- the number of customers whose bank discovered that the customer's computer was infected with an active online banking Trojan.

These figures also indicated a substantially lower intensity of attacks in 2013 than in 2012.

Initiatives on the part of the banks, including warning customers, rapidly closing down false websites, intercepting answers and monitoring transactions, were effective.

Losses where phishing was involved in attacks are included in the loss figures for both payment card fraud and online banking fraud. Thus the escalation of phishing activity in 2013 did not result in higher online banking losses. One reason for this may be, as mentioned previously, that IT users in the Nordic countries are among the most security conscious in the world with respect to IT security, and have the lowest rate of infection with viruses and

malware.

Norges Bank's statistics on online banking in 2012 show that about 430 million online banking payments were made. Online banking agreements in Norway totalled 6 092 944.

7.5.2 Loss figures in other European countries

The overview Fraud the Facts 2013[52] issued by the UK Financial Fraud Action (FFA) shows an increase in card-related losses in 2012. Card-not-present losses rose 11 per cent, and accounted for a total of 63 per cent (equivalent to approx. GBP 246 million) of card-related losses. Losses associated with online banking also increased in 2012, which may be due to more sophisticated types of phishing.

The UK is mapping the amount of phishing through the number of identified false websites in the name of financial institutions. There is no direct connection between phishing and loss figures, but the false websites conceal losses associated with both card-not-present transactions and online banking.

Figure 8 of Fraud the Facts shows a massive increase in the number of infected websites up to November, when a dramatic decline occurs (see arrow). The decline is due to the fact that the special police authority for electronic crime in the UK, the Police Central eCrime Unit (PceU), exposed a band of professional fraudsters and succeeded in stopping the botnet administered by the band.

Figure 8: Phishing attacks on UK banks

Number of phishing websites targeted against UK banks and building societies by month 2005-2012

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2012	18,252	6,629	14,362	20,669	24,578	26,818	39,767	41,734	27,869	30,036	3,523	2,404	256,641
2011	5,803	5,757	6,828	5,698	6,216	6,896	7,402	8,062	23,083	9,397	15,395	10,749	111,286
2010	2,654	3,135	4,810	4,335	5,406	5,277	5,873	5,861	5,689	6,977	4,552	7,304	61,873
2009	4,206	5,161	5,004	3,422	3,917	4,335	4,415	4,845	3,900	4,903	4,191	5,864	51,161
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	43,991
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	25,797
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	14,156
2005	18	29	27	54	72	122	153	160	190	267	255	353	1,700

Source: Financial Fraud Action UK

Loss figures from Belgium published on Febelfin[53] show that online banking losses increased by over 50 per cent from 2012 to 2013.

[52] http://www.financialfraudaction.org.uk/downloads.asp?genre=consumer

[53] http://www.febelfin.be/nl/aantal-gevallen-van-phishingfraude-neemt-toe-1

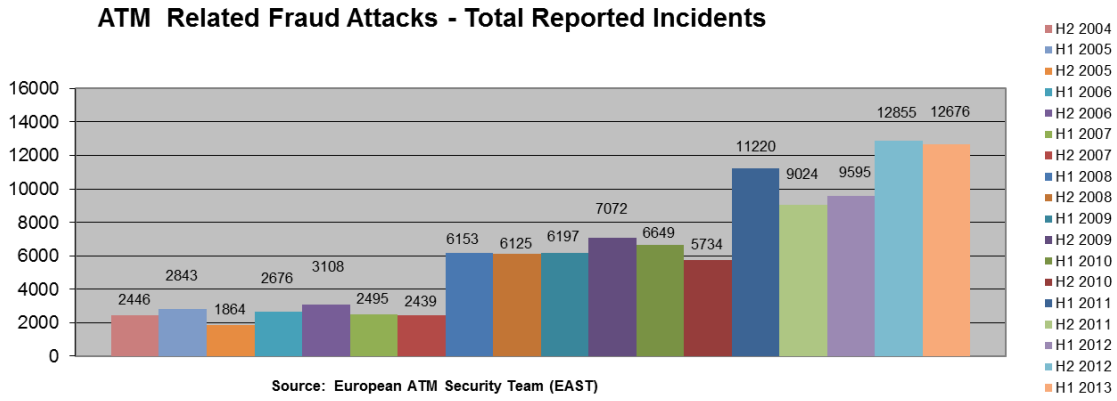
However, loss figures published by the Dutch Banking Association[54] show declining loss figures. Losses in the Netherlands in the second half of 2013 were equivalent to only a third of the losses in the first half of 2012.

7.5.3 Fraud attacks and losses on ATMs in the EEA

The European ATM Security Team (EAST)[55] prepares semi-annual reports which show ATM-related attacks and losses in the EEA.

In recent years, with the exception of 2010, there has been an overall increase in fraud attacks on ATMs in the EEA; see Fig. 9. However, the losses have remained at the same level for the past three years. Almost all losses are related to skimming. Because magnetic strips are still used on payment cards in a number of countries, they are particularly vulnerable to skimming attacks. Skimming of Norwegian cards occurs almost exclusively in other countries.

Figure 9: ATM-related fraud attacks within the EEA



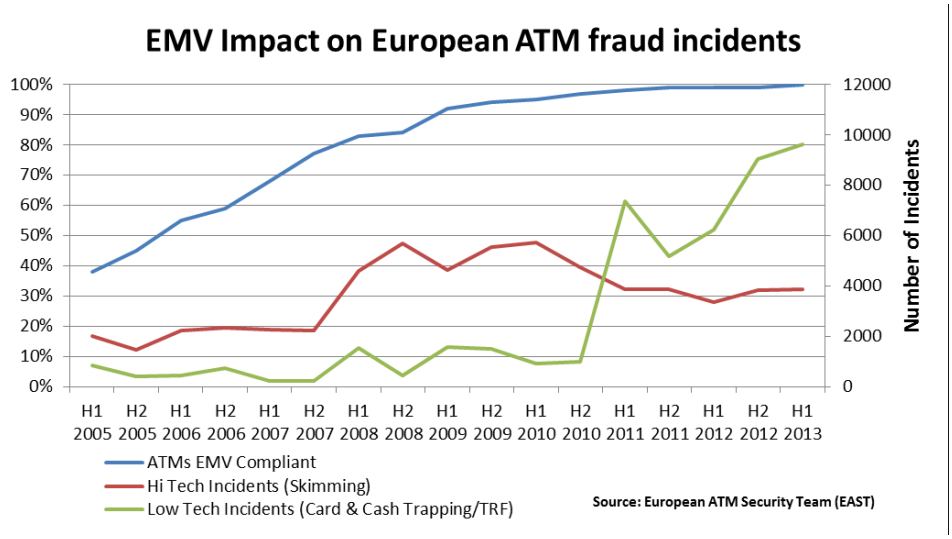
Source: EAST

As the figure below shows, there has been a marked shift since 2011 from "Hi Tech" attacks (skimming) to "Low Tech" attacks (card and cash trapping/transaction reversal fraud (TRF)) without a corresponding shift in losses, since about 97.5 per cent of all losses are associated with skimming.

[54] http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html

[55] The source is the semi-annual ATM Crime Report of the European ATM Security Team (EAST)

Figure 10: How the implementation of the EMV standard has affected fraud attacks on ATMs



Source: EAST

The number of physical attacks on ATMs within the EEA has remained at about the same level, around 2,000 annually, for the past five years. RAM attacks and ATM break-ins account for the majority. However, losses show a falling trend. This type of attack is seldom seen in Norway.

7.6 Netiquette, mobile phone etiquette and card etiquette

Since banks' payment services and other activities are increasingly digital and electronic, it is important that financial institutions have relevant and up to date "etiquette" information for their services clearly visible and easily accessible to cards, online banking and mobile devices. The information should cover both private and corporate customers and have simple links to supplementary websites. Finanstilsynet has noted that some institutions have conducted security campaigns.

There is a great deal of information available on a number of websites about netiquette, i.e. advice on how to behave on the internet. There are similar guidelines on the use of payment cards and mobile devices. Many of the websites place particular emphasis on protection of privacy and general netiquette. Nettvett.no,[56] for which the Norwegian Post and Telecommunications Authority is responsible, also provides advice on online banking and trading and mobile devices.

Finanstilsynet has looked at the information provided by a number of institutions on netiquette, mobile etiquette and card etiquette. There is plentiful information on the institutions' websites, but the coverage, overall information and visibility varies. Discussions of card etiquette, netiquette and mobile etiquette are often to be found on different pages of the individual institution's website. Assembling this information in one place makes it more accessible to users. There are also often different websites for individuals and for corporate customers. Many institutions also have useful inks to good netiquette websites, such as

[56] http://www.nettvett.no/

nettvett.no and norsis.no,[57] which in turn have links to other sites, such as those of the Norwegian Consumer Council[58] and the Consumer Ombudsman.[59]

It is important that the institutions provide sound information and advice on caution regarding security in connection with the use of electronic banking services. Establishing exhaustive information pages and keeping them updated may be a laborious process, but at the same time they will constitute an important supplement to the services provided.

7.7 Development of EU legislation

Proposed new Payment Services Directive (PSD2)
Changes are needed in the existing framework conditions for payment services, to take into account regulatory adjustments, clarifications and the incorporation of technological and market-related developments with a view to providing greater homogeneity across national legislations. The proposal also seeks to promote greater cooperation and repeal regulations that inhibit and distort competition. The proposal may entail amendments to the Financial Contracts Act and the Financial Institutions Act, the Regulations relating to Payment Service Providers and the Regulations on the use of information and communication technology (ICT) and in the financial industry's self-regulation in areas such as payment services (the Blue Book).

The proposed new Payment Services Directive implies among other things

- that third-party service providers (TPP) who do not hold payer's or payee's funds, shall be regulated to comply with requirements relating to security, data protection and liability. TPPs must be registered and supervised as payment institutions in order to be allowed to offer payment services. This means that they will be subject to the same rights and obligations and special security requirements as other payment service providers. The directive provides clear guidelines regarding access to account information, authentication requirements and correction of transactions and liability for unauthorised transactions.
- that it shall also apply to cross-border transactions where one leg of the transaction is executed within the EEA, and in some contexts also for all currencies.
- a harmonising of the rules for limiting the customer's objective liability in connection with unauthorised transactions to 50 euros, if the customer does not observe his security obligations
- no limits on liability. In the event of gross negligence, the payer may within eight weeks unconditionally require repayment of directly debited amounts, provided that the goods have not been consumed.
- updated rules regarding which payment-related activities may be exempted from the directive.
- streamlining and harmonising of requirements regarding security measures for assets held in the payment system.

[57] https://norsis.no/

[58] http://www.forbrukerradet.no/

[59] http://www.forbrukerombudet.no/

- expansion of the regime for restricted permits to engage in payment services by reducing the threshold for such permits
- requirements regarding payment service providers' management, control and reporting of risk and notification and reporting of incidents.

The proposed directive also contains changes that imply that the European Banking Authority (EBA) is expected to contribute in several areas by

- ensuring consistent and homogeneous/uniform supervision
- providing guidelines and draft regulatory and technical standards in various areas, such as ensuring the establishment of adequate security requirements or clarifying "passporting" rules for payment service providers operating in several member countries. Passporting allows an institution with a licence in an EEA country to freely establish branches and agencies in other countries, unless the host country has major objections. These branches and agencies will then be subject to oversight by the supervisory authority in the home country.
- establishing a European access point for information on registered payment institutions in order to ensure greater openness and disclosure.

Proposal for regulation of interchange fees for card-based payment services
As part of the work on a new Payment Services Directive, it is proposed in a separate regulation (MIF Regulation) that multilateral interchange fees (MIFs) should be regulated.

The proposal outlines card use in a regulated and in a non-regulated area. The regulated area covers consumers' use of payment cards in payment terminals, online payments and mobile payments, but it applies only to transactions in the four-party schemes and the "licensed" three-party schemes. The unregulated area consists of all payment card transactions and card-based payment transactions that fall outside the regulated area. This includes "commercial" cards, cards issued by third-party providers and withdrawals from ATMs.

The regulation is divided into two main parts: rules concerning interchange fees and surcharges and rules for good business practice. The whole regulation applies to the regulated area but only the rules for good business practice apply to the non-regulated area.

Proposed rules concerning interchange fees involve caps on fees linked to debit and credit cards of 0.2 per cent and 0.3 per cent, respectively. A two-stage process is proposed, with application to cross-border payments a short time after the legislation has been adopted, and to all national consumer card payments two years later. Prohibition of surcharges is also proposed.

Rules for good business practice concern:

- the right to issue and acquire cards for the whole EEA
- separation of payment schemes from the processing of card payments
- limitation of the "Honour All Cards Rule", which implies that "similar" types of cards must be treated in the same way.
- issuer's right to co-branding and user's right to choose means of payment, which will affect co-branding of Norwegian cards (BankAxept and Visa). The current priority rule will then no longer be legal.

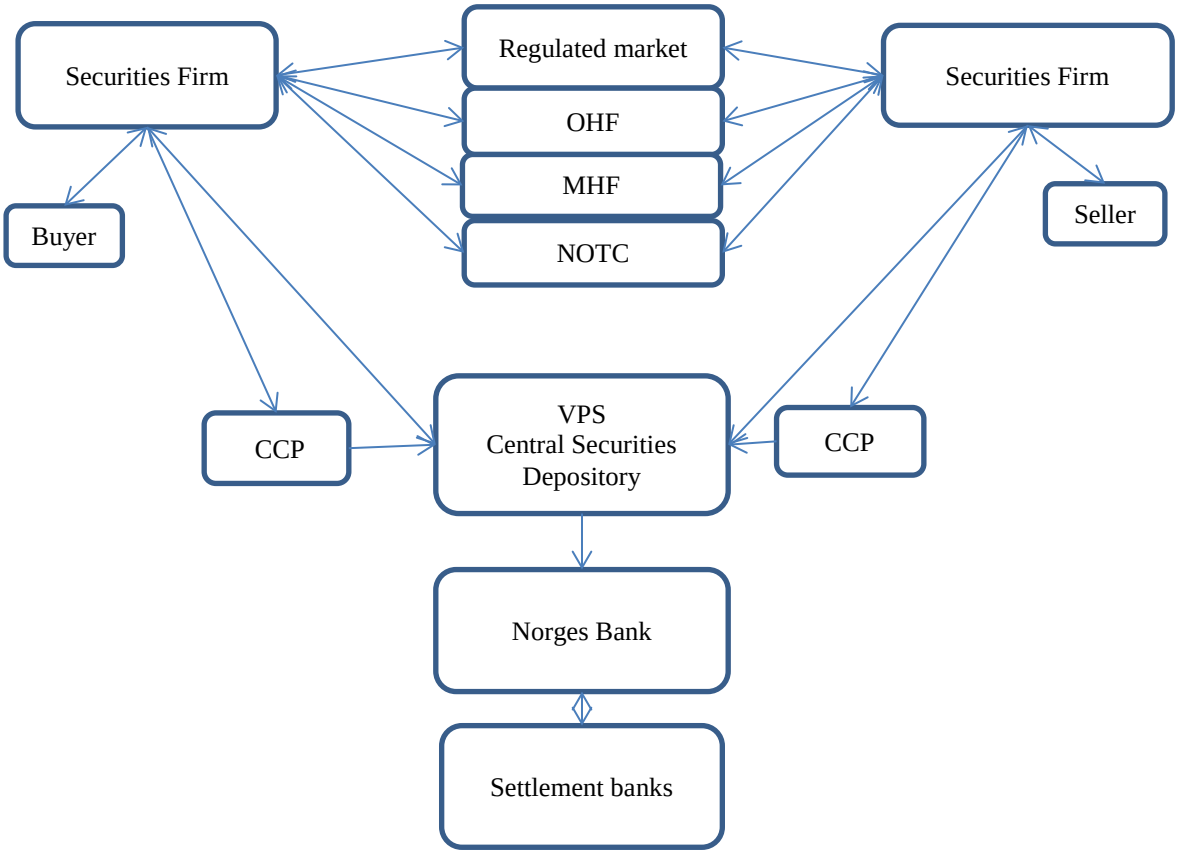
- the rule that issuing banks must offer and charge payees individually for the different card brands and payment cards
- the duty of payment service providers to provide payees with information on each payment transaction carried out
- prohibition of rules that prevent dealers from informing consumers of the actual costs of card-based payment services and regulation of dealers' right to guide consumers towards their preferred payment instrument

8 The securities area

Extensive changes are taking place in the area of securities which in combination may represent a risk related to the scope and quality assurance of these changes. Here, too, old legacy systems represent a challenge, and conversion will entail risk during the process. There are several regulatory changes in this sector that will affect infrastructure and operators in an increasingly borderless EU. New marketplaces for securities trading based on cross-border electronic trading affect the existing marketplaces in terms of both volume and earnings and help to create a need for change.

The following is a flow chart showing important roles and relationships in the securities sector. The overall picture in this sector in Norway is still one of both high stability and high quality, but there have been incidents, and given the changes expected to occur in this sector in the near future, ensuring acceptable risk may be a challenge.

Figure 11: Roles and relationships in the securities sector



Source: Finanstilsynet

8.1 Risk of underinvesting in the event of reduced earnings

The framework conditions for the Norwegian securities trading infrastructure has undergone major changes. Changes in the Securities Trading Act ensuing from a desire for more competition over securities services and lower costs for investors have resulted in the Oslo

Stock Exchange now accounting for less than 50 per cent of turnover of shares that are primarily listed on the Oslo Stock Exchange. The liquidity of Norwegian listed shares is now spread over a number of different marketplaces such as Chi-X, BATS and Nasdaq OMX.

In order to be able to offer combined liquidity from these marketplaces, the securities firms have set up IT systems that can trade across several marketplaces simultaneously. One of the results of this automation of trading is that market skewness and delays that traders with an investment horizon of less than one day used to exploit have been considerably reduced. This means that the bulk of the turnover that this type of customer represented for securities firms has dwindled away. The commission income of non-bank stock-broking firms sank from NOK 2.4 billion in 2007 to NOK 0.5 billion in 2012. The consequences for small securities firms of increased infrastructure and trading system costs exceeded the reduction in transaction costs. As the trading volume in the secondary market has fallen at the same time, the profitability of securities firms for which this has been a substantial source of income has also dwindled to nothing.

Lower income and higher costs may translate into pressure on the IT sector to reduce costs, and this may have negative consequences for both the quality and the security of IT system administration.

8.2 Risks associated with algorithmic trading

In the last couple of years there have been cases where algorithms used for high-frequency trading in the Norwegian equity market have resulted in unintended trading activity due to programming errors. This has resulted in losses for securities firms. The cause of the errors has been failure of or deficiencies in the company's change procedures.

The consequence of such faults in algorithmic trading may be substantial losses for the company carrying out the transaction, and market prices may also be affected.

8.3 Back-office systems in the securities market

Most Norwegian securities firms use very much the same back-office systems today. This has made it possible for the supplier to distribute the heavy costs of developing these systems among all operators, and thereby achieve economies of scale. The risk, on the other hand, is that expertise in this area will also become concentrated, and the advantages offered by a market with a number of suppliers will be lost.

8.4 Outsourcing of core systems

Securities firms have also increased their outsourcing of front- and back-office systems to system providers. In the short term, this reduces overall costs, and will probably also reduce the number of fault situations due to operations locally at the individual enterprise. Concentration risk will increase, however, and any fault situations will have major consequences for the entire market. One of the challenges faced by securities firms in outsourcing their core systems is to retain sufficient internal systems expertise for management and control of suppliers.

8.5 Concentration risk in the network infrastructure

Securities market participants all use very much the same network infrastructure in relation to marketplaces and clearing houses. This infrastructure has so far proved both robust and cost-effective. Finanstilsynet is particularly concerned by the fact that this represents a concentration risk, with major potential consequences in the event of fault situations.

8.6 Regulatory development

Over the next few years, new regulation of financial infrastructure operations in Europe will have a considerable impact on Norwegian securities firms and appurtenant infrastructure. The new rules must be expected to require many system adjustments and substantial investment in the development of new systems, often with a short implementation deadline. This in turn will normally require that securities firms invest significant resources in testing and implementation. Short deadlines may also put considerable pressure on the development of specifications for systems and the systems themselves. Delays can easily occur, and the result may be development under time pressure with the result that the solutions have faults and deficiencies, which may have undesirable consequences for production and stability in the securities market.

Examples of imminent regulatory changes in the EU include the Capital Requirements Directive (CRD IV), the European Market Infrastructure Regulation (EMIR) and the Financial Instruments Directive concerning investment services (MiFID II). These changes will entail new reporting requirements for institutions, with challenges relating to a pan-European choice of system and probably considerable work in making the associated local adaptations. New reporting requirements in connection with short trading are also in the offing.

The Foreign Account Tax Compliance Act (FATCA) will also generate changes and new system designs. Pursuant to FATCA, an agreement between the US tax authorities and the Norwegian Ministry of Finance requires the release of information on American taxpayers who are clients of Norwegian financial institutions.

8.7 Securities firms' handling of sensitive corporate data on IT systems

Information that goes astray is a known risk factor. Sensitive corporate information in securities firms and information concerning corporate events may cause considerable harm. Corporate information that may affect share prices must be protected. The firms must ensure that the information is adequately protected during storage and transport, in connection with printouts and e-mails (encryption), and when stored on flash drives. The firms must also ensure adequate control when using cloud-based file exchange systems like Dropbox to distribute sensitive information.

From now on, Finanstilsynet will place emphasis on supervision of processes for handling access to such data areas, and the use of logs for detecting leakage of information that may affect share prices.

8.8 Risk in connection with changes of key infrastructure components for securities trading

The Norwegian Central Securities Depository (VPS) is currently replacing major components of its core systems. This is a large-scale project and will therefore involve risk. Finanstilsynet expects the VPS project to perform high quality risk assessments and that it will follow these risk assessments up through the project.

9 Glossary

Term/abbreviation	Meaning
3-D Secure	3-D Secure is an XML-based protocol used in internet payments. It provides an extra layer of security to card transactions by verifying the user in relation to the card issuer, irrespective of the payee. In connection with the use of Visa, which developed the protocol, it is called Verified by Visa.
Advanced Persistence Threat (APT)	Persistent attacks on systems aimed at acquiring confidential information. Normally consists of an exploratory phase in which many methods are used, an implementation phase which proceeds as covertly as possible, often with low intensity, and frequently a final phase to cover tracks.
Anti-Money Laundering	(AML)
BFI	See Contingency Committee for Financial infrastructure
Big Data	The concept is not well defined, and is used with slightly varying meanings by different operators and in different contexts. It involves large quantities of data collected from both internal and external sources, in both structured and unstructured form. It requires substantial storage capacity and high processing power for extracting valuable information. The expectations are that this should enable informed decisions to be made rapidly in difficult cases.
Botnet	A term compiled from the words 'robot' and 'network'. A network of programmes on various servers linked together via the internet. The programmes work together on a given task.
Business intelligence	Methods and technologies for converting raw data into useful and meaningful information about the business. Popularly defined as user-friendly interpretation/presentation of large quantities of data.
CERT	Computer Emergency Response Team. Team of experts who deal with cyber security breaches.
Cloud computing	Remote network-based services. Distributed computing over a network. Possibility of running software on a large number of networked servers. Cloud computing may be both private-and public sector, or a combination of the two. The term is used differently by different service providers; the services are often delivered via the internet.

Computer emergency response team	See CERT.
Contingency Committee for Financial infrastructure	Committee for coordination in the event of financial sector crises. Chaired by Finanstilsynet.
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.
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
FATCA	Foreign Account Tax Compliance Act
FI-ISAC	Financial Institutes – Information Sharing and Analysis Centre. A European initiative consisting primarily of participants from CERTs, banking organisations and police authorities. In Norway, a collaboration between NSM, BSK and Finanstilsynet. At present an informal collaboration between individual countries and defined authorities, supported by ENISA. The USA has established an authority covering the same area. Exchanges semi-confidential information on vulnerabilities, attacks and measures associated with the use of the electronic payment systems.
Forking	Trapping money in ATMs so that it cannot be released, nor can it be withdrawn by the ATM. When the customer has gone, the money is picked up by the fraudster.
Internet of Things (IoT)	At present a somewhat undefined concept. Concerns the fact that things can be linked to the internet in many different ways: as identifying 'tags' for objects, or in a more sophisticated way via WiFi networks, for example. Many devices have built-in computers and can communicate with other devices and service centres. The deployment of sensors for acquiring data is also included in the concept. The technology makes it possible to have services performed from anywhere, at any time, by anyone, by means of any compatible device.
ISACA	Information Systems Audit and Control Association – an independent, non-profit organisation. Works on developing and promoting the use of globally accepted and industry-leading knowledge and practice for information systems. ISACA stands for**,** but has now changed its profile to an IT Governance organisation.

ISO 20022	ISO 20022 is the ISO financial services messaging standard. It contains descriptions of the messages and business processes and their maintenance.
Jailbreaking	For iPhones: changing a telephone's security settings, for example by allowing the user to use an operator other than the one to which the telephone is locked (if it is locked to an operator). The supplier does not support such changes, and security holes may ensue.
MIF Regulation	Regulation on multilaterally-fixed interchange fees for card-based payment transactions
Miscalibration	Often used about judging information on the basis of the wrong starting point/premises, so that incorrect conclusions are drawn.
Multisourcing	Distribution of deliveries among a number of suppliers, but in this context such that different products are procured from different suppliers.
NIS Directive	EU directive designed to secure a high common level of network and information security in the EU
Offshoring	Procuring services from outside the borders of the country
Outsourcing	Procuring services from outside one's own institution
Overconfident	Self-assured because of a large quantity of information. May overlook vital factors that are not included in the information base.
Overlay services	Third-party services in the interface customer–bank.
Phishing	Pretending to be someone else, and in this guise seeking information from a person. This is an attempt to exploit the person's trust in the original sender.
PKI	Public key infrastructure. Consists of hardware, software, procedures, guidelines and personnel necessary to create, manage, distribute, use, store and revoke digital certificates.
PSD2	New payment services directive from the EU (so far at draft stage).
RAM attacks	Malware that reads the hardware memory, where information is not encrypted.
Rooting	For Android: Like 'jailbreaking' for Apple/iPhone.

Sandbox	A virtual container (protected area) where it is possible to run a program without it affecting other programs.
TPP / Third Party Providers	Concept from the PSD2 Directive. These are service providers that provide payment services and that do not normally hold the payer's or the payee's accounts.
Trojans	Viruses that pretend to be ordinary programs, but which contain malware.

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO