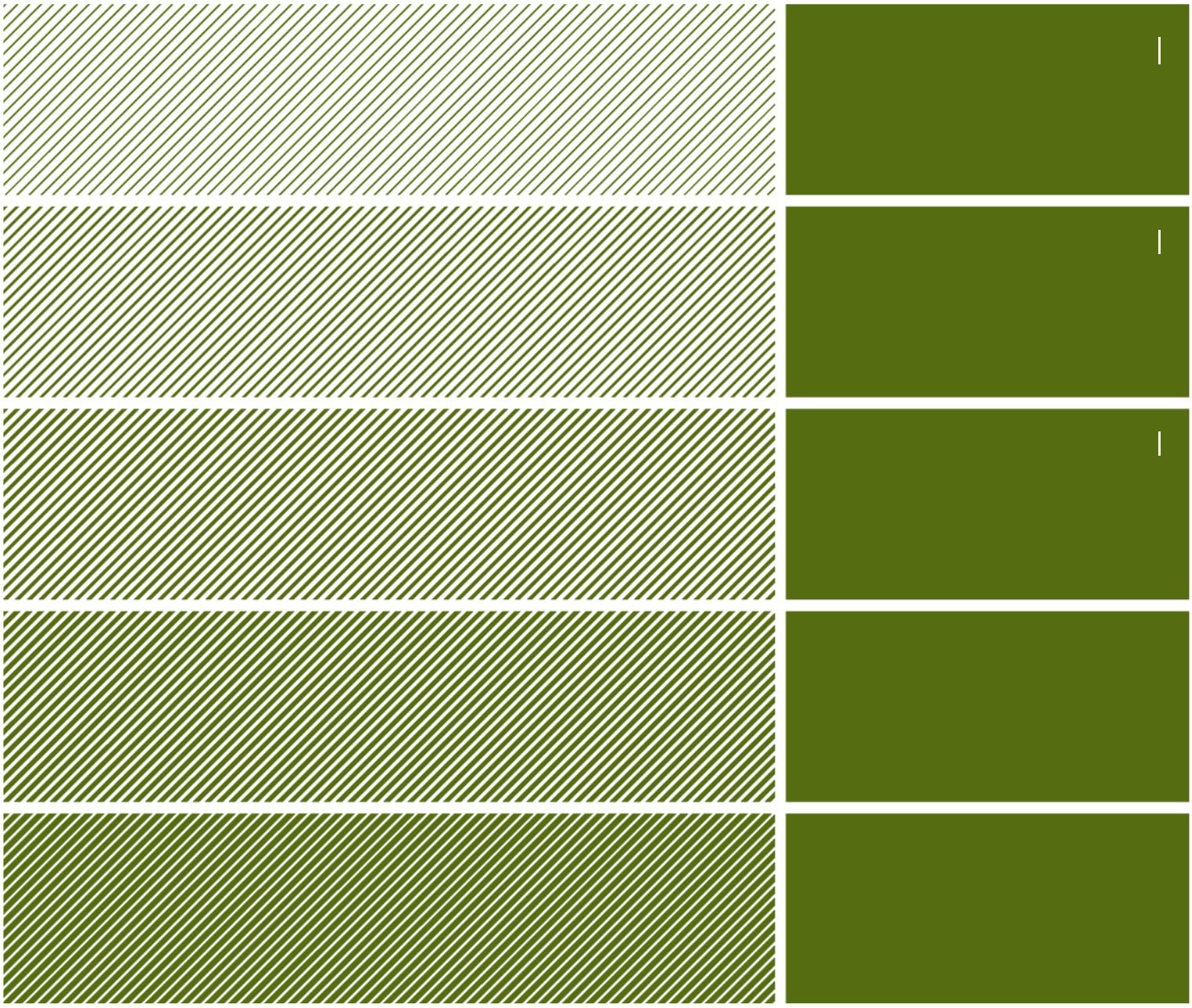
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Report

Risk and Vulnerability Analysis 2011

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



Risk and Vulnerability Analysis (RAV) 2011

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

Finanstilsynet, 28 March 2012

Translation as of April 2012

Contents

1 Introduction

Finanstilsynet (the Financial Supervisory Authority of Norway) performs an annual risk and vulnerability analysis (RAV analysis) of the financial sector's use of ICT. The report is based on data from a number of internal and external sources, and contains assessments of how identified global risks can impact the financial sector in Norway. Technological developments and the financial sector’s introduction and use of ever more complex services is making work relating to risk more demanding for both the individual enterprise and the authorities. New technology often contains unknown vulnerabilities which during the early phase can be both exploited by criminals and result in failures.

The internet opens the way for global electronic crime, or cybercrime. If the financial sector is to be at the forefront, it must have access to correct information on international trends and systems for handling and reacting, both legally and technologically, to undesired incidents.

In order to understand what may give rise to higher risk in the future, it is important to have the facts of the risk situation and to be capable of determining which factors may change over time and result in higher risk.

2 General trends

Changes due to cooperation, mergers, increased cross-border competition, product development, cost-cutting programmes and access to new technology require a great deal of change management. Change means greater risk. It therefore pays to know what drives the changes, so that they can be brought about in a controlled manner.

2.1 New internet protocol

Work is currently in progress to introduce Internet Protocol Version 6 (IPv6[1]) as a supplement to and in due course replacement for Ipv4, because there is beginning to be a shortage of IPv4 addresses. Preparations for a transition to IPv6 have been in progress for many years. Nevertheless, only a small amount of internet traffic (approx. 1 per cent) takes place by means of IPv6 today. The life of IPv4 has been extended by means of various technical solutions such as dynamic address assignment and address sharing, but the need to change to IPv6 is now starting to be critical for a number of reasons:

- Some parts of the world have virtually no IPv4 addresses left.
- Technical extension of the life of IPv4 may result in users in different places getting the same IP address with lack of traceability and other complications as a consequence.
- Extending the life of IPv4 entails major unnecessary investment in equipment which may be wasted when the transition to IPv6 takes place.
- IPv6 contains improvements and new advantages that the users are interested in.
- The wide and increasing spread of mobile devices (speech, video and data) and extensive use of machine-to-machine communication (M2M) can only be realised with the larger address space of IPv6.
- Major service providers such as Google are switching their services to IPv6. Dominant international operators such as AT&T have adopted an IPv6-only policy.

The Norwegian public sector, represented by the Agency for Public Management and e-Government (Difi) intends to introduce IPv6 as a collateral standard.

IPv6 implies a number of improvements. The address space has been increased from 32 bits to 128 bits, packet switching is more efficient, address assignment is more dynamic, one-to-many communication is improved, encryption and authentification are possible as part of the protocol, the quality of service (QoS) has improved as have other factors.

The switch from IPv4 to IPv6 is intended to be seamless from the users' point of view. A number of transitional mechanisms have been developed to ensure that IPv4 nodes and IPv6 nodes can communicate over IPv4 and IPv6 networks. This is necessary because hardware and software that require IPv4 will continue to exist for many years – perhaps 10 years or more. The transition mechanisms also contain potential weaknesses that may be the starting

[1] **IPv6** is version 6 of Internett-protokollen and is the successor to IPv4. The main reason for developing a new standard was to handle the shortage of IP addresses. At the same time, a number of deficiencies in IPv4 were rectified.

point for outages, service degradations, non-availability and vulnerability to attack.

The situation among the major internet providers in Norway is that some are already delivering mainly IPv6, some will introduce IPv6 in the course of 2012, and some are planning a major roll-out in 2013. Financial sector users must decide how to relate to this. It is probable that a number of service providers globally will switch to IPv6 as a standard for their services in the course of 2012.

2.2 The internet as a critical infrastructure

An increasing number of services use the internet, and society as such is growing more dependent on the internet. Health services, telephony, police, electricity and finance depend on the internet. In the past, telephony continued to function even during power cuts, but this is not necessarily the case today.

Securing the internet is a challenge because the following aspects of security are not known:

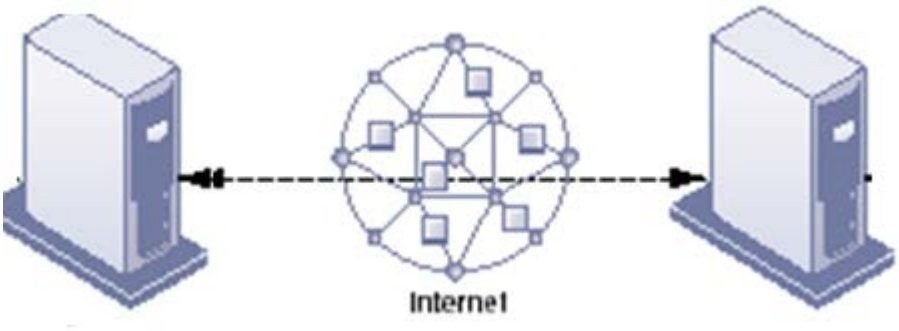
- The topologies are not known. Attempts have been to analyse a few of them; even fewer have been made public
- Neither peering points[2] nor Service Level Agreements (SLAs) between operators are known
- Routing strategies[3] are not known
- The routing policies[4] used are not known
- Correlated vulnerabilities arising from co-location of cables and routers are not known

This last point was illustrated to the full by the fire at Oslo Central Station in 2007, when the contingency system was co-located with the primary system.

NorNet[5] is an example of experimental network research. NorNet is a set of network nodes where virtual networks with user-defined routing protocols and applications can be tested. A key question that this research may answer is whether robustness and performance can be increased by using several networks dynamically.

[2] Peering points. The internet is a collection of networks, all linked together so that data can be transmtited from one network to another. Often two networks are not connected together directly, but are connected via a third-party network.
[3] Routing strategies that apply to all packets. Examples: “minimum hop number”, “static routing”, “dynamic routing”.
[4] The data packets’ routing, prioritisation, service flag etc., determined on the basis of access lists, packet size and other properties of the packets. The rules are set by the network administrator.
[5] NorNet is a national infrastructure for experimental network research financed by the Research Council of Norway.

Figure 1: There are several ways forward



Use all line suppliers

One prerequisite for being able to answer the question is knowing whether the lines are independent and autonomous, i.e. whether one incident will damage the lines of several suppliers. As far as Finanstilsynet knows, there is no complete overview of this area.

Serious incidents in the telecommunications network in spring 2011 affected large parts of the telecoms infrastructure in Norway. Some operators did not have access to alternative routings and were hard hit.

Nevertheless, it is the many small incidents that are a major challenge. Statistics on mobile broadband show that 1 of 3 connections are down for more than 10 minutes per day. There are many nodes involved in a connection, and downtime may be as high as around 1.5 per cent. This is considerably more downtime than is usual for critical components in an ICT infrastructure, where there is often a downtime requirement of less than 0.05 per cent.

Payments that use mobile broadband, for example sale of tickets on buses, or settlement for taxi transport, will not function in such a situation. Inadequate availability, as described above, could be incompatible with some mobile services, such as health services. But measurements show that suppliers of mobile services fail independently of one another. They are very rarely (0.02 per cent) down concurrently. In other words, there is a high potential for greater robustness if it is possible to use the networks of several operators. For uses that require high availability, it may pay to offer one subscription that uses all networks. Laboratory tests show that this is fully possible in purely technical terms. As far as Finanstilsynet is aware, no such option exists today.

2.3 Telecoms deliveries in Norway

The financial sector is completely dependent on telecoms services for the parts of its activities that are currently based almost 100 per cent on digital systems and data communications. This applies within the individual financial institution, between financial institutions and ICT suppliers and with suppliers and business partners outside Norway.

If telecommunications fail, it will be noticed immediately, since banking services in today's solutions mainly extend all the way to customer service points. This applies to financial institutions' own branch networks, ATMs deployed in banks or public places, EFT/POS[6]

[6] EFT/POS electronic funds transfer – point of sale

systems at merchants' terminals (shops etc.) and services that are distributed via internet and telephony to where the customer is located.

There are few suppliers of land-based infrastructure via copper or fibre-optic cabling: in practice, only Telenor, Ventelo, TeliaSonera and a few minor local operators. Most communications systems in Norway will be dependent at some level or other on the physical infrastructure functioning.

It is known as a result of incident reporting to Finanstilsynet that there are constantly incidents that cause communication link failure even though the communication was supposed to be protected with contingency systems. It often proves that a telecoms supplier that does not deliver the actual cabling himself purchases it from others, and that the topography is such that two different suppliers use the same physical cable.

It is difficult for financial institutions to avoid this, since for various reasons the suppliers of the physical network do not issue details of the topography. One solution for the financial institution may then be to ask the telecoms supplier to confirm that the delivery in question has redundancy[7].

When it comes to the financial institutions' communication with customers, a gradual transition is in progress from traditional landlines to wireless communication. The customer's unit is often a portable device linked via wireless communication to a landline network or directly via 3G mobile network. A gradual transition to IP communication through data networks like the internet is also under way. The developments are making it more complex and difficult for the individual end-user to maintain control of the communication level.

There are problems with respect to availability, confidentiality and integrity associated with use of today's telecoms systems. In 2011 there were a number of serious availability problems in communications in Norway, for example during the storms of December 2011. This, in conjunction with problems that arose in the ICT suppliers' backbone network, has made telecoms an area where more attention is required to ensure acceptable operational risk and availability.

[7] Redundancy is often built into systems that require high reliability. In IT systems, two or more computers may work in parallel with the same tasks and reflect one another, so that if one of them goes down the other can take over.

2.4 Developments in services offered by payment systems

2.4.1 Online banking on mobile devices

Secure use of banking services over the internet requires ensuring that the following fundamental security elements are present:

- Authentication: who am I?
- Authorisation: have I the right to do this?
- Authenticity: traceability, non-repudiation
- Confidentiality: no unauthorised person can read the information
- Integrity: no changes can be made unnoticed
- Availability: the certainty that communication between two or more parties is actually possible

Before mobile technology was generally available, online banking via a browser using PC technology (Windows or a Unix/Linux variant) or Mac was the most commonly used application. The technology has been known for many years, and weaknesses and vulnerabilities have been gradually weeded out. With upgraded operating systems, anti-virus protection and firewalls, as well as upgraded browsers, few or no losses due to security failure are seen in the actual online banking applications. This does not exempt users from taking their own precautions in connection with online banking. It is not advisable to perform sensitive transactions over open public wireless networks (WiFi hotspots).

The first step towards making banking services over the internet mobile was to make BankID available by mobile telephone. Here the user's private key is stored on the SIM card. Apart from this, online banking proceeds via a browser as before, provided that the internet bank offers log-on by mobile telephone.

SIM cards are issued by mobile operators. BankID for mobile devices is offered by a number of operators. With ever more sophisticated components, 3G and 4G technology, SIM cards with greater storage capacity and programmability and smart phones and tablet computers, which can also be mobile telephones, it is proving increasingly difficult to deliver a consistent product. What worked on one mobile telephone model will not necessarily work on another.

As a result of the development of mobile technology and market developments with increasingly sophisticated equipment, internet applications are moving from the traditional PC onto mobile equipment such as smart phones and internet tablets such as iPads. This equipment is delivered with special operating systems (OS) for controlling the many functions and programs on the equipment. Three operating systems currently dominate the market:

- iOS on Apple equipment (iPad, iPhone and iPod Touch)
- Android, a Linux-based OS owned by Google, for smart phones and tablets
- Windows Phone, a further development of Windows Mobile from Microsoft, for smart phones and tablets

There are also other operating systems on the market, but with smaller market shares:

- BlackBerry OS for BlackBerry smart phones
- Symbian OS – earlier extensively used on Nokia smart phones and others
- Palm OS for smart phones
- Bada OS from Samsung for their smart phones

Mobile equipment such as smart phones and tablets normally have one or more internet browsers available, but they often have a different structure from the corresponding browser for PCs. Browsers are often down-scaled versions of the PC versions. Opera has OperaMini and Opera mobile, Dolphin has been specially made for the mobile world, etc. Mobile equipment does not normally have antivirus software and firewalls of the kind known from the PC world. The security risks inherent in an individual browser or mobile unit do not appear to have been fully determined.

Whether or not a browser on mobile equipment can be used for internet banking depends on whether the combination of equipment and browser offers an operating environment with security that is accepted by the individual internet bank. Two-factor authentication (2FA) can be achieved either with one-time password (OTP) tokens or with mobile BankID, the latter being either a separate mobile from the device running the internet banking session or the same one. Many banks have their own internet applications for mobile equipment and browsers which are accessed by writing “m.bankname.no” or “mobile.bankname.no” in the browser’s URL field.

2.4.2 Mobile banking using apps

Developments in the very wide-ranging market for smart phones and tablets, with increasingly sophisticated possibilities and very wide market spread, have opened an entirely new market for software development. Small applications can be downloaded from the internet onto mobile equipment, either free of charge or at a very low price. The applications are known as “apps”, and can carry out a variety of tasks, from games and entertainment to business transactions, including banking services. Banks have clearly believed that they should be in this market, and have developed mobile banking apps for the various segments. iPhone, iPad, Android smart telephones and tablets and Windows Phone are upcoming competitors in the same market.

Some examples of mobile banking apps that are in the market today:

Figure 2: iPhone app from DnB

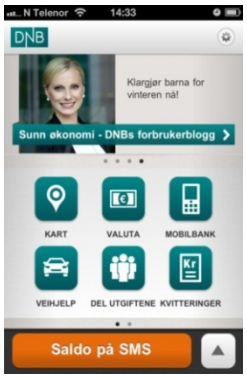


Figure 3: Android app from Nordea

Figure 4: Windows Phone 7 app from SpareBank 1

Figure 5: iPad app from Fokus Bank

Storebrand Bank and others have an interesting security token app supplied by Encap instead of the traditional security token (e.g. DigiPass from Vasco). The security token app is independent of telecoms supplier, but requires access to broad-band communication. The app is activated by a user-chosen PIN code in the same way as BankID on a mobile device.

As a result of the rapid developments in this area, there is no overview of the risk elements that may be present in the composite environment consisting of SIM technology, hardware, operating system, banking apps, other applications in the equipment, communication (WiFi or mobile) and user interaction.

The Norwegian Data Inspectorate points out that several hundred thousand apps are available from different “app shops”. The apps handle large quantities of personal data about users, often without the users being aware of it themselves. It seems obvious that if apps can be downloaded free of charge, there must be underlying factors that make this a profitable business. It seems very likely that the “tapped” information may be a tradable commodity. Whether this market is legal or not is an open question. The Data Inspectorate has placed emphasis on privacy protection and how the app handles personal data. The Inspectorate is concerned that the app supplier should publish information on how the app handles personal

data. The Data Inspectorate's report makes it clear that other aspects of the spread of apps than privacy protection should also be studied and subjected to risk analysis[8]. For the full report, see http://www.datatilsynet.no/Global/04_veiledere/app_rapport_DT2011.pdf.

BankID Norge is planning to issue its own app for BankID. The BankID app will enable customers to use BankID the way they are used to doing on a PC. The objective is to create an app that has the same functionality as BankID on a PC. The first app version will make it possible to log onto online banks and make transactions over the internet with mobile devices. Later it will also be possible to sign documents (published 3 February 2012 on BankID's website).

There is every possible reason for banks to keep these developments under observation and exercise their responsibility for security throughout the transaction chain when customers use online banking services via mobile devices.

2.4.3 Internet shadow services

2.4.3.1 Bitcoin

Bitcoin[9] is a digital currency established in 2009. The name of the currency also refers to the open source program Bitcoin that is used to transfer money. The maximum number of bitcoins that can be in circulation has been fixed at 21 million. This is thus a static currency once all bitcoins have been distributed. Bitcoin is based on person to person technology (P2P), and operates without any kind of central server or intermediaries. All payments are verified automatically through nodes in the P2P network, and the system is constructed such that it is not possible to create more money or to steal that of others. This is ensured by means of a block chain which is stored by all the nodes in the network.

Bitcoin can be compared to Monopoly money where each player buys virtual money called bitcoins to carry out commercial transactions in a closed trading environment. There always has to be liquidity in "real" money available if the players want to change from bitcoins to USD or EUR, for example. At present this activity is proceeding outside the control of the authorities and the risk is unknown.

The system is virtual and the US authorities have indicated that they want to stop it before naive users become too involved. In order for such a system to work, there has to be a "wealthy" sponsor.

2.4.3.2 Microloans/SMS loans

A number of enterprises now offer customers the option of taking micro- or sms loans. The amounts involved are often small, for example NOK 1000–3000. The loan period is 30 days as a rule, and there is no interest, but a fixed charge is applied. A loan of NOK 3000, for example, will entail a fixed charge of NOK 565 and the interest rate will then be 18.8 per cent per month.

[8] The Norwegian Data Inspectorate's report *Hva vet appen om deg* [What does the app know about you?], September 2011: http://www.datatilsynet.no/Global/04_veiledere/app_rapport_DT2011.pdf
[9] http://bitcoin.org/

2.4.3.3 Electronic or digital wallets

Electronic wallets are a form of electronic payment system that a number of countries are trying out. The purchaser transfers an amount from his or her bank account to an electronic card by means of a special terminal or his or her own computer. The purchase amount is transferred from the card to a separate "electronic balance" in the shop. The electronic balance does not have to be emptied with every transaction, but is aggregated over time and transfers amounts to the bank according to established routines.

The advantages of an electronic wallet over a bank card are that there is less loading on the banking systems, no traces linking customers to particular transactions (as with cash) and that it can be used in situations where the bank card system's identification process is not very practical (as with travel by public transport). On the other hand, stringent requirements must be made of both the card, which must contain its own processor and a more secure storage medium than the magnetic strip of bank cards, and of retail outlets, which must not be accessible to unauthorised persons and must not lose money in the event of a power outage.

2.5 Use of social media

The use of social media has increased sharply in recent years. Because of advantages like information sharing and effective interaction and communication, many financial institutions have started using social media, both internally and in their dialogue with customers.

When social media are used, the boundary between private and professional can be very indistinct. Incautious or unwise use may, for example, result in unauthorised persons securing information about both employees and the business by compiling data. The employee's use of social media in connection with work may involve a risk that makes it necessary for the employer to lay down guidelines and follow-up procedures.

2.6 Outsourcing

2.6.1 Offshoring

Economic and resource-related savings and the fact that that increases institutions' flexibility, are important reasons for enterprises outsourcing ICT services. High costs and/or a shortage of resources in Norway often lead to the purchase of ICT systems and services from outside Norway. This has resulted in price pressure on suppliers in Norway. It is important that the expectations of and from both parties are optimally clarified, so that the agreement reflects the customer's expectations of functionality, quality and security.

Outsourcing, particularly to suppliers outside Norway (offshoring) gives the flexibility to buy services as needed and to terminate the service when the need comes to an end.

Risk identification and management are important in outsourcing. Ensuring that the supplier has the resources and qualities necessary to ensure delivery according to agreement can be a challenge.

Other challenges are the regulatory and legal risk of moving ICT services to countries with which one is not thoroughly familiar. The service purchaser cannot assume that the service

supplier is aware of differences in rules and regulations etc. in the national legislations. It is the purchaser of the service who has to identify the different risks and in collaboration with the supplier to take steps to reduce risk to an acceptable level.

The legislation of many widely used offshore countries is far less stringent than it is in Norway. This applies, for example, in the sphere of privacy protection. Efforts should be made to compensate for inadequate legislation by including equivalent provisions in the agreement with the external supplier. At the same time, however, it is reported that the same countries have a limited ability to enforce the provisions of the agreement; for further information in this respect, see http://www.doingbusiness.org/rankings where India, for example, is rated number 182 of 183 when it comes to enforcement of the provisions of agreements. In some offshore countries there may also be a tradition of favourising customers who are willing to make settlement in untraditional manners. This may affect deliveries to customers who are not willing to do so.

2.6.2 Cloud computing

The expression “cloud computing” is often used about delivery of a service from the internet, such as systems for external data storage. Cloud computing has attracted a great deal of attention and is a variant of outsourcing services. From the available literature and surveys we see that the greatest risks for both suppliers and purchasers of cloud services are associated with security breaches and IT governance. With cloud computing, too, it is crucial to take account of the need for confidentiality, integrity and availability.

Suppliers of cloud computing services often have infrastructure that can compete with traditional outsourcing in both price and performance. But this same infrastructure may mean that data leave the home country of the customer, get lost, and that the purchaser of the cloud service has no control over where the data are or who has access to them.

Cloud computing in its present form is not adapted in such a way that it is particularly appropriate for financial institutions to use this service for systems that are of importance to the institution (customer and ledger data). In order for it to be possible to use cloud computing for important parts of the financial sector’s systems, a clarification must be made with respect to IT governance, transparency with respect to where the data are stored, who has access, overview and control of infrastructure, internal control, auditing and supervision.

Over the past 20 years, India’s IT industry has grown hugely. All the major IT companies have either established their own offices there or have entered into partnerships with Indian companies. Service suppliers in India are now also under pressure with respect to price and quality. New countries are competing for customers. For example, the cost level in some countries in Eastern Europe is now lower than in parts of India. There is also a trend whereby suppliers increasingly want to move further upstream in the value chain of their customers by taking over the operation and maintenance of their customers’ business processes.

2.7 Internet crime (cyber crime)

Norwegian online banks were increasingly under attack from various internet bank Trojans in 2011. As a result of counter-moves from banks, losses were minimal. The same trend is seen in other countries, but with varying loss figures. In 2010, banks in the Netherlands suffered

ten times higher losses due to Trojan attacks than in 2009, and the number of attacks doubled from 2010 to 2011. The Trojan attacks are becoming more automated as more logic is incorporated in the progams. Transactions can be generated without the use of an on-site surveillance and command centre. This development is alarming because it opens the way for mass generation of transactions on a hitherto unseen scale. Phishing[10] is a part of the concept. Phishing is constantly being used in new scenarios. The common denominator is that the party from whom the information has been extracted loses assets and/or may be suspected to be the guilty party in a fraud scenario when the stolen information is used as payment in various situations set up by the swindler.

E-mail is used to recruit "mules" who can make their account available as a beneficiary account for online banking attacks. The inquiry may be camouflaged as recruitment to a lucrative position in an international company. The person supplying the account information may do so in good faith, and may remain ignorant of the fact that the account is being used as a transit account for online banking fraud.

A number of variants on phishing are used to request credit card information via e-mail, where the sender claims to be your bank, your credit card company or similar. In an example from abroad, a swindler established a travel agency. Credit card data he head phished were used to buy expensive trips to exotic destinations. The "phisher" then swiftly re-sold the trips from his own travel agency, but now at campaign prices that are paid to the phisher through Western Union.

Another example is that phished credit card information is used to purchase advertising space in an online shop where fictional products are sold against advance payment. This is a type of ID theft where the rightful owner of the credit card is left standing as the guilty party when the product is not delivered.

Other countries in Europe have experienced fraud with SIM cards where mobile telephones are used for two-channel authentication for logging onto online banks. Weaknesses association with authentication requirements in connection with the ordering of new SIM cards are exploited. Swindlers order new SIM cards in the name of telephone owners. For a short period, both the old and the new SIM card function, and this is the time the swindlers need to attack the online bank. In the Netherlands mobile phone suppliers and banks now cooperate on exchange of information when mobile customers ask for a new SIM card.

In 2001 there was a massive DDOS[11] attack on Rabobank in the Netherlands. The intensity of the attack varied, and it lasted a total of more than 3 weeks.

2.8 Identity theft

Finanstilsynet uses the term 'identity theft' when someone has dishonestly obtained personal data that are abused in order to unrightfully secure financial advantage or other benefits without the knowledge of the rightful owner.

[10] Phishing is the term used for extracting information by means of inquiries of various sorts to individuals, e.g. requesting information in the name of another.
[11] In practice, Distributed Denial-of-Service Attacks involves sending digital inquiries to a website on a scale that causes the system to collapse.

Identity (ID) theft includes skimming of card data when cards are used in ATMs and EFT/POS retail terminals, hotels, restaurants etc.. Ccopying of information from card acquisition centres has so far has only happened on a large scale abroad. It also includes copying and misuse of information from another party's PC, particularly use of internet banks.

The problem area can be broken down into an acquisition phase, where personal data are acquired in a purposeful way, and an attack phase, where the elements of information that have been gathered are compiled for use in a targeted attack.

In Norway, data from ID theft are also known to have been used as elements in larger attacks, where both unfaithful servants and use of data from ID theft are involved in crimes that have resulted in major losses.

International sources report that ID theft is a growing problem. The English-speaking part of the world appears to be particularly under attack at present. In the USA, ID theft is already a significant and growing financial problem for society at large.

ID theft as a type of crime has also reached Norway, and it is a serious problem for those who are subjected to it. There are few formal statistics on the subject, but there is reason to believe that the problem is growing, and that it puts substantial strain on the victim.

It is important for the financial sector and the authorities to monitor developments carefully and to endeavour to find effective counter-measures before ID theft becomes too wide-spread and has negative effects on the areas indicated above. In the financial sector there is already important work in progress in this area, both through industry organisations and in individual institutions. Finanstilsynet also collaborates closely with the Norwegian Data Inspectorate and other relevant authorities.

2.9 Internal fraud

Internal fraud may be a result of unfaithful servants and weak control systems. The information Finanstilsynet possesses about internal fraud in financial institutions both in Norway and abroad indicates that this is a growing problem. The inspectorate assumes that there is underreporting of fraud of this kind, particularly when limited losses are involved. However, it looks as though cases that entail major losses are reported to the police and to Finanstilsynet.

The general globalisation and greater labour mobility may be one reason that it is difficult to know one's employees sufficiently well. It is also likely that criminal groups are aware of persons from their environment who are employed in financial institutions and are able in various ways to apply pressure to the employee to engage in criminal acts. There is reason to believe that there are periods when there is activity to get persons employed who are later intended to engage in criminal acts.

It is cause for particular concern when an employee (unfaithful servant) in a financial institution takes part in an internationally organised digital attack on payment services, for example in the area of online banking, which can cause major losses.

It is important for the financial sector to focus on this problem going forward. This applies particularly to banks. Sound employment procedures and effective control of access rights are important areas where steps can be taken to limit this problem, which appears to be growing.

2.10 The area of securities

2.10.1 Common settlement rules in the EEA area

Work is in progress in the EU on a pan- European settlement system called TARGET 2 Securities (T2S). The work is being directed by the European Central Bank (ECB), and its aim is to centralise clearing and settlement of securities transactions in order to bring about a larger common platform and a greater opportunity for achieving higher efficiency, lower transaction costs and higher security. TS2 is intended to cover securities transactions in all currencies within the EEA. It has not been decided when or if Norway will become linked to T2S.

There are also change processes under way that are largely market-driven, involving the establishment of new marketplaces and technology-based solutions in trading and in investors' connection with the market.

The sum of the various processes within the EU in the area of finance requires changes and adaptations that may give rise to risk that it is important that the financial sector is capable of handling. What this will mean for the role as securities register of Verdipapirsentralen ASA (the Norwegian Central Securities Depository – VPS) has not been established.

2.10.2 Robot trading

Market players can achieve major returns with the aid of programmed algorithms which make transactions automatically on the basis of particular market signals and form the basis for high frequency trading (HFT). Computerised share trading constitutes a growing proportion of trading on stock markets worldwide. In Sweden, HFT accounts for about 10-20 per cent of turnover on the stock exchange, and on the US stock exchanges it accounts for about 60 per cent of trading.

Many are of the view that HFT supplies liquidity to the market, reduces personnel costs and increases competition between stock exchanges. Others point to the risk of HFT driving the market instead of following it, and that HFT creates "noise" for investors who want to invest on the basis of companies' net asset value, which may reduce liquidity.

To enable them to exploit a market opportunity as fast as possible, it is important that the computers that operate HFT are located close to the stock exchange. They should preferably be co-located with the stock exchange. Only the biggest players can afford this. An important group of smaller players may therefore be squeezed out of the market.

It has been claimed that HFT may make the market unstable, for a number of reasons. Algorithms tend to be fairly similar, so they reinforce each another. Many of them will sell or buy the same share at the same time, and this may create large, unpredictable fluctuations. Incorrectly programmed computers may also trigger other computers to sell and buy shares, which may increase the risk of major fluctuations. The explanation given for the "flash crash" in New York on 6 May 2010, when the Dow Jones index fell 9 per cent in 10 minutes, was

that a computer program over-reacted to a market signal. Another example is the systems of a Swiss HFT company, listed on the Stockholm Stock Exchange, that automatically placed a large sell order and updated the price limit many times in order to match buy orders, thereby driving the price down to an unusually low level.

European stock exchanges have taken a joint decision to co-ordinate the minimum price differential between two levels (tick size) in an order book on the European markets with the specific aim of increasing trading liquidity and minimising transaction costs. This has made it cheaper to go in and out of a position and more attractive for HFT traders, because price differentials between marketplaces now arise more easily, and at the same time it is cheaper to buy and sell.

HFT is a relatively new phenomenon, and is constantly changing and developing. The risks and consequences associated with HFT have not been fully analysed. Finanstilsynet will monitor developments.

3 Payment service systems

3.1 General information on payment systems

Payment systems are central to all economic activity. All trading in commercial or financial products culminates in an agreed monetary settlement. In Norway, payment systems are governed by laws and regulations and through the financial industry's self-regulatory system which is 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 interbank systems (transactions between banks) and payment service transactions between customers (retail or corporate) and banks. New technology has strongly influenced systems for payment services in recent years. Cost-effective operations, user-friendliness and security have been key elements.

In 2011, Norwegian payment systems mediated some 2 billion transactions (credit transfer and card). Over 95 per cent of the payments take place electronically in a seamless digital transaction chain between two interacting parties. Only 1.1 per cent of payments take place by way of paper-based forms.

Retail customers' use of internet banks accounts for 59 per cent of all payment transactions. This amounts to 13.4 per cent of the volumes in billions of kroner that are transferred. Corporate customers' use accounts for 41 per cent of all transactions, which is equivalent to 86 per cent of the value (amount).

BankAxept has 87 per cent of the value of retail market card payments. Norway is a world leader in the use of payment cards.

A large proportion of the electronic infrastructure that the payment systems use for operations is outsourced to ICT suppliers. The liability of enterprises that are subject to licensing is not affected by the outsourcing. It is important to ensure that all elements and players in the entire transaction chain between payer and beneficiary are included in the management of operational risk. It is important to ensure the necessary expertise and time to be able to fully govern the operating situation of both own operational resources and IT suppliers with vendors, if any. Finanstilsynet took up this problem in Circular 20/2011 (Norwegian text).

The framework conditions for payment systems in Norway are affected by intra-EEA harmonisation. The Payment Services Directive has been fully implemented in Norwegian legislation. Under the new rules, all types of institutions that wish to offer national or international payment services are subject to authorisation. The implementation of the Payment Services Directive in Norwegian law has opened the way for the establishment of payment institutions.

Norges Bank's "Annual Report on Payment Systems 2011" contains supplementary comments and statistical data on this area.

3.2 Risk and vulnerability in payment systems

Transaction chains are expanding and their complexity is increasing with new electronic services, new interfaces and more sub-contractors, increasing the risk of error.

Serious incidents in payment systems are reported through Finanstilsynet's incident reporting system. A more detailed account is given in section 4.3.

Retail and corporate customers now use several different channels in relation to banks in order to make payments. Having several payment channels reduces the risk that bank customers will be unable to effectuate their payments. If one channel is inoperative, it will often be possible to use another.

In Norway, the number of operators of core systems for banks and financial institutions is small. This may represent a not insignificant concentration risk, but may also contribute to better governance.

Established contingency solutions for payment systems are important for preventing undesired incidents. Robust solutions to avoid problems such as technical errors of the single point of failure type, regular reviews of continuity requirements and testing of contingency solutions are key elements of preventive work.

The Norwegian Banks' Standardisation Office decides on and lays down Norwegian reporting standards and mandatory security requirements that must be applied in payment services. Furthermore, most of the payment card companies in the market comply with the international Payment Card Industry Data Security Standard (PCI DSS) which sets requirements for merchants, among other things. Under the standard, an evaluation and assessment of compliance with these requirements must be carried out at least once a year.

At present, the risk of criminal attack is greatest at the interfaces between customer and bank. This applies to both payment card fraud and attacks on online banks.

3.3 IT Governance of payment systems

Systems for mediation of and making payments constitute a substantial part of the critical infrastructure and functions of society.

Governance of the ICT activities related to payment services must therefore be given high priority. The commercial operations must have a sense of ownership and involvement with respect to functionality, changes, problems and risks. Requirements must be set with regard to structure, order, quality, and to ensuring that work is carried out in accordance with approved standards and methods. In Finanstilsynet's experience, many financial institutions carry out risk assessments once a year, usually in connection with their reporting on internal control. Large parts of the ICT activities related to payment systems in Norway are outsourced, and a great deal is outsourced to the same suppliers. As mentioned earlier, this represents a risk related to concentration among suppliers of both ICT operations and application development. It is important that the individual financial institutions cooperate on measures to ensure that the concentration risk is acceptable and assessed in risk analyses.

Imposing requirements on a major IT supplier that in reality has few competitors can be a challenge. When outsourcing services, institutions must ensure that they are adequately qualified to administer such agreements and to set requirements in connection with outsourcing. Establishing requirements for and following up on suppliers located outside Norway is particularly difficult.

In some inspections, Finanstilsynet has noted inadequate qualifications among governing bodies and the executive management of financial institutions. This applies both to IT generally and to outsourcing in particular. This may make it difficult to obtain an overview of all the elements in the transaction chain.

Governance of the payment systems is a crucial part of the overall governance of the institutions' ICT activities.

3.3.1 Risk associated with shared systems

In addition to the requirements following from legislation, banks in particular conduct an agreed form of self-regulation. This self-regulation primarily affects the transaction bank, and covers jointly developed services and systems that are used by the entire banking sector to provide an effective transaction chain. This constitutes an essential part of the financial infrastructure, which in recent years has become more complex.

The self-regulation is documented in the "Blue book" and is administered by Finance Norway. The regulations are available on FNO's website:

http://www.fnh.no/no/Hoved/Avtaler-og-regelverk/Bank-og-betalingsformidling/Betalingssystemer-og-felles-bankinfrastruktur-/

In 2011, Finance Norway and Finanstilsynet jointly developed a more fundamental understanding of what the operational risk picture looks like, and who has the primary operational responsibility. Finance Norway has accordingly updated relevant documentation.

3.4 Overview of losses related to payment services

The tables show losses for the last three half years. The figures have been obtained from Finance Norway and the Norwegian Banks' Standardisation Office in collaboration with Finanstilsynet.

It is first and foremost payment cards that account for major losses. The various loss categories are annotated below.

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

Type of payment card fraud	2010 2nd half year	2011 1st half year	2011 2nd half year
Misuse of card information, card not present (CNP) (Internet transaction)	9,401	9,358	14,832
Stolen card information (including skimming), misused with counterfeit cards in Norway	1,765	97	371
Stolen card information (including skimming), misused with counterfeit cards outside Norway	31,740	24,890	32,450
Original cards lost or stolen, misused with PIN in Norway	14,395	15,913	16,311
Original cards lost or stolen, misused with PIN outside Norway	5,149	2,135	4,873
Original cards lost or stolen, misused without PIN	4,239	2,254	2,234
TOTAL	**66,689**	**54,647**	**71,071**

Losses in the category *'Misuse of card information, card not present (internet transaction)'* are largely associated with hacking, but phishing is also one source of these losses.

The category *'Stolen card information (including skimming), misused with counterfeit cards in Norway'* was strongly reduced in 2011 compared with 2010. There were several skimming cases involving Norwegian ATMs in the summer and autumn of 2010. There was nothing similar in 2011. Norwegian payment cards are skimmed abroad, and information in the magnetic strip is copied and used to produce counterfeit cards. Skimming of Norwegian payment cards abroad usually also involves reading of the PIN code, and the counterfeit cards are used with the PIN. Counterfeit cards can also be used without PINs for some payment services that do not require a PIN.

Counterfeit cards made on the basis of skimming both in Norway and abroad were almost exclusively used abroad in 2011. POS terminals and ATMs in Norway require chips on Norwegian debit cards and this excludes the use of counterfeit Norwegian payment cards with only a magnetic strip.

The main cause of the category *'Original card lost or stolen, misused with PIN in Norway'* is pickpocketing and 'shoulder surfing'. Somebody watches and reads the PIN code the user keys into the payment terminal or ATM and then steals the card, or the reverse: someone steals the card and compels the victim to reveal the PIN code. In addition, some cards and PIN codes still sometimes get lost in the post.

Table 2: Losses related to use of online banking (figures in thousands of NOK)

Type of online banking fraud	2010 2nd half year	2011 1st half year	2011 2nd half year
Attacks using malware on customer's PC (Trojans)	0	658	6
Attacks that exploit vulnerabilities in online banking applications (hacking)	0	0	0
Lost/stolen security device	2,398	602	2,719
TOTAL	**2,398**	**1,260**	**2,725**

Despite massive Trojan attacks on Norwegian online banks in 2011, losses were small. However the costs associated with measures increased substantially. A major amount was lost as a result of passwords and one-time security tokens being stolen. In the second half of 2011 in particular there were major fraud cases that were reflected in this loss area.

4 Findings and observations

4.1 Some findings from IT inspections in 2011

4.1.1 IT suppliers with inadequate delivery capability

A number of institutions where Finanstilsynet has carried out IT inspections have indicated that they are not satisfied with the supplier's ability to deliver application development and management. Often the same supplier operates the systems and manages many of the applications. The institutions are frustrated over the failure of their desire for new functionality to be heard. Repeated delays and the absence of contributions to analyses and creativity on the part of the supplier frustrate the institutions' desire for innovation and new product development. After a while, many institutions look around for other business partners.

4.1.2 Inadequate control of whole transaction chains in which many operators are involved

Most financial institutions have outsourced operation of IT systems, and many have also outsourced application development and management. Finanstilsynet's inspections have revealed that having more operating models has made it more difficult for institutions to ensure control of the transaction chain. Payment card transactions and internet bank transactions pass through the Norwegian payment infrastructure, which is operated by a number of different suppliers. In order to compete with other operators and reduce costs, the primary IT suppliers choose to outsource some of their tasks to vendors.

4.1.3 Inadequate governance of the overall risk picture

Collating the results of risk analyses that have been carried out proves to be a challenge. This applies in particular in large institutions where risk analyses are carried out in different business areas and levels of the organisation. The risk analyses appear to be fragments that are not connected together and do not reflect one another. In large organisations there is often both a bottom-up and a top-down approach to risk analysis. The results of the two are not always compared.

As a general rule, it appears that institutions should allocate more time and resources to performing risk assessments. Preparing reliable risk assessments requires expertise and experience. There are many guidelines, but no template for how it should be done in the individual case, or at what level, or how risk and the measures implemented should be documented and followed up.

It is important to perform risk assessments in advance of major IT changes. It is also important that the risk assessment indicates who is responsible for measures to reduce risk.

Many institutions have not established procedures for checking that IT processes and routines are complied with. Good internal control is not achieved merely by having sound and documented procedures; it must also be ensured that they are complied with.

Finanstilsynet has also noted that some institutions that have outsourced their IT activities do not have an adequate overview of the supplier's risk management and internal control. This

may be attributable to inadequate agreements, or that the institution does not have sufficient staff to stipulate requirements, order and follow up the IT supplier. This may be a particular challenge for small institutions, which purchase a substantial part of their ICT activities and do not have sufficient internal staffing.

4.1.4 Demanding risk analyses when IT is outsourced to low-cost countries

Outsourcing to low-cost countries introduces new problems and risks that may be difficult to assess. The countries and regions in question may be remote, with unknown culture, language and legislation. Financial institutions often base themselves on risk analyses conducted by major IT operators such as Gartner, Accenture and Capgemini, which have established themselves in the countries in question, and on ratings, for example of country risk. The results of surveys conducted by Transparency International or Gartner are published as an index of the perceived degree of corruption in the countries. It is important to analyse in detail what a high corruption level can mean in terms of risk and what measures may be relevant to handle this risk prudently. Some enterprises conduct their own country analyses. One relevant problem is ensuring that the rules and regulations in the country where the tasks are performed are not an obstacle to compliance with the Norwegian rules and regulations, and that the risk is acceptable.

In Circular 14/2010, Finanstilsynet issued guidelines for outsourcing of banks' IT tasks to low-cost countries. As a general rule, there is high risk associated with outsourcing tasks linked to the operation of payment services and core systems. In Finanstilsynet's view, it is a requirement that financial institutions do not base themselves exclusively on risk analyses performed by the operators in question, but carry out their own analyses.

4.1.5 Failure to test that contingency systems function

IT inspections conducted in 2011 also revealed inadequate testing and verification that continuity and disaster recovery plans function according to intention. There are still many operators who, owing to a failure to test and verify, have not ensured that their disaster recovery plan will function in the event of disrupted operations. Some financial institutions appear to place more emphasis on testing business continuity plans than on disaster recovery plans.

Continuity is often tested by means of duplicate systems that switch periodically between being the primary and the secondary production location. The challenge is to test all levels of the transaction chain. In the outermost levels we still see that contingency systems, for example on the network side, do not function according to intention in the event of disruptions. Tests of continuity also include testing the network.

Disaster recovery plans are complex to test. Here, too, all levels of the transaction chain have to be taken into account. The institutions' documentation from disaster recovery tests that have been carried out show how important these tests are. Finanstilsynet regards tests as crucial for ensuring that the disaster recovery plan is the real alternative it is intended to be in a crisis situation.

4.2 The institutions' own assessments

In order to gain insight into the financial institutions' own assessments of their ICT risk, Finanstilsynet has conducted dialogues with fourteen financial institutions of various types and sizes. The dialogues concerned problems and challenges experienced in 2011, and the risks that are regarded as being the most serious in 2012, and will therefore be in focus.

The greatest problems/challenges in 2011:

- The card services incident in Easter 2011 is regarded by most banks as the most serious problem in 2011. In the wake of the incident, measures have been implemented to reduce the probability of such an incident occurring again and having such extensive repercussions. Agreements, interfaces and procedures are reported to have been reviewed and improved, and a study of critical components is planned.
- A number of institutions point to inadequate operating stability as a risk as well as a problem they experienced in 2011. Much of the responsibility for this is attributed to the operations service providers.
- Inadequate delivery quality from suppliers, both in projects and in connection with daily operations.
- Attack on internet banks and associated services. Few other types of institutions appear to have experienced serious cybercrime.
- Stability and availability in the wake of major changes has been found to be a problem in some institutions.

Risk areas in 2012

- Operating quality and stability of systems and infrastructure
- Confidentiality and integrity of customer data
- Internet crime
- Concentration risk in shared functions, such as the Norwegian Interbank Clearing System (NICS) and BankID
- Quality of institutions' own deliveries and systems
- Quality of suppliers' services and deliveries, and overview and control of suppliers' risk and internal control
- Requirements with respect to cost-effective solutions, time-to-market, and the consequences these may have for IT work and systems
- New services and devices (mobile telephone services, internet tablets etc.)
- Employees' use of social media
- The risk of intentional or unintentional misuse of data in connection with increased use of consultants who are given access rights to enable them to do their work

Problems that are in focus in 2012

- Measures against cybercrime, including monitoring of internet-based services
- Security surrounding self-service channels, including mobile devices
- Improved processes and procedures, including change management, quality assurance, project management, portfolio management and implementation
- Conduct evaluations of suppliers and sourcing options
- Improve risk analyses

4.3 Incidents reported in 2011

There were a number of serious incidents in 2011. In February Norwegian internet banks were hit by a coordinated malicious attack involving a Trojan code. During Easter the card authorisation service of many banks failed, with the result that many card customers had problems paying for goods in shops, and the incident also had negative after-effects for the perceived amount available in accounts. These two incidents are described in detail in sections 4.4.1 and 4.4.2.

In July there was an interruption in the BankID service. It lasted for 6 hours, and paralysed most logging onto Norwegian online banks and other services where BankID is used for authentication. Banks with an alternative authentication mechanism available in their online banking gateway were least affected.

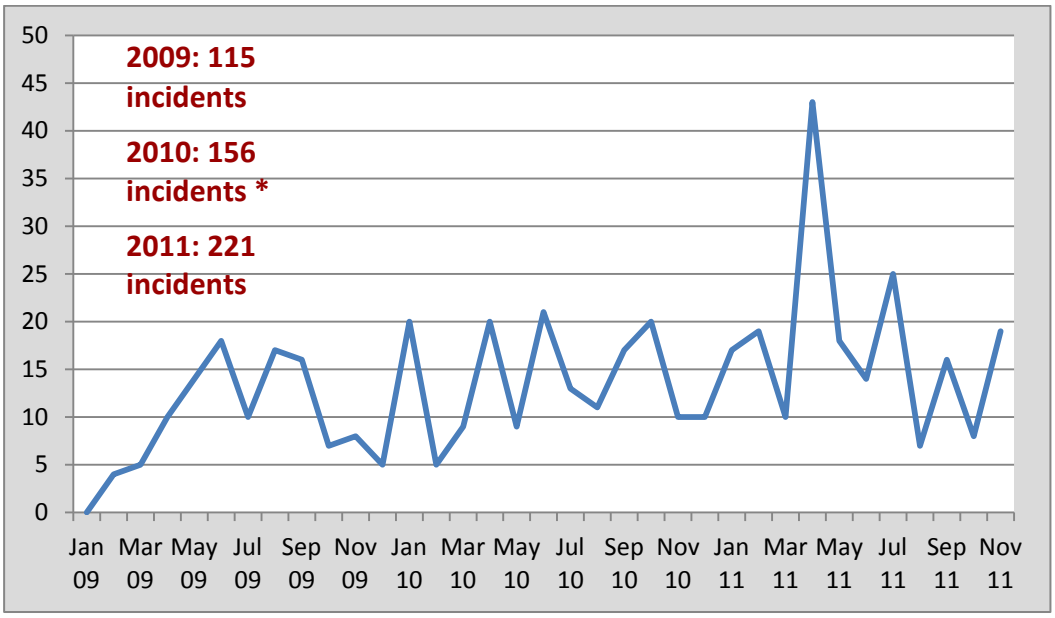
The terrorist action on 22 July had little impact on the financial sector. Some bank premises and pension funds in central Oslo suffered material damage.

In September the Oslo Stock Exchange had to suspend trading for over three hours because of a system outage experienced by the exchange's supplier, London Stock Exchange.

The availability downtime of Norwegian online banks appears to be at about the same level as in previous years. Finanstilsynet notes that the online banks are most affected by outages and failures are different from year to year which. The reason for this may be the degree of attention from a common supplier, or aging platforms that require an increasing amount of work to keep up to date. Upgrading of firewalls and contingency systems are repeat offenders as causes of failure. Banks experience the paradoxical effect that it is precisely in their work to ensure continuity in online banking that causes interruptions in the availability of the internet bank.

Finanstilsynet has received more reports of undesirable incidents in 2011than previously, largely because of incidents that affected many financial institutions simultaneously. Incident reporting is a well-established arrangement. Banks and their suppliers are quick to report after an incident has occurred. Other types of financial institution report to a lesser extent.

Figure 6: Incidents in the period 2009 to 2011



Incidents reported in the period January 2009 to December 2011

* Skimming of ATMs is counted as 1 incident.

Figure 7: Incidents in 2011, by month

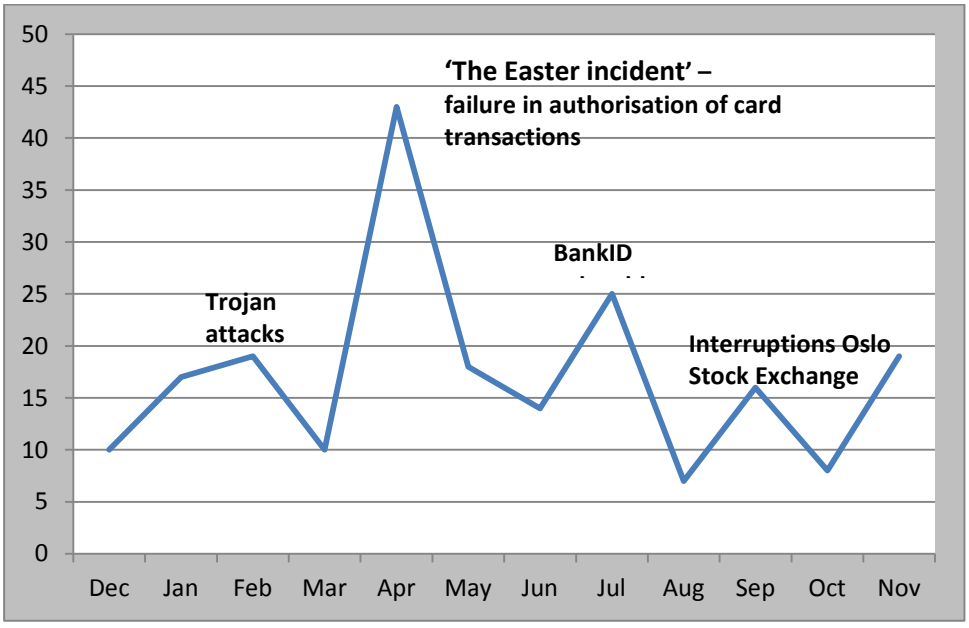
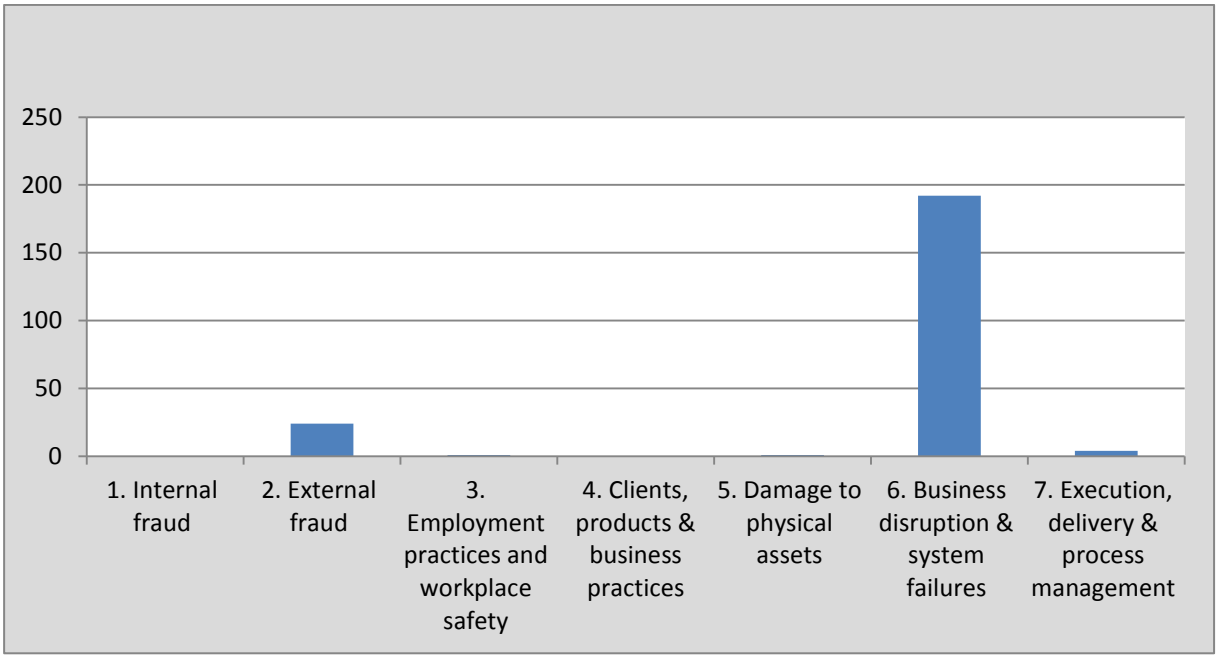


Figure 8: Incidents reported in 2011 distributed among Basel II's seven loss event categories



4.3.1 Trojan attacks

Norwegian internet banks were subjected to malware raids throughout 2011, particularly the Trojans SpyEye and Zeus. The attacks peaked in intensity in February, when the URLs (internet addresses) of most Norwegian online banks were reproduced in malware intended to be disseminated to Norwegian banking customers' PCs. Customers' PCs were infected with malware from notices or downloads from a website or an e-mail. PCs with poorly updated security (anti-virus protection, spam filters, firewalls etc.) are most vulnerable. The malware lies in wait for the customer to log onto the online bank (key in the online bank's URL). The customer is then presented with a false website (phishing) which overlies the ordinary site and is almost identical to the bank's website, with the bank's logo etc. The language is improving steadily, but in the attacks in 2011 there were still perceptible spelling errors. The log-on codes the customer enters are picked up by a command centre with real-time monitoring of infected PCs and used to make false transactions. Because of the collaboration between the banks on exchange of information about infected PCs and false beneficiaries, almost all transactions were stopped before they were executed. The losses were low; see table in section 3.5. Most transactions were transfers to other countries. Small banks suffered the highest losses because they were not as quick to be included in the established cooperation between the banks, BSK and NorCert[12]. This has now changed.

4.3.2 "The Easter incident" 2011

On the Wednesday before Easter, one of the busiest shopping days of the year, problems in using payment cards developed. Customers found that card payments in payment terminals and withdrawals from ATMs were interrupted or proceeded extremely slowly. The problems concerned both BankAxept transactions and transactions with international cards. Of a total of

[12] NorCERT department in NSM where Nor indicates Norway. CERT: Computer Emergency Response Team.

4.3 million payments with cards, 1.4 million remained in STIP [13] with over 4 seconds of waiting time for a response from the terminal and about 200 000 transactions were rejected. Customers with cards issued by banks that use the authorisation system of EDB ErgoGroup ASA (EEG) were hardest hit. The cause of the problem was a hardware defect on EEG's primary server for authorising receipt of cards. The contingency system proved not to be upgraded with the same capacity as the primary system. The primary server was updated in autumn 2010 to enable it to handle the volume of transactions in the Christmas traffic. As a result of an error the secondary server was not upgraded similarly.

The operating error proved to have serious consequential errors. Because of the slowness of the processing, many customers made several attempts to use their card. This resulted in duplicated reservations on customers' accounts, and in some cases transactions were carried out several times because they were keyed in more than once at the user site.

The last general ledger run of capital transactions before Easter took place on Wednesday afternoon. Because of the failure of EDB's authorisation system, reservations were sent from Nets from Wednesday 20 April after the capital update had been run. This continued until Friday morning. Thus the transactions were entered in the wrong order and were not cancelled out as they normally are. The right amounts were charged to the accounts concerned, but at the same time the disposable balance was reduced by the same amount, i.e. they were charged twice. The disposable balance shown for many customers was then too low, and for some it was even shown as being empty.

There were no banking days in Easter, and a number of accounts were therefore not rectified before the banks ran a general ledger update (settlement) on the first business day after Easter.

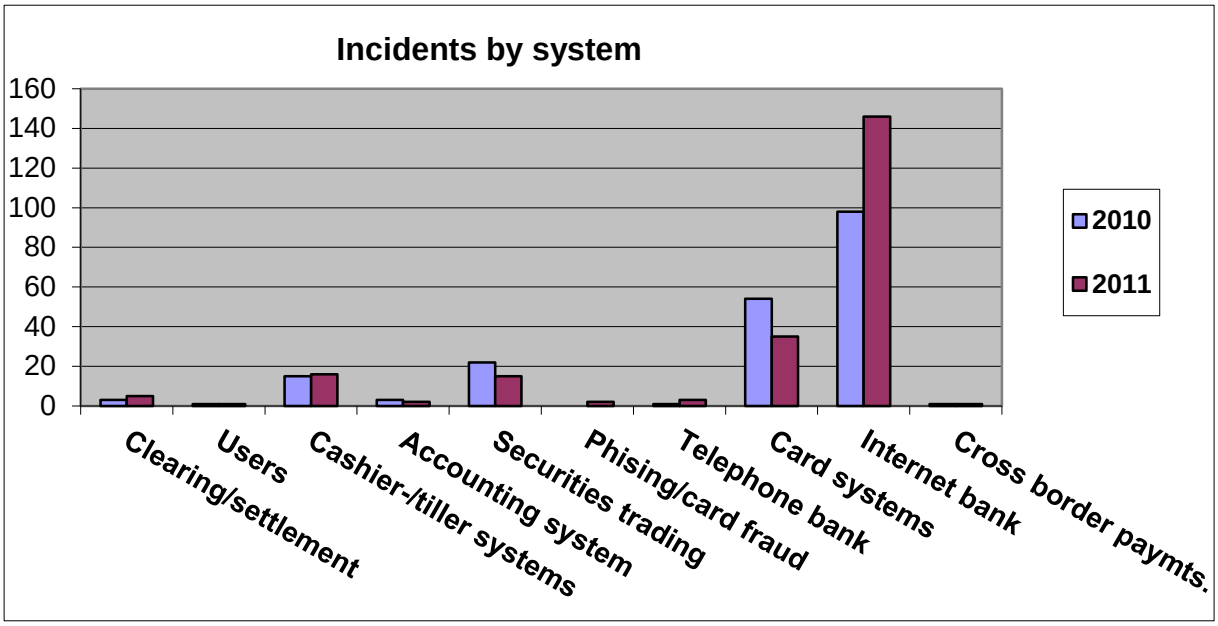
On Sunday 24 April EDB ran a deletion of reservations and removed the majority of the reservations. The remainder were removed in subsequent runs up to and including Tuesday 26 April.

[13] STIP: Stand In Processing – forms part of an agreed scheme without account balance checking.

4.3.3 Analysis of incidents

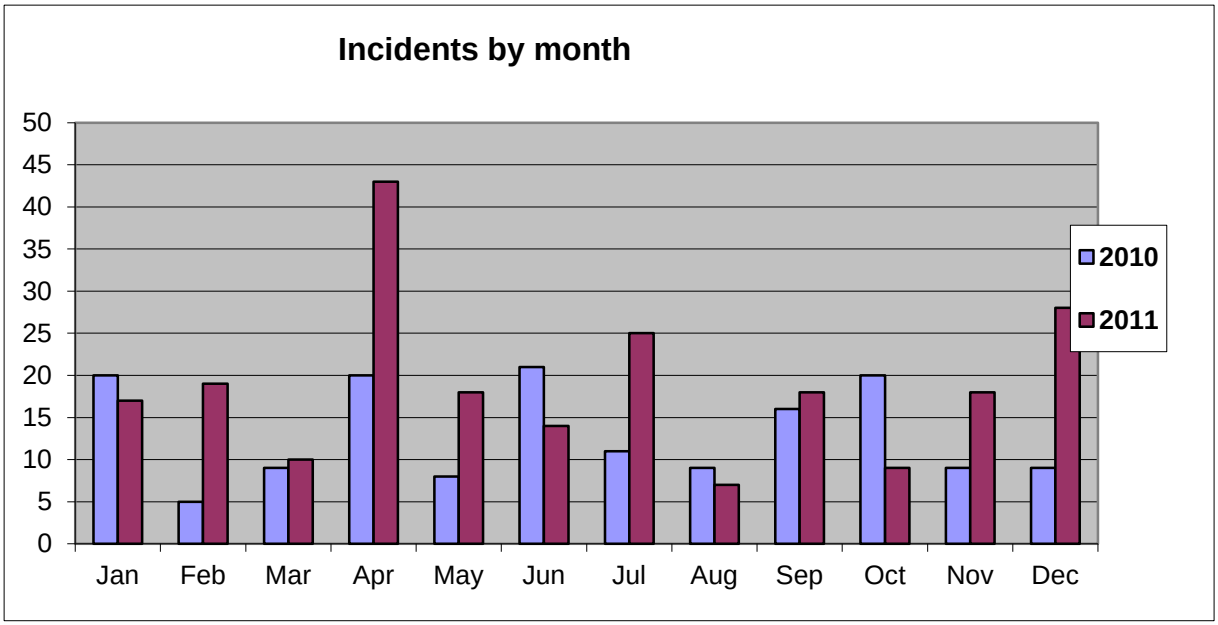
The graphs below show developments from 2010 to 2011.

Figure 9: Incidents by system/product



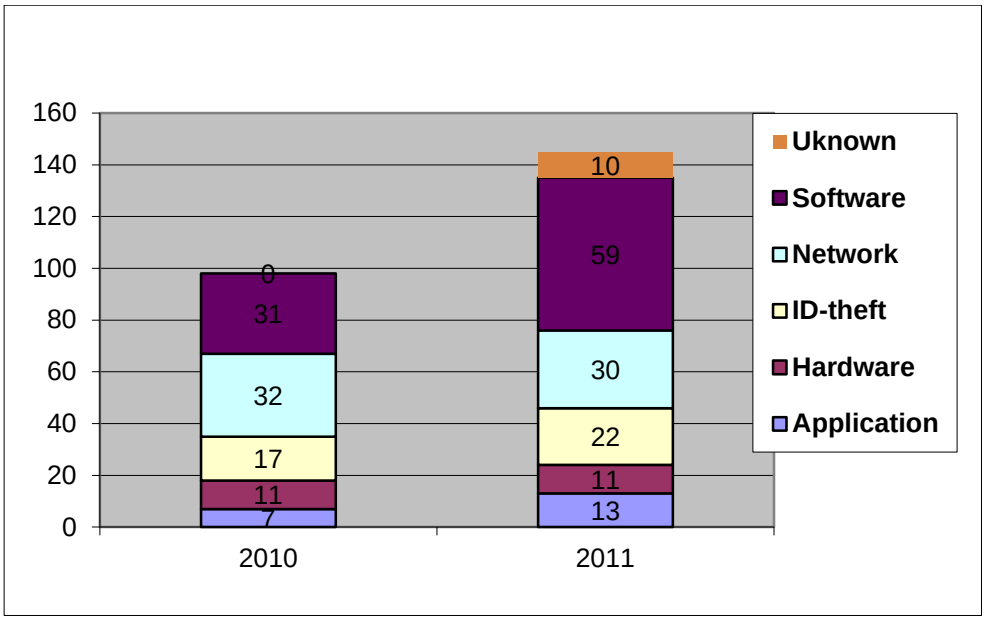
There have been no dramatically negative developments. Internet banking distinguishes itself by an increase in reported incidents of about 40 per cent.

Figure 10: Incidents by month in 2011



The increase in April is due to the “Easter incident”; see section 4.3.2.

Figure 11: Incidents in online banks – numbers distributed by cause



The above graph shows where the cause of the incident lies for online banks. It must be interpreted as meaning that it is not necessarily a fault in software (SW), a network, hardware (HW), etc. that has caused the incident. In the case of software, the reason for the fault is often that the software itself functions the way it is supposed to, but has been put into operation sub-optimally, and consequently the online banking service does not function as intended. For instance, parameters may have been set incorrectly, or are no longer compatible with the operating environment or have not been adapted to the traffic, etc.

The basis for the breakdown in the graph above is:

Software (SW) is all auxiliary software that constitutes the operating environment of the internet banking application. This may be application servers, web servers, database servers, CICS, software for monitoring the internet bank, certificates, queue systems (MQ or others) and other standard off-the-shelf systems delivered by third parties.

Networks cover routers, switches, domain name systems, gateways, network address translation, intrusion prevention system/intrusion detection system, lines, firewalls etc.

ID theft consists first and foremost of phishing and Trojans. There have also been incidents where a customer has gained access to another customer's account and there have been errors in the authentication functions. These are included here.

Hardware (HW) is the machinery the internet banking applications run on and errors may consist of microcode errors, overloading, incorrect parameter setting, sudden and inexplicable disruptions.

Application the incidents here are associated with defects or weaknesses in the actual internet bank application, i.e. the part of the code developed by the bank.

The figure shows that software is still the predominant cause of incidents. It still appears to be difficult to maintain a stable operating environment for online banking applications.

There were 16 serious or critical incidents associated with firewalls in 2011. Finanstilsynet notes that maintaining an overview of the consequences of changes associated with firewall rules and updating of firewall configurations present substantial challenges.

It is worth noting that errors that are innocent in themselves may lead to consequential errors that may have very serious consequences. This is illustrated by an incident associated with a memory leakage which led to online banking, mobile banking, telephone banking, SMS banking, online loan systems, online systems for entering into agreements, card systems, POS systems, online business systems and banks' internal sales and customer follow-up systems and credit processing systems going down.

4.4 Risk areas identified from other sources

4.4.1 Cloud computing

Sony has placed a large amount of the client base for its PlayStation Network in a cloud computing system. There is said to be data on about 100 million customers who play online games on Sony's gaming network. The data that is stored externally contains extensive personal details such as name, address, gender and date of birth, as well as log-on information, albeit encrypted. There is also information about payments and card data on some of the customers. Sony's system was compromised and had to close down for several days in 2011. It looks as though whoever hacked into Sony's bases has used the strength of cloud computing, which provides the computing power and storage capacity necessary for the task.

The Sony example illustrates the risks of cloud computing.

4.4.2 The attack on RSA and results thereof

Data security circles reacted with astonishment and alarm when it turned out that RSA, a company in the EMC group, had been subjected to an advanced persistent threat (APT) attack in March 2011, and that information concerning RSA SecurID had been stolen. This information was then used in an attempt to attack Lockheed Martin, a major US manufacturer of defence material. RSA has since admitted that the stolen data could make a large number of SecurID one-time code generating tokens worthless, and they have offered to replace the tokens of customers who use them for business purposes.

The data breach itself was performed as a three-stage operation: The attack started when an employee was tricked into opening an infected spreadsheet from an e-mail purporting to contain recruitment plans for the year. The infected spreadsheet then used a hitherto unidentified flaw (zero-day flaw) in Adobe Flash to install a remote control device. More PCs were then infected in order to reach PCs that had access to the sensitive information. The data were acquired, compressed and exported to an external machine that had also been taken over, and then sent to the party committing the breach.

APT attacks of this kind, which use a combination of apparently simple fraud and high-tech exploitation of zero-day flaws in software, are very difficult to detect and stop since anti-virus programs do not recognise attacks of this kind.

RSA SecurID is used as a one-time password generator in two-factor authentication (2FA) for online access to banking services. It is therefore critical if the system is infiltrated.

5 Identified areas of risk

5.1 Outsourcing risk

Individual institutions are responsible for their own ICT activities. This also applies when all or some ICT activities are outsourced. Incidents in 2011 have revealed that some institutions do not have a full picture of the transaction chain, for example in the area of payment systems.

A prerequisite for having a full overview is that agreements are established with all relevant operators, and that the agreements are harmonised to enable delivery of the desired result.

The costs of outsourcing ICT services receive a great deal of attention. It is important that the agreements take account of the interests of both customer and supplier, to ensure that any savings are not at the expense of the security and quality of the ICT deliveries.

Finanstilsynet regards cloud computing as being equivalent to outsourcing of services and therefore treats it in the same manner. Institutions shall, on their own or through formalised cooperation with other enterprises, ensure control of their own data and have sufficient knowledge of the ICT infrastructure to ensure that all the requirements of the Norwegian ICT Regulations are met.

The agreement must ensure that institutions are also given the right to inspect under supervision those of the supplier's activities that relate to the agreement, and that Finanstilsynet is given access to data from and the right to inspect the ICT supplier.

5.2 Inadequacies in governance

Finanstilsynet points to three factors that are crucial to governance of ICT activities, and which do not generally appear to be taken sufficiently into account.

Framework conditions, in which processes, routines, procedures, instruments, clarification of roles and responsibilities etc. are documented, are necessary to enable institutions to work rationally and efficiently within the framework, in compliance with the requirements and towards the objectives that have been set for the institution. It is a prerequisite that the processes, procedures etc. have been thoroughly reviewed. Finanstilsynet has found that institutions do not always have such a framework in place, and that the framework is not always anchored and known in the organisation. It is also necessary for institutions to establish procedures and practice to ensure that the framework conditions are complied with.

Risk management shall contribute to the institutions’ attaining their objectives and adhering to their strategies. In order to achieve the desired effect, it is necessary to work through the risk assessments, to identify means of reducing risk. An officer with responsibility for implementing measures must be appointed and a deadline for implementation must be set. The risks must be followed up and reassessed at regular intervals. This also applies to ICT activities. In the experience of Finanstilsynet, inadequate provision is often made for risk

assessment and management in the sphere of ICT, and they are therefore not the governance instrument they could be.

Because they fail to perform, or perform inadequate risk assessments prior to a decision to outsource, many institutions do not have a true overview of the risk they run in outsourcing. Institutions that outsource are also responsible for risk management and internal control in those activities that are outsourced. Many institutions do not have sufficient insight into the risk management and internal control of their suppliers.

5.3 Criminal attacks on payment systems

5.3.1 Assumed background to the criminal activities

Organised crime targeting banks' payment systems is an ongoing and growing problem. It is probable that many of the attacks that take place in the northern and western parts of Europe have a basis in organised crime. These environments often have a complex structure with project-like forms of attack. It is therefore difficult to find effective means of stopping this type of crime. Important measures to combat this internationally are community building and democratisation in the core areas in question, police cooperation (which is already taking place through Interpol and Europol), various cross-border programmes and collaborations in Europe, for example the CERT collaboration, collaborative programmes associated with the development and use of the internet, and specific collaborative programmes in the financial sector.

5.3.2 Internet banking crime

In 2011, a number of banks in Norway were subjected to attacks on their online bank by means of Trojan programs. Different types of Trojans were used:

a) Trojans that have to be combined with active monitoring, i.e. that require a man-in-the-middle system, to change the contents of customers' transactions with banks, for example amounts and account number with re-use of one-time and other codes unnoticed by the customer.

b) Trojans that already have the logic programmed in. This latter is perhaps the most serious type in terms of possible volumes in an attack, and requires less costly input on the part of the criminals. Many methods are used to infect the individual users' PCs with Trojans. Phishing and spam are probably some of the means used, where clicking on a link in an e-mail results in the Trojan being updated in a PC. Visits to various websites is another.

The banks' awareness of this problem, coupled with close cooperation with the various operators, is an important factor in the battle against this type of crime. The authorities' awareness of the problem may also be of importance.

It is evident that the situation must be monitored closely, and that there must continue to be investment in security measures in this area.

5.3.3 Payment card fraud

Payment card fraud is the area where the financial industry has suffered the heaviest losses. In 2011, misuse of some 17 000 payment cards was reported, and overall losses associated with payment cards totalled over NOK 125 million.

Skimming of payment terminals and ATMs in Norway has been reduced. The requirement that all payment cards have chips and all payment terminals have a chip reader has contributed to this, and the use of false cards with magnetic strips has been almost eliminated in Norway. But skimmed information from magnetic strips on original cards is still being copied into magnetic strips on false cards and used abroad, and this is where the greatest losses are suffered. Skimming itself also takes place abroad for the most part, both with and without reading of PINs in addition. In Norway the payments that can be made at payment terminals without a PIN are very limited, but it is more usual in a number of other countries. One useful possibility offered by many banks is a regional block that can be placed on cards. Card-owners can restrict the use of their card to a desired geographical region at any time.

Substantial losses are also associated with loss of original cards with PINs. This is associated more with traditional theft and robberies.

Misuse of card information without the use of cards, i.e. in online trading, is associated with not insignificant losses. There is a bewildering flora of variations on the theme here. Some type of phishing is often used to extract credit card information, but there may also be data leakages in the form of hacking into retail sales systems or the like. Credit card information is used in increasingly sophisticated business cases to maximise returns, but also to mask fraud. The rightful owner of the card may appear to be guilty of dubious transactions in which the card has been involved.

Financial institutions use sophisticated surveillance systems to monitor card fraud. It is important to focus strongly on card fraud in order to maintain control of losses.

5.4 Risk of disrupted operations and system error

5.4.1 Contingency systems

Incidents that affect the financial ICT infrastructure show that contingency solutions are not always available as they are expected to be by the institution that is affected. Contingency systems are not always maintained in parallel with the production system. Annual tests, cf. Section 11 of the ICT Regulations, often provide useful information to form a basis for updating contingency systems.

New technology offers greater robustness. Today customers can access financial services by means of mobile devices, via the internet, via telephone banking, by appearing in person at the bank, or by means of standing orders such as e-invoices and direct debit.

However, the core systems are as sensitive as ever and must have good contingency systems.

5.4.2 LacLack of overall picture

Incidents show that some institutions have challenges associated with inappropriate architecture. It may be a matter of a non-optimal data model, where the ownership and

definition of data entities and attributes are unclear. It may also be that the ICT architecture is not sufficiently layered, which can present challenges with respect to maintenance. New functionality may have undesirable and unintended consequences for other systems. To be on the safe side, new data entities tend to be defined for special purposes, which presents further challenges with respect to maintenance and overview.

Financial transactions are processed automatically in a processing chain in which a number of operators participate. Incidents in 2011 show that the operators could have cooperated better on surveillance and alerts to the advantage of all concerned. Institution B receives transactions from institution A according to a regular pattern ("calendar" and volume). B, who detects a departure from the pattern, can alert A. A and B subsequently cooperate on rectifying, clearing up etc. Some sound initiatives were taken in this area in 2011.

5.4.3 Parameter setting; difficult testing the transaction chain and associated infrastructure

Incidents that affect the financial ICT infrastructure indicate that maintaining the operating platform may be a challenge. The platform consists of an extensive set of auxiliary systems, both hardware and software, which the end-user service (e.g. online bank) is dependent on. It is complicated configurating and maintaining application servers, database servers, web servers, communication software, surveillance, certificates, access rights, firewalls etc. A number of factors, such as changes in system loading, number of users and new end-user functionality, can result in a need to change software parameters, which requires detailed knowledge and close surveillance.

Thorough testing is a prerequisite for stable operations. A number of institutions have test environments that closely reproduce the production environment. Some institutions use programmed tests (scripts) extensively, and benefit considerably from them in connection with regression testing of new releases of the applications. But Finanstilsynet also sees institutions that frequently have to recall new releases, make corrections, re-test and start production anew. The institutions waste time and resources and this creates noise among their customers. Thorough testing is a good investment.

Financial transactions are carried out automatically from start to finish. All processing is automated, from the customer's entry of the transaction up to and including the accounting and archiving. A number of financial institutions are involved in the processing of a transaction. There may be a need to regression-test the entire transaction chain, i.e. testing must also be carried out in relation to systems that the institution does not have direct control over. Carrying out such extensive tests may be an organisational and technical challenge. It requires good cooperation among all those involved.

6 Further follow-up by Finanstilsynet

6.1 IT oversight

Finanstilsynet has developed a comprehensive programme for IT oversight and oversight of different aspects of payment services. The breakdown into areas is very largely according to industrial standards. The modules to be used for the individual inspection are chosen on the basis of a risk assessment of the institution in question. The purpose is to administer and further develop the institution. The modules are available on Finanstilsynets website[14] with a view to relevant institutions also being able to use the modules for their own work.
It is planned further developing this system by selecting particular topics. The following areas have been chosen:

a) IT governance,
b) disaster recovery and emergency planning,
c) electronic payment systems,
d) ICT infrastructure and
e) outsourcing, including offshoring and cloud computing.

The plan is to use relevant topic modules for the most systemically critical institutions and view these in context with other ordinary IT oversight, incident reporting and the duty to report on payment services as a basis for assessment of the level of operational risk for the ICAAP[15] processes.

6.2 Payment services

6.2.1 Duty to report

It is important for Finanstilsynet to remain updated on changes that take place in payment services. There are extensive technological developments in progress in the field of mobile devices which are increasingly acquiring the same features as personal computers. The financial sector, particularly banks, is adopting this technology and offering solutions to its customers on new mobile devices. The risk picture may become more complex, and a high degree of expertise may be required in order to acquire and maintain an adequate overview of the risk picture. In order to ensure that it has adequate information on developments in this area, Finanstilsynet will maintain the duty to report.

6.2.2 Cooperation

There are many operators in the field of payment systems in Norway who have responsibilities and tasks that lie close together in the regulations and to some extent overlap. In order to be sure that tasks do not fall between two stools while at the same time ensuring coordination to avoid duplication of work, Norges Bank and Finanstilsynet have cooperated closely on payments for a number of years. In 2011 a joint document that regulates this area was drawn up on cooperation and division of responsibilities between Finanstilsynet and

[14] http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/Egenevalueringssporsmal/
[15] Internal Capital Adequacy Assessment Process (ICAAP) requires regular performance of an internal capital adequacy process in order to adopt a position on capital requirements.

Norges Bank. Both organisations believe that this close collaboration is yielding positive effects and contributing to efficient use of resources. The collaboration will continue in 2012.

Finance Norway's Service Office, Section for Payment Systems and Infrastructure, takes care of many important tasks for the banking sector. This applies in particular to shared systems in the area of payment services. Finanstilsynet has therefore aimed for close cooperation with FNO in this area. The collaboration also includes the Norwegian Banks' Standardisation Office (BSK). Finanstilsynet believes that close cooperation in the area of payment systems may serve to increase the attention to problem areas and risk management.

6.3 Risk and vulnerability (RAV) analyses

Finanstilsynet receives information from many financial institutions concerning their compliance with the ICT Regulations. Finanstilsynet can thereby form an opinion on what is best practice in the areas covered by the ICT Regulations. Against this background, Finanstilsynet can form a picture of which institutions have a potential for improvement and can influence the institutions in the direction of best practice.

Finanstilsynet receives incident reports; see Section 9 of the ICT Regulations. This enables Finanstilsynet to identify single points of failure, i.e. ICT components that may affect large parts of the financial ICT structure if they do not function according to intention. Each institution sees the consequences for its own activities. Finanstilsynet's challenge is to assess the consequences for the industry as a whole.

In their work on risk analyses, the financial institutions prioritise the aspects over which they feel they have best control, i.e. first and foremost ICT infrastructure that is delivered and controlled by the institution itself. Finanstilsynet assesses the risk analysis of the individual institution through regular inspections, thereby contributing to an assessment of the overall risk picture for the industry. In this overall assessment, it is also important that Finanstilsynet maintain contact with the supervisory authorities. This provides useful insight into threat trends and security measures.

Finanstilsynet urges institutions to pool their knowledge of vulnerabilities and current threats. As part of its oversight of the institutions, Finanstilsynet reports current threats to the institutions. Finanstilsynet also makes anonymised overviews that are distributed among the institutions. Finally, Finanstilsynet assembles the institutions annually to inform them of findings and trends detected through incident reporting.

6.4 Incident recording and reporting

Finanstilsynet has gradually built up a substantial incident database that represents a valuable source for analyses of trends and relationships. In the event of serious incidents that strike many institutions simultaneously, Finanstilsynet assembles the industry for a meeting to clarify the situation and agree on common measures. This applies in particular to security incidents where exchange of information is important to enable effective measures to be implemented.

Ensuring stable, high quality reporting can be a challenge. Major banks and financial institutions are therefore followed up with meetings on reporting. In order to focus attention on and show appreciation for the reporting carried out by the institutions, Finanstilsynet invites relevant contact persons in the institutions to an annual incident seminar with relevant topics associated with incident management.

In the wake of the Easter incident, the banks have identified a number of factors that can be improved. Many of the proposals from the banks have resulted in specific measures. Finanstilsynet is working on a review of the documentation from the banks, and will follow up the results of this work in relation to the individual bank and the banks' primary suppliers.

6.5 Contingency work – Contingency Committee for Financial Infrastructure

Through the medium of the Contingency Committee for Financial Infrastructure (BFI), which is chaired by Finanstilsynet, contingency exercises are planned and conducted across financial institutions and suppliers. In 2011, two exercises were conducted under the auspices of BFI: 1) exercise in the payment systems area, under the leadership of DNB and 2) exercise in organisation and procedures, conducted under the leadership of Finanstilsynet. In our experience, regular exercises in contingency planning are necessary to ensure that they function in a real emergency situation.

Proposals based on original proposals prepared by BFI have been drawn up in collaboration with Norges Bank to prioritise telecommunications and power supply for specific key institutions, as have proposals for alternative means of payment in an emergency situation. The proposals form part of the general contingency work for the financial sector and have been submitted to the Ministry of Finance.

BFI represents an important meeting place between different operators in Norway who have responsibilities in the Norwegian payment system. The committee has many responsibilities, but has a particular focus on contingency work, and is therefore concerned with following up incident trends. Conducting exercises in order to be optimally prepared in the event of a serious incident is important and receives priority. Finanstilsynet will continue the work of developing BFI and remain responsible for the chairmanship and secretariat of the committee.

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