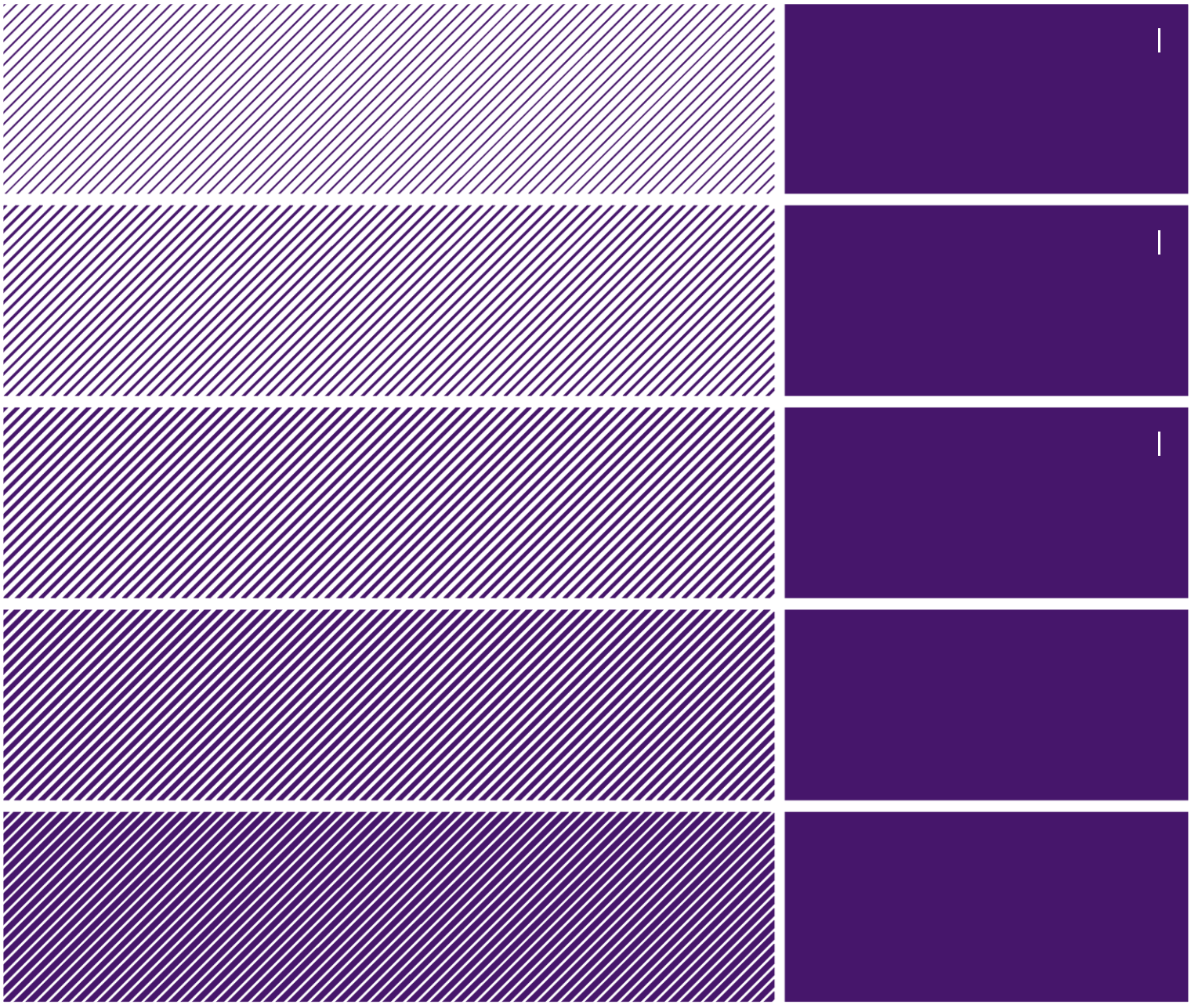
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Report

Risk and Vulnerability Analysis (RAV) 2010

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



Contents

1 Introduction 5

2 General trends 6

2.1 IT Governance 6
2.2 Inadequate management of large projects 6
2.3 Changes often lead to error 7
2.4 The ICT supplier landscape 7
2.5 Outsourcing and offshoring 7
2.5.1 Developments and risk situation 7
2.5.2 Control of outsourcing of ICT services 8
2.6 ITC infrastructure 9
2.7 Cloud computing 10
2.8 Algorithmic trading 12
2.9 Use of mobile units 13
2.10 Development of services in payment systems 13
2.11 Internet crime 15
2.11.1 Developments in crime 15
2.11.2 Risk reduction measures 16
2.12 Theft of information 17
2.12.1 Identity theft 17
2.12 Internal fraud 18

3 Payment service systems 20

3.1 General information on payment systems 20
3.2 Risk and vulnerability in payment systems 21
3.3 Management and control of payment systems 22
3.4 Notification requirement - Systems for payment services 23
3.5 Overview of annual losses related to payment services 23

4 The findings and observations of Finanstilsynet 25

4.1 Findings from IT inspections in 2010 25
4.1.1 Testing of disaster recovery plans 25
4.1.2 Coordination of processes 25
4.1.3 The resource situation 26
4.1.4 Risk and vulnerability (RAV) analyses 26
4.1.5 Institutions' ICT expertise 26
4.2 Interviews –institutions' own assessments 26
4.3 Reporting of incidents to Finanstilsynet 28
4.3.1 Incident reports in 2010 28
4.3.2 Findings from incident reports in 2010 29
4.4 Outsourcing to countries other than Norway 31
4.5 Questionnaire surveys conducted in 2010 31
4.5.1 Duty of notification – Section 3-2 of the Payment Systems Act 31
4.5.2 Regulations relating to requirements regarding the design of ICT systems for members of the Norwegian Banks' Guarantee Fund 32
4.6 Incidents culled from international sources 32
4.6.1 The theft of data from a testing system in Cleveland, USA 32
4.6.2 The National Bank of Australia 33

4.6.3 An incident in DBS Singapore 33

5 Identified areas of risk 34

5.1 Skimming attacks on ATMs 34

5.2 Attacks on online banking services 34

5.3 Inadequate testing and verification of disaster recovery plans 34

5.4 Lower-quality operations due to organisational changes implemented by ICT suppliers 35

5.5 Lack of management and control in connection with outsourcing 35

6 Further follow-up by Finanstilsynet 36

6.1 General 36

6.2 Current efforts focused on risk areas 36

6.2.1 Skimming 36

6.2.2 Online banks 36

6.2.3 Disaster recovery plans 37

6.2.4 Management and control in connection with outsourcing 37

6.3 IT inspections 37

6.4 Handling emergencies 37

6.5 Handling of ID theft 37

6.6 Information and communication 38

6.7 CoMiFin 38

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 information and communications technology (ICT).

At the outset of the work on the RAV analysis it is important to ensure that Finanstilsynet has sufficient information about the risk associated with the financial sector’s use of ICT and payment systems.

It has been important to identify means of securing more information on quantitative data which, in conjunction with qualitative data, provide a basis for risk assessments. One important part of this work has been to establish mandatory reporting of ICT incidents to Finanstilsynet.
In 2010, Finanstilsynet collaborated with other financial sector organisations to obtain correct information about losses associated with selected payment areas. This adds to an understanding of the risk level and the need for action.
The RAV analysis is an important tool for Finanstilsynet, but it can also be used as a source of information in the work on risk in individual financial institutions and trade organisations. The RAV analysis is also an important contribution to international ICT cooperation.

2 General trends

2.1 IT Governance

Corporate management and control of ICT is essential for financial institutions because ICT provides important premises for the activity as a whole. At the international level, management and control of ICT have become synonymous with the concept of IT governance. As such, it must form an integral part of corporate governance. Experience to date shows that ensuring relevant involvement by business management and creating awareness of the link between ITC activities and the activities of the institution as a whole still present challenges.

The Regulations on the Use of Information and Communication Technology (the ICT Regulations) define factors and requirements that must be observed in order to ensure appropriate direction and control of ICT activities.

Adequate management and control are important for fulfilling commercial requirements, for risk management and for compliance with regulatory requirements. Sound technical guidance and methods are available in this area. The fact that problems due to lack of coherent direction and control of ICT activities still arise is therefore cause for concern.

2.2 Inadequate management of large projects

We still see major financial sector projects failing, and that the management's inadequate knowledge of management and control of ICT projects impacts on progress, cost control, quality and the realisation of anticipated gains. This may have very serious consequences that are not always reported and followed up in an appropriate manner.

Good management is contingent on the management being involved and stipulating requirements regarding reporting on progress and irregularities. In the estimation and budgeting process, the institution can draw on experience from similar projects. This is only possible, however, if the institution has a quality system that can capture this experience. A work breakdown structure1 (WBS) from a similar project can provide an overview of all necessary activities. Lack of an overview may lead to activities being omitted and to underestimation of both costs and resource requirements.

The follow-up process is essential in all projects. It is important to use milestones that are well defined for all deliveries that are to result from the activity. Inadequate definition may lead to a situation where the activity is reported as 90 per cent complete, but where the last 10 per cent proves in practice to be far more than this. Without precise progress targets and sufficient breakdown of tasks in terms of scope and time, both calendar time and budgets may be used up before discrepancies are detected.

Progress, prerequisites, risk and dependencies must be closely monitored throughout the project period. Failure to do so will often result in acute situations for which no preparations have been made. This will require input of resources that may take time to procure, which may prevent the start-up of other activities.

Project management has developed considerably in the last few decades. There are several readily available project methods that have been designed according to recognised standards, for example those of the International Project Management Association (IPMA) or Project

[1] Work Breakdown Structure: A tree structure that shows a breakdown of the work that has to be done to achieve an objective.

Management Institute (PMI). Good project management is assured by using recognised project methods that are applied by qualified project managers.

2.3 Changes often lead to error

A requirement that major cost cuts be made often makes it necessary to change the system portfolio, and hence results in change. Inadequate management and control when these measures are implemented may result in poorer quality and higher operational risk.
In addition to requirements for cost-cutting and higher earnings, some segments of the financial industry are subject to extensive regulatory amendments as a result of international recommendations, EU directives and national regulations. The combined effect of all these factors may be that several major changes are required in ICT systems at one and the same time, thereby presenting a risk. Examples of such regulatory changes are the Pension Reform, the Basel III regulatory requirements and Solvency II in the area of insurance.
It is vital that risk assessment and management of operational risk form an integral part of institutions' efforts to adapt to new rules, cut costs and implement efficiency measures.

2.4 The ICT supplier landscape

Further consolidation is taking place as already large suppliers merge their operations. In Norway, EDB Business Partner ASA and ErgoGroup AS have formed the company EDB ErgoGroup ASA (EDB). Norwegian BBS and Danish PBS have established a joint company, NETS, with its head office in Denmark, and a Norwegian subsidiary, NETS Norge AS. SDC (Skandinavisk Data Center), which is operations service provider for the Terra banks, has initiated a process with Bankernes EDB Central (BEC) to establish the company Nordisk Finans IT, whose combined operations will be handled by JN Data (Jyske Bank og Nykredit). SDC's IT operations will be moved from IBM to JN Data through a strategic partnership.
The desire to achieve economies of scale and other synergies is an underlying reason for the mergers. The application portfolio can be coordinated and rationalised. The scale factor is also important in connection with systems development and purchases.
There is also a clear tendency for IT suppliers to exploit opportunities to cut costs and increase access to resources by moving significant portions of their activities to low-cost countries. Over time, the combined effect of these changes may entail risk as a result of a reduction in institutions' ability to exercise their own management and control and an increase in concentration risk. It will therefore be important to monitor developments among suppliers.

2.5 Outsourcing and offshoring

2.5.1 Developments and risk situation

In the Norwegian financial sector in general and banking in particular, there is a long tradition of extensive outsourcing of ICT. In the case of banks, this used to be regarded largely as part of their own risk assessment activities, since banks were both owners and users of the suppliers in question. The situation has changed, and now most ICT suppliers are free-standing operators, often listed on stock exchanges and with owners outside Norway. Suppliers are subject to cost-effectiveness requirements imposed by both owners and customers. They increasingly resort to offshoring to meet these requirements, both by

acquiring companies in low-cost countries and through other types of collaboration. The objective is to gain access to more resources, both expertise and capacity, at a lower cost. This trend results in a complex and demanding situation for both customers and suppliers with respect to direction and control, risk management and compliance with rules and regulations. If this type of outsourcing, with extensive use of offshoring, becomes widespread in the financial sector, it may imply a higher risk level. This applies to both the individual institution and the financial sector as a whole. Risk management requirements must be assessed in the light of this overall picture.
With certain exceptions, there are no rules that directly restrict financial institutions from outsourcing other than specific requirements that must be fulfilled. For example, a risk assessment must be performed. The individual financial institution must ensure compliance with laws, regulations, other relevant rules (e.g. internal regulation that is used among banks) and its own guidelines. It will therefore be important for the institution that is intending to outsource to ensure that all necessary analyses have been performed, documented and form the basis for a decision. If the institution opts for outsourcing, there will be provisions in the agreement between customer and supplier designed to ensure proper control of the outsourced activities.
In Circular 14/2010 on outsourcing of banks' ICT tasks, Finanstilsynet places clear restrictions on outsourcing to areas designated high risk areas. The restrictions relate to specific functions/areas of banking activity. It is Finanstilsynet's clear impression that banks have adapted their activities to take account of these assessments.

2.5.2 Control of outsourcing of ICT services

In order to deal appropriately with the delivery and discharge statutory responsibilities, it is necessary for purchasers of services to possess their own expertise in the area that is being outsourced (Section 12 of the ICT Regulations). Such expertise can be provided by the organisation itself or it can be procured from a consulting company, for example. It is also common for institutions to cooperate, either bilaterally or through trade organisations, for example, in order to maintain this expertise at a high level.
In order to be able to check an extensive delivery, it is necessary to divide it into appropriate units and make a detailed breakdown that enables verification to be performed. This must cover quantity, quality and security. To ensure maximum focus on quality, it should be made clear to the supplier that this is being monitored and that it is important to purchaser.
Agreements between customer and supplier have gradually become well-formulated and specific with detailed requirements relating to quality and pricing. But there are still examples where the quality is not good enough. Performance measurement in the field of information security is still an immature area, but there are a number of specific requirements. ISO 27002 is a code of practice for information security, and ISO 27004 a standard for measurement for information security management.
Past experience shows that measurements of this type must be organised so that they do not cost too much, or else they will not be carried out. Automated measurements that the systems report themselves are desirable. The measurements shall consist of quantification of ratios, counts, percentages or references to a pre-determined scale. Subjective assessments such as "high", "moderate" and "low" are not reproducible and have little meaning except in reports to the next level within the organisation.
Agreements must be revised at regular intervals to take account of new requirements and new systems. New forms of reporting and measurement for which there are currently no standards

or established framework will probably also be needed. The agreement should contain clauses to the effect that this area is to be further developed during the agreement period.
There must be special regulation of duties in the case of termination. The service provider must be obliged to provide competent personnel to arrange for handover to or conversion for another supplier. When making a transition to other systems, it must be required that the necessary professional assistance be provided for data extraction or conversion of registers.

2.6 ITC infrastructure

The long tradition of replacing manual processing with automated processing continues at an undiminished pace. In 2010 we saw developments where ICT services became more closely integrated in real time. An example of this is electronic loan applications over the internet with subsequent automated processing. Another is algorithmic trading of securities, foreign currency, etc. ICT activities have become more pervasive.
Finanstilsynet finds that institutions do not always have a documented overview of the interrelationships in their ICT systems. A number of the incidents that affect institutions and which are reported to Finanstilsynet show how the ICT systems are interconnected, and in which situations systems can impact one another negatively – either by "infecting" one another, or by one problem affecting several systems. These relationships do not always appear to receive adequate attention from institutions. Due to lack of an overview, faults may have more serious consequences than anticipated and efforts to reduce vulnerability may not be given high enough priority.
Extensive ICT activity generates a need for close control of daily operations. Good monitoring and alarm procedures are required. In the past, it was common to use measuring instruments that measured the properties of a single resource, such as the fill ratio of a dataset, utilisation of a data channel, etc. Transaction chains have become longer, and challenges such as capacity problems in one link in the chain may feed through to and have major consequences for services elsewhere in the chain. As often as not, a number of services share the same resources. This means that problems in one service, for example an undesired loop or freeze situation, may impact other services. For financial reasons, institutions are not in a situation where they have sufficient ICT resources in all areas to meet every conceivable need. Consequently, tools that optimise the use of resources are needed. So-called "intelligent" software agents are used more and more. They "take the temperature" at a number of places in the transaction chain under different conditions with respect to amount of traffic, type of transactions that predominate at different times of the day etc., and use analysis to predict possible current or future resource problems or other problems. There are examples of agents that go even further, by reallocating ICT resources "in flight".
Finanstilsynet observed a number of incidents in 2010 that indicate that monitoring and alarm procedures could be better. Most institutions have satisfactory monitoring and alarm procedures in the later phases of a developing incident. However, Finanstilsynet has registered a number of incidents that indicate fundamental weaknesses in monitoring in these late phases as well.
Many institutions still do not detect many of the incidents until the service is unavailable. They then analyse their way back to the cause of the problem, contact the supplier, find software patches, install them and test them. Finally the correction must be put into operation. Valuable time is lost due to late alerts. Preventive monitoring of the type described above (see the example of intelligent software agents) could be used more in institutions.
In 2010, financial institutions continued the trend of using available means of communication to supply services. New types of mobile banking are appearing, and more and more services are being offered by way of the mobile channel. Shops are increasingly offering banking

services. This means that the distribution of services has become more robust. If one channel is unavailable, customers can use another. This is a positive development. But if the central service is unavailable, the one that serves all the channels, the situation will be serious. There were a number of systemic changes in Norway in 2010. Norges Bank introduced a new settlement system in May 2010. In November, Norwegian Interbank Clearing System (NICS) introduced a third daily settlement for clearing. In August, Oslo Clearing launched a new system in which Oslo Clearing is the central counterparty for clearing and settlement in the securities market. The introduction of these changes has largely proceeded according to plan.

2.7 Cloud computing[2)]

Cloud computing (CC) was probably the most talked about and presented topic in ICT technology in 2010. NIST3 defines CC as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

CC does not represent any new functionality or new technology. The services and resources offered through CC are the same as those offered by traditional data centres, but the delivery model is new. The difference is that the customer, who in this connection is the supplier of an internet-based service operated through CC, no longer knows where his own applications and data are processed. In the long term, the fact that the institutions pay for actual use can make it cheaper to use CC than to scale one's own capacity. This also reduces the financial risk associated with offering new services for which the institution does not know the pattern of use in advance.

NIST summarises the essential features of CC:

- Customers are assured of automatic access to computing resources such as server and network capacity without the need for direct interaction with the individual supplier of services.
- Computing resources are available over the network, and can be accessed by means of various thin and thick client platforms such as mobile telephones, laptops, PDAs etc.
- CC suppliers have a pool of computing resources that can serve many customers. Physical and virtual resources are dynamically allocated and released on the basis of customer needs. Customers normally have no control or knowledge of the exact location of the resources that are used, but can stipulate requirements regarding location (in the network) at a higher level of abstraction - e.g. country, state or data centre. Examples of CC resources are data storage space, CPU power, memory, network bandwidth and virtual machines.
- Computing resources can be dynamically activated. Rapid upscaling is achieved by allocating more resources and rapid downscaling by releasing resources. Customers experience that capacity as unlimited; computing resources can be procured on any scale at any time.
- Resource allocation is controlled and optimised automatically through measurement at a level of abstraction appropriate to the type of service, for example storage capacity,

[2] **Cloud computing** is a term used for everything from data processing and storage to software on servers in external server parks linked to the internet.
[3] National Institute of Standards and Technology, USA
http://csrc.nist.gov/groups/SNS/cloud-computing/

CPU power, bandwidth and active user accounts. Reporting takes place in a manner that assures insight for both supplier and user of the service.

The operations delivered according to a traditional operating agreement between a large company and an IT supplier will also have most of the above characteristics. So CC is not anything fundamentally new. But with CC, customers have to accept that operations take place somewhere "up in the clouds", without the customer knowing exactly where data and functions are stored. The concept "private clouds" is used about CC where operations within certain areas are tailored to meet the requirements of a single customer, for example to ensure compliance with national regulations and direct control of data and software, and also in cases where the company itself owns and operates the system. The differences from traditional outsourcing are then limited.

CC probably makes the greatest difference to small and medium-sized enterprises, and CC suppliers tend to target this segment. CC can be ordered over the internet, e.g. as an e-mail service or CRM service, and delivered the same day without the customer having to think about where and how the service is produced. Agreements are made without any form of human interaction between the parties to the agreement. Standard contracts and product packages are often used, as well as associated pre-defined SLA requirements.

For small enterprises, the security level offered by a CC service may be higher than they could establish themselves. CC is an immature area, however, and there is not yet much information available on the issue of security.
ISO/IEC JTC 14/SC 385 is working on the security aspect of CC. The following is a brief account of the problems associated with sending information over the internet with respect to assuring data flow and data security as long as they are in the clouds.

- Confidentiality
  Users do not have full control of their data. The CC model can expose data that is shown to the service supplier. These data flows, for example logs, can be used for purposes other than those desired by the buyer of the service or the end-user. CC suppliers seldom use encryption, as the internet banks do. End-users have no control of how suppliers authorise their employees. It may be difficult, at worst impossible, to check that suppliers do not use data to expand their own business activities.

- Integrity
  Data can be monitored or manipulated by external forces, such as government authorities or employees of the supplier. Databases in the clouds may be tempting targets for criminals, particularly if the security is inadequate. In such cases it may be impossible for users to know whether the data have been exposed to unauthorised persons or whether they have been lost.

- Availability
  Availability in the internet may be both slower and poorer than in an intranet. The network can also be blocked by various external forces. Data may be corrupted by the supplier's employees, and the authorities may block the internet to prevent the unwanted dissemination of information, i.e. conduct censorship. Courts may also

[4] **ISO/IEC JTC 1** is the Joint Technical Committee 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
[5] Reaching for the Clouds: Privacy Issues related to Cloud Computing - Canadian National Body

allow seizure or disclosure. Measures of this nature may affect a third party who uses the same CC as the customer who is initially subjected to these measures, because it may be difficult to distinguish between users in a situation of this nature.

- Compliance with laws and regulations
  Without control of where data are located, there is no control or overview of the laws that regulate access to and use of the data. Legal regulation of data protection often depends on who owns the data. At times it may be unclear who owns data that has come into being in the cloud, not least derived data and logs. It is difficult for the authorities to check that laws and regulations are being complied with when they do not know where data are being stored and processed, or how they are protected. The location of the physical storage unit may also be of importance. The use of CC must be regarded as a type of outsourcing/offshoring. Security issues must then be considered in the same manner as for data hacking and solutions must be provided in the form of backup and recovery of data in the event of disasters and in emergency situations.

Simplicity, ease of use and flexibility are the forces behind CC. As pointed out above, there are also a number of disadvantages associated with CC. Achieving the same degree of security inside a boundless cloud as outside demands special security measures. The heavyweights among the CC suppliers are engaged in developing solutions for secure access control, encrypted communication, customers' control of own data and monitoring of CC systems. However, there is a long way to go before CC is ready for the banking sector's core activities.

2.8 Algorithmic trading

In recent years a number of new technological systems have appeared in the securities trading markets. The new systems have introduced new risks and challenges for the control authorities. The examples below illustrate some of the challenges.
New ultra-high-frequency trading systems open the way for short-term speculation. Based on market information, buy and sell decisions are automatically executed based on decisions made by pre-programmed algorithms.
Some surveys reveal that many of the algorithms are fairly similar. In other words, the algorithms will reach similar conclusions concerning a decision to buy or sell. This leads one to think that algorithmic trading could possibly reinforce market fluctuations and lead to instability. Another viewpoint is that algorithms act like humans, with the only exception that the algorithms are better than humans at capturing recorded fluctuations and acting on them, hence in principle there is no new risk involved. The survey "Rise of the Machines: Algorithmic Trading in the Foreign Exchange Market" analyses the relationship between the share of transactions conducted by algorithms and the volatility of the foreign exchange market. The survey concludes that there is no positive correlation between volatility and the share of transactions conducted by algorithms. The conclusions indicate that algorithmic trading in the foreign exchange market does not cause instability in the form of increased volatility.
High-frequency trading, ultra-high-frequency trading, algorithmic trading and dark pools are concepts used in the new high tech trading systems. In 2008 the US Securities and Exchange Commission (SEC) performed an analysis of the risks associated with the new technology.

On 6 May 2010 the much debated Flash Crash occurred. The Dow Jones index fell first by 300 points, then by 600 points in the course of five minutes. Twenty minutes later, most of the 600 points had been recovered. The US Securities and Exchange Commission and Commodities Futures Trading Commission (CFTC) examined the chain of events and presented a picture of a market that was so fragmented and fragile that a single large trade could cause the equity market to plunge dramatically. The incident was sparked by a fund trying to sell an unusually large number of securities. In the end, there were no buyers. High-frequency sellers then started aggressive selling, which exacerbated the fall.
New technologies have led to the emergence of a number of new marketplaces in recent years, such as OTC6 and "dark pools". These marketplaces are less transparent than stock exchanges and other regulated markets. The lack of transparency makes it difficult to trace transactions. In some cases the order books are not available, which makes it difficult to detect activity that takes place immediately prior to a trade, and which could indicate attempts at price manipulation.
Finanstilsynet notes that there are different perceptions of the risk associated with the new technical systems and the new marketplaces. This may indicate that the risks have not been fully analysed. Finanstilsynet is therefore monitoring this area very closely.

2.9 Use of mobile units

Mobile units have become an increasingly important part of ICT infrastructure. They present challenges to security when they have access to institutions' internal systems, including office support systems such as e-mail and calendars.
A number of the risks that arise can be ascribed to portability and extensive use of unprotected wireless networks. The use of open wireless networks increases the risk of sensitive information falling into the wrong hands.
Since most modern mobile units can store large quantities of data, it is important that they have adequate security mechanisms and centralised administration. Security mechanisms that enable encryption of sensitive information ought to be a prerequisite for any unit that is part of an institution's ICT infrastructure.
If an institution uses mobile units in its ICT infrastructure, this should also be covered in the institution's security policy. Aspects such as authentication, encryption, updates and security administration should occupy a central place in the guidelines for use of mobile units.

2.10 Development of services in payment systems

A payment service comprises all elements in the transaction chain between payer and beneficiary. This applies in all markets, private and corporate, and in all payment systems, national and global.
The Financial Institutions Act stipulates which institutions can provide payment services, and states that none can engage in payment services without authorisation. The way is now open for a new category of institutions called "payment institutions". A number of institutions are expected to apply for authorisation as payment institutions, and then to offer payment services to both retail and corporate customers.
All payment services depend on infrastructure, which can be divided into two main parts. One part is the communication infrastructure, where a bank or payment institution communicates with a payer on the one hand and a beneficiary on the other. The other part is the cash settlement, which requires entry of the payment transaction on the payer's account (debit) and

[6] OTC = over the counter, i.e. a market for non-listed securities.

on the beneficiary's account (credit). Accounting can take place within the same payment institution or bank without transfer of cash provided that both parties have accounts with the same institution. If the parties have accounts in different institutions, the transaction will be cleared in a clearing centre and processing will not be completed until a final cash settlement has taken place between the institutions' settlement accounts in the central bank or another approved settlement bank.
Development in payment services normally relate to customers' communication with a bank or a payment institution. However the functioning of the shared infrastructure is equally important.

PayPal is the most widely known payment institution internationally. The institution was established in the USA on the basis of internet trading, but was later taken over by eBay and expanded worldwide. The institution currently has about 220 million accounts. The service concept that is offered is that the payer is charged via a credit card or PayPal account, and the beneficiary is credited on an internal PayPal account. PayPal uses an ordinary bank as settlement and liquidity supplier in the management of the PayPal customers' money. PayPal is a major account operator where it is possible for two parties who both have a PayPal account to carry out rapid transactions. In consequence, PayPal does not participate in the traditional interbank market. If a payment beneficiary wants cash in his or her account in an ordinary bank, it has to be transferred out of the PayPal system and into the traditional banking market.
The competitive advantage of PayPal is that money can be moved instantaneously by way of internal transactions in its own system. Users can transfer money simply between iPhones by means of this function. The program can be downloaded free of charge from the Apple iTunes Store or Apples App Store for iPhone or iPod Touch. Transfers between PayPal accounts take place instantly when users hold their iPhones out towards one another.
Because the transactions take place within a separate system, however, money is not moved. This is only a debit/credit transaction or transfer of information between two customers' accounts in the PayPal system. Similar transactions are made within Western Union, the Hawala system and traditional banks in the case of simple transfers and/or between own accounts. Efficiency, in terms of both transaction time and the use of liquidity, increases with the size of the individual institutions. In a large institution there is a greater probability that a number of customers will be able to trade with one another. Other examples of new services that may entail risk are so-called overlay payment services, which in some cases operate between customers and banks. This type of system must be thoroughly evaluated with respect to risk, security and regulatory compliance before it is introduced.
In recent times, internet portals and enterprises such as Facebook, Google and Twitter have emerged as potential marketplaces and suppliers of payment services and simple loans. Participants in these internet areas may make bilateral payment transactions, either in organised form or individually, and other financial transactions that entail transfer of liquidity and also risk-taking through direct lending. Facebook, Google and Twitter exploit network effects because they have many users who want to trade with one another. The transaction volume may be very high, but each individual transaction is for a relatively small amount. It is not clear at present how the situation will develop. There is particular uncertainty as to how transaction security and the possibility of economic crime in these marketplaces should be handled.
Developments in services in the corporate market are most pronounced in services targeting large, typically international enterprises. New services are often first developed here in response to market demands. After a while they are further developed for medium-sized and small enterprises.

Over the last few years, there has been a gradual trend towards more use of standardised international message types based on ISO 20022 XML, where institutions are also direct users. It started with Swift enabling enterprises to conduct all sorts of transactions with banks or other financial institutions. Today some 800 enterprises are direct users of payment or other settlement services through the Swift network. This has resulted in a considerable increase in the efficiency of the enterprises' liquidity handling and all associated administration.
Swift has now launched the product eBAM (electronic Bank Account Management). This service comprises the opening of accounts, changing of account data and registration of authorisations and signatures directly with the individual banks that the enterprises use. Enterprises were previously compelled to resort to manual services offered by their banks, but now they can improve efficiency by doing this back-office work themselves. The banks can also cut costs by simplifying existing interfaces with their corporate customers.

2.11 Internet crime

2.11.1 Developments in crime

The financial industry reports a growing threat level in internet crime.
The Hewlett Packard (HP) study "Cyber Security Readiness" indicates that more than half of the enterprises in the USA (56 per cent) and over a third of European enterprises (38 per cent) claim to have been subjected to a national cyber-attack. 78 per cent of organisations in the USA and 60 per cent of European organisations believe that a cyber-attack will substantially impact critical national infrastructure in the next two years. A large majority believe that a cyber-attack is difficult to detect (88.5 per cent), cannot be swiftly rectified (86.5 per cent) and that there are no good countermeasures against attacks of this nature (82.5 per cent).
From Symantec's survey "2010 Critical Information Infrastructure Protection", it emerges that 53 per cent of suppliers of critical infrastructure say that their networks have been subjected to politically motivated cyber-attacks. Respondents state that they have experienced attacks an average of ten times in the last five years, and that these have cost them USD 850 000 on average.
According to the HP study, 80 per cent of the enterprises in the survey believe that they are a part of critical infrastructure. This applies to enterprises in the oil and gas, telecoms, financial, power supply and water supply industries. The enterprises state that they realise the seriousness of the situation and the need to be prepared. But the survey shows that less than half of them are actually capable of resisting a cyber-attack, according to HP.
The authorities in a number of countries, including Norway, have been subjected to attacks with very serious consequences. Attacks in the wake of the Wikileaks revelations demonstrate clearly that attacks can do great damage and exert considerable pressure on the authorities and suppliers of internet services. Some of the attacks have targeted the financial industry's information network, as a reaction to financial institutions cutting off access to Wikileaks accounts.
Facebook and Twitter are examples of enormous social networks where the participants communicate over the internet. There is an obvious risk that these networks may be exposed to various kinds of cyber-attacks. For example, on 6 August 2009, the Norwegian News Agency reported the following: "Micro-blog service Twitter was knocked out on Thursday by a malicious cyber-attack".

The social networks may be arenas for “social engineering” (fraudulent acquisition of information) and sophisticated collection of personal data which is then subject to abuse. In well organised, planned attacks, data collection of this nature will often be one of a number of sources of information. The trend appears to be for attackers to combine various techniques in order to maximise their returns. Social engineering, malware and technical manipulation of equipment are all aspects of ID theft that is used to open an account in another person's name and use services under another identity in various electronic channels.
There are many indications that the attackers are well organised. The bot farmer who controls the bot network is the one who develops and cultivates the bot network[7], i.e. the computers that are used to carry out the attacks. The criminals rent and use the network. Helpers are equipped with false passports and use their passports to open bank accounts. In many cases, one person will open several accounts under several different identities. Stolen identities are abused for purposes of gain. Recent arrests in the USA and the UK indicate that there are organised groups behind fraud, and that they have the resources to engage in profitable internet crime on a grand scale. In 2010 there was increased activity from known Trojans like Zeus and Torpig against internet banks in Norway. Typical of the attacks is that the customer’s PC becomes infected with Trojan malware when they open a spam e-mail, click on links or download from websites. The malware/malicious code ensures that the user’s PC is linked to a bot network and a server in a control centre operated by whoever has distributed the code. The control centre can read the user’s typing on the PC. The Trojan then goes into hibernation. When the user keys in the URL of his internet bank, the Trojan program starts. From here on the attack is often based on “phishing". The user is presented with a log-on window which is indistinguishable from the bank’s, but contains more fields for filling in log-on information. The Norwegian in this user dialogue is often poor. The internet address that appears in this false log-on window is often false, and often lacks the security marking that is present in a true internet bank, i.e. the padlock to the right of the address in the URL field. The control centre in the bot network monitors the infected PCs in real time. The customer’s log-on data are stolen and the control centre logs on as the customer in the customer’s internet bank and enters transactions. The beneficiary accounts – called “mules” – are usually in a bank abroad.

Norwegian internet bank customers are also subjected to various attempts at phishing through e-mails from senders posing as banks or another relevant institution.
Antivirus programs prove to be fairly ineffective against Trojans that are not already known on the internet. Moreover, when a Trojan code has infected a PC, it can be changed via the master server so that an antivirus programme that has gained control of the original profile will not recognise the Trojan code again anyway.

2.11.2 Risk reduction measures

Banks both inside and outside Norway are attempting to increase their security as the threat level escalates. Santander offers all customers free software that limits the functionality of the

[7] BOT (from Robot) stands for malware that allows the attacker to take control of the computer. Bots are also known as ”web robots” and as a rule are part of a whole network of infected computers, also called the ”bot network”, which is often made up of infected machines all over the world. Since the bot-infected computer is subjugated by its master, a lot of people call these machines “zombies”. The criminals who control them are called bot farmers or bot masters. Some bot networks may consist of a few hundred or a few thousand computers, while others have tens or hundreds of thousands of “zombies” at their disposal. Many of these computers are infected without their owners knowing it. Possible symptoms? A bot can make a computer work more slowly, show strange messages or quite simply crash.

internet browser. According to the supplier, a tunnel is established for secure communication with the website. This is designed to prevent malware from inserting data and stealing information that is presented to the internet browser. Malware is automatically removed. The software establishes a direct connection between the bank and a round-the-clock analytical service that checks both for known threats and for incipient threats.
In recent years, National Westminster Bank has gradually introduced new measures linked to customer use of online banking. A while ago, the bank required that customers install software with security functions. The bank has recently made key customer functions contingent on customers installing the bank's security card and card-reader on their PCs.
In 2010, there was a breakthrough in international collaboration to combat internet crime. Cooperation among the police authorities of several countries led to the rounding up of a sophisticated ring of cyber criminals. The criminals were in the process of stealing up to USD 220 million from bank accounts that had been compromised by means of the Zeus virus.
Finanstilsynet notes that there is more or less informal collaboration among financial institutions, both nationally and internationally. This is how Norwegian banks were warned that customers had been compromised by the Zeus virus. At European level, alerts should preferably form part of a more formal, structured type of collaboration that will make it possible to react more rapidly and that will be better fitted to handling more concerted attacks. An EU-funded development project, CoMiFin[8] (www.comifin.eu) has developed an IT platform to support collaboration of this type. The CoMiFin project is designed to make it simple to set up a decentralised (peer-to-peer) IT platform that supports analysis of traffic data from participating financial institutions, and which alerts these institutions to attacks. There is also another type of collaboration in this area in Europe through authorities and financial sector operators: Financial Services ISAC (FI-ISAC), a European internet-based organisation associated with the financial sector. ISAC stands for "Information Sharing and Analysis Centre".
Finanstilsynet is aware that Norwegian banks are considering a number of possible means of reducing risk of internet crime. Relevant measures are that customers limit the selection of accounts that money can be transferred to, that all transfers can only be made to a pre-updated beneficiary register, and that each merchant has different single-use codes for each customer. The single-use code will then only be valid for a particular merchant, which will make it less interesting for an attacker to use. Measures that can be implemented rapidly include intelligent surveillance that recognises Trojan markers, exchange of information about "mule" accounts and manual control of all transactions to other countries.

2.12 Theft of information

2.12.1 Identity theft

Data leakage from an organisation's network is a growing security problem. The consequences of leaks from large registers may be considerable. For example, thousands of customers, Norwegians among them, were affected when the data register of one of Visa's and Mastercard's Spanish partners was hacked in the summer of 2009. The register contained information about cards and use of cards. We have to go back several years in Norway to find leaks from payment system registers. The case in point was leakage from a register that was operated on a server on behalf of merchants that were restaurants and hotels. Leaks have also

[8] CoMiFin is an EU-funded development project: Communication Middleware for Monitoring Financial Infrastructures

been registered from large and small public databases and registers. According to experience from countries outside Norway, leakage from data collections and card registers is widespread and also affects Norwegian customers.
The information that is stolen is often sufficient to enable the intruder to acquire and misuse the identity of another person or an institution. A stolen identity can be used in many ways, notably for the production of counterfeit bank cards and for siphoning money from bank accounts. It can also be used to buy goods and services, to open new accounts, take up loans and procure passports or other proof of identity. It can be a challenge for individuals to prove to banks that they have not acted negligently, so that they cannot be blamed for losing account data. In the past, Norwegian banks have largely covered their customers' financial losses in cases like this.
In addition to copying card data acquired, for example through a data leak, other sources of identity theft include theft of bank cards, passports, pay slips or other documents containing personal data .
Theft of identity has become increasingly widespread in Norway too. Norwegian identities appear to be attractive. The scale of thefts in terms of number and resulting financial losses is unclear, however. There is no overall reporting or overview at present. Not all cases are reported to the police, and not all cases are reported to Finance Norway (FNO), as reporting of losses from banks to FNO is voluntary. As a result, there are identity theft figures in circulation that cannot be verified.
Information to users and institutions is important, and is available on the Norwegian Data Inspectorate's website and also on the inspectorate's site www.slettmeg.no. NorSIS, part of the government's concerted effort to promote preventive information security, has also launched an identity theft project, and has established the website www.idtyveri.no.

2.13 Internal fraud

An unfaithful servant is an employee who abuses his or her trust or access to systems and information. Motives will typically be to do damage or to achieve personal gain. Unfaithful servants who are familiar with ICT systems can represent a serious threat.
Unfaithful servants are a growing problem for both the public and the private sector worldwide. What makes it so serious for some enterprises is that many events can take a long time to detect – long enough to put a small firm out of business or harm its reputation.

The two sectors that are most seriously affected by unfaithful servants are two of the most closely regulated areas – banking and finance, and general government administration. The challenges here are that the control mechanisms established to expose fraud, for example through internal audits, are not always equally good at detecting internal fraud. Norway focuses strongly on direction and control through the rules and regulations for the financial sector, and this may have contributed to the assumption that the problem is moderate compared with other countries. But events indicate that the problem may be growing. According to the Association of Certified Fraud Examiners (ACFE), findings in 2010 show that incidents of fraud are of the same type, irrespective of where in the world they occur. The survey revealed that more than 43 per cent of the reported cases of internal fraud took place outside the USA.

More than 80 per cent of the incidents in the study were perpetrated by individuals in one of six departments: accounting, operations, sales, executive management, customer service or procurement. More of than 85 per cent of the fraudsters had no previous charges or

convictions for fraud-related breaches of the law. The ACFE found that the average loss in cases of occupational fraud in 2010 was USD 160 000.

3 Payment service systems

3.1 General information on payment systems

Payment systems are essential to all economic activity. All trading in commercial or financial products culminates in an agreed monetary settlement. The structure of national payment systems is almost identical in all OECD countries: a central bank, various types of banks, payment institutions or other financial institutions are active participants in a chain of financial service providers, the links of which make up the payment systems. In Norway, payment systems are governed by the Payment Systems Act and other laws and regulations, and through the financial industry's self-regulatory system administered by Finance Norway (FNO).

In 2009, transactions effected through payment services in Norway totalled NOK 11 568.6 billion.9 Over 98 per cent of settlements took place by means of electronic payment methods. Only 1.7 per cent of payments were made using paper-based giros. In the retail trade, which totalled an estimated NOK 678 billion, roughly 70 per cent of payments were made electronically. About 2/3 of cash was withdrawn from ATMs or withdrawn in connection with purchases. Cash paid out at a bank counter accounted for around 10 per cent of retail sales. In Norway, the most important instrument of payment in the corporate market is online banking, which accounts for 61 per cent of transactions. Company terminal giros account for 23 per cent. BankAxept cards are used for 80 per cent of card payments in the private market, in terms of value. Norway tops the global list for use of payment cards.

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. In this type of payment system, a distinction is made between transactions between banks, an inter-bank system (bank-to-bank transactions) and transactions between private customers (payment services between the customer and the bank). Systems for payment services have been significantly improved by technological advances in recent years, with focus on cost-effective operations, user-friendliness and security.

A large part of the electronic infrastructure that is used is already outsourced to independent ICT suppliers that have their own plans and goals. However, the responsibility imposed through laws and regulations on institutions subject to authorisation will always lie with the institutions. This responsibility encompasses all the elements and participants at every link of the transaction chain between the payer and the payee. Finanstilsynet has discovered that, in many cases, this responsibility is not clearly understood, even by key senior management staff. Many institutions must focus greater attention on this responsibility, particularly by ensuring that they have the requisite expertise to fully manage and control the operational relationship with the supplier or, if relevant, the sub-supplier, to whom the payment systems have been outsourced.

The framework conditions for payment systems in Norway have been affected by increasing harmonisation within the EEA. This applies in particular to the standardisation and design of the payment services offered. The Payment Services Directive, which is a full harmonisation directive, was fully implemented in Norwegian legislation as of 1 July 2010. 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 door for a new type of enterprise, payment institutions. The provisions

[9] Norges Bank's Annual Report on Payment Systems 2009

governing payment institutions apply to all entities engaged in money transfer operations, and may cover enterprises/individuals who do not perceive their own activity as being subject to authorisation. All banks will have to assess, for example, whether private individuals with bank accounts in which there are frequent inflows and outflows of large amounts of cash are actually engaged in activity subject to licensing as a payment institution. If this type of activity is identified, the banks must ask these companies or persons to apply for authorisation as a payment institution since such activity is illegal without authorisation.

3.2 Risk and vulnerability in payment systems

The increased use of electronic systems provided by many different suppliers in the design of flexible payment services expands the transaction chain and increases the complexity of the payment systems. This can lead to a greater risk of error.

In 2010, three serious incidents in payment systems were reported in Finanstilsynet's incident reporting system (see section 4 for details). These incidents were caused by errors in the core systems which resulted in payment delays.

In order to manage and control such risks, the authorities have established a regulatory framework consisting of various laws and regulations. The most important of these are the Payment Systems Act and the Regulations on the Use of Information and Communication Technology (ICT). Oversight under the Payment Systems Act is exercised by Norges Bank with respect to interbank systems and by Finanstilsynet with respect to systems for payment services and securities settlement. Close, continuous collaboration has been established between Norges Bank and Finanstilsynet to ensure that the oversight function can be exercised as effectively and securely as possible.

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 carry out their payments. If one channel is inoperative, it will often be possible to use another.

Suppliers offering new means of payment are often registered outside Norway. These suppliers must now comply with the provisions that were implemented through the Payment Services Directive.

In Norway, the number of operators of core systems for banks and financial institutions is small. This can present a significant concentration risk.

It is important that contingency solutions be established for payment systems in order to safeguard against incidents. Robust solutions to avoid problems such as technical errors of the type "single point of failure", regular reviews of continuity requirements and testing of back-up solutions are key elements of preventive efforts.

The Norwegian Banks' Standardisation Office (BSK) sets BSK standards and binding security requirements for the EFT/POS10 system (BankAxept) in Norway. Furthermore, most of the payment card companies in the market comply with the international Payment Card Industry Data Security Standard (PCI DSS),11 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. Controls in this area may be inadequate.

The risk of criminal attack is greatest in the interface between customer and bank. As far as payment cards are concerned, such attacks consist of the theft of information in or concerning the card and cardholder, and the theft of the card itself with its PIN code. The first is a question of fraud by means of various methods related to use of the card, but can also be

[10] Electronic Funds Transfer/Point of Sale

[11] Payment Card Industry Data Security Standard

information gone astray within the bank. These risks are addressed by incorporating security measures in the systems. The theft of cards and PIN codes is often a result of cardholder behaviour.
In 2009, over 21 000 cases of payment card fraud were recorded in Norway.12 The total loss amounted to NOK 215 million, up 8 per cent on the previous year. Fraud amounts to approximately NOK 0.3 per NOK 1 000 in transactions. No losses were recorded in connection with online banking in 2009. Losses relating to paper-based giro services totalled NOK 6.1 million, which is NOK 0.047 per NOK 1 000.

3.3 Management and control of payment systems

Payment systems and services are part of society's critical functions and infrastructure. Management and control of the ICT activities related to payment services must be given high priority. Institutions' business staff must have a sense of ownership of and be involved with respect to functionality, changes, problems and risks. Requirements must be set with regard to structure, order, quality and formalities, and to ensure 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. Where payment services are concerned, this is hardly sufficient. Under the ICT Regulations, a risk assessment must be carried out prior to making changes that will affect ICT security, and the Regulations regarding risk management and internal control require, among other things, that institutions assess the material risks associated with their activities on an on-going basis. This also applies to the parts of their activities that are outsourced.
Under section 9 of the ICT Regulations, financial institutions must report ICT incidents to Finanstilsynet. Finanstilsynet notes that a majority of incidents reported in 2010 are a result of errors or instability following the implementation of changes. This applies to both system changes and operational changes. In Finanstilsynet's opinion, there appears to be a need for greater focus on change management, including testing, quality assurance, documentation and approval before the changes go into production. Under the ICT Regulations, procedures for change management must be established, documented and followed up. This is also in accordance with recognised international methods, standards and good practice.
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, there is a trend towards supplier concentration. In addition to the concentration risk that the new, large suppliers may present, experience has shown that when mergers take place, more attention is focused on financial matters, earnings and internal synergies than on meeting customer demands, needs and expectations.
Imposing requirements on a major supplier who in reality has hardly any competitors can be a challenge. When outsourcing services, institutions must ensure that they have sufficient competence13 to manage such agreements, and to set requirements in connection with outsourcing. Establishing requirements for and following up on a supplier located outside Norway is particularly difficult. In this connection, an effective risk culture, risk assessments and risk management play an increasingly important role in the efforts of banks and suppliers to ensure the stability of payment services. It is important that the risk assessments that are

[12] Norges Bank's Annual Report on Payment Systems 2009
[13] Section 12 of the ICT Regulations

carried out relate to and cover the aspects specified by the institution's guidelines[14] for its ICT activity.
Whenever outsourcing operations, the outsourcing institution must safeguard security[15] in the manner described in the ICT Regulations, the Regulations relating to risk management and internal control (Internal Control Regulations) and the Payment Systems Act. It is important to make security measurable wherever feasible, so that it is possible both to assess risk and take preventive action where necessary.

3.4 Notification requirement - Systems for payment services

Under section 3-2 of the Payment Systems Act, institutions must notify Finanstilsynet if they establish systems for payment services or make changes in such systems. Notification to Finanstilsynet is based on a self-evaluation process in which institutions answer 19 key control questions. The provision in the Act is a risk-reducing measure.
In the past five years, Finanstilsynet has received a varying number of annual notifications, and has considered whether this could be due to non-compliance with this requirement. In the first three quarters of 2010, Finanstilsynet received no notifications of new or amended systems for payment services.
In 2010, therefore, Finanstilsynet asked financial institutions to conduct a special review and assessment of vulnerabilities in connection with payment services. This request targeted the institutions' own internal development projects which might be subject to the notification requirement. The object of the notification requirement is to be able to identify risks associated with ICT-based payment systems and to do inspections.
In response to Finanstilsynet's request, financial institutions sent in 18 notifications in the last quarter of 2010. Ten of these notifications were sent by one institution.
Based on this survey, Finanstilsynet has reason to believe that the notification requirement is not sufficiently incorporated into the banks' administrative procedures, or in the units responsible for ensuring that the institutions comply with official laws and regulations (compliance officers). Responsibility for giving notification of new systems and changes in existing systems for payment services has been allocated to a variety of organisational units where this type of reporting does not appear to be a primary responsibility.
Another reason might be that notification of new and amended payment service systems is always given retrospectively and often at the same time as or after the system enters into production and is launched on the market.
In 2011, steps will be taken to improve institutions' follow-up of and compliance with the notification requirement.

3.5 Overview of annual losses related to payment services

In collaboration with Finance Norway (FNO) and the Norwegian Banks' Standardisation Office (BSK), Finanstilsynet sent letters to banks to collect data on losses, which also included losses related to payment services. The intention is to follow this up in the future so as to be able to present data on losses on the same services over time. This will make it possible to see loss trends, which will give individual institutions, industry organisations and the public authorities a better basis for tailoring appropriate measures. Finanstilsynet has initially decided to present loss data for selected payment services, broken down into the

[14] Section 2 of the ICT Regulations
[15] Section 5 of the ICT Regulations

categories online banking, use of cards in service channels, ATMs, EFT/POS payment terminals and use of cards for Internet transactions via web shops.

LOSSES RELATED TO USE OF PAYMENT CARDS (figures in NOK 1 000)

Type of payment card fraud	2010[1]
Misuse of card information, card not present (CNP) (Internet transaction)	9 401
Stolen card information (including skimming), misused with counterfeit cards in Norway	1 765
Stolen card information (including skimming), misused with counterfeit cards outside Norway	31 740
Lost/stolen cards, misused in Norway	14 395
Lost/stolen cards, misused outside Norway	5 149
Lost in mail	4 239
TOTAL	**66 689**

1) Data obtained from Finance Norway and the Norwegian Banks' Standardisation Office in collaboration with Finanstilsynet.

LOSSES RELATED TO USE OF ONLINE BANKING (figures in NOK 1 000)

Type of online banking fraud	2010
Attacks using malware on customer's PC (Trojans)	0
Attacks that exploit vulnerabilities in online banking applications (hacking)	0
Phishing (fraudulent attempt to obtain confidential information)	0
Other forms of online banking attacks	0
Other (thefts of code cards and other information)	2 398
TOTAL	2 398

As the statistics show, losses related to activity in Norway are still moderate compared to information on losses from other comparable countries. However, the card-related losses are substantial, and earlier estimates indicate that they are on the rise. It looks as though losses in Norway fluctuate somewhat in accordance with criminal use of new technology and the financial industry's establishment of countermeasures. The losses that take place outside Norway are significant. These can be based on information that may have been stolen in Norway and sent to a recipient outside Norway through the Internet. Online banking losses are still very low. In general, losses in 2010 were related to more traditional types of theft and not to web-based attacks.

4 The findings and observations of Finanstilsynet

Finanstilsynet maintains regular contact with financial institutions in a variety of ways, and has up-to-date information on the status as regards ICT issues. In 2010, there were numerous points of contact between Finanstilsynet and the financial sector, as will be seen in the following chapters. These consisted of inspections and interviews scheduled as part of Finanstilsynet's planned activities, but also of meetings arranged at short notice in response to information that has come to Finanstilsynet's attention regarding incidents and special trends.

4.1 Findings from IT inspections in 2010

Finanstilsynet maintained a high level of activity in connection with IT inspections in 2010. A total of 26 on-site inspections were carried out, in addition to 31 document-based IT inspections. The inspections targeted banks, insurance companies, various types of securities-related institutions, debt collection agencies, real estate agencies and several of the major ICT suppliers in Norway and the rest of the Nordic region. Under section 12, Outsourcing, of the ICT Regulations, Finanstilsynet has the right to inspect a supplier in connection with an inspection of the financial institution that has outsourced services to the supplier. Findings from the IT inspections show that some areas require special attention.

4.1.1 Testing of disaster recovery plans

Based on the results of IT inspections, Finanstilsynet has found that there are often deficiencies in the scope and quality of the testing of institutions' disaster recovery plans. The portfolio of IT systems is complex and based on services provided by several suppliers. The testing of a disaster recovery plan requires a type of end-to-end testing entailing the participation of all parties involved in order to ensure the desired functionality in a crisis. It is not sufficient that the ICT supplier conduct tests. The financial institution itself must also participate. If the system platform or supplier is changed, ensuring that the disaster recovery plan is adapted to a new environment can prove to be a challenge. The testing of disaster recovery plans on a new platform is often carried out too late.

4.1.2 Coordination of processes

Most institutions have established good, well-functioning ICT operational processes. Standards are generally applied, and ISO 20000 (ITIL), in particular, is a standard to which reference is often made. Through inspections carried out in 2010, Finanstilsynet has noted that while the individual operational process may function as intended, the processes do not communicate adequately with each other. For instance, the application development and management process staff may not ask for or share information to a sufficient degree with the change management, testing and capacity planning process staff.

4.1.3 The resource situation

Several of the solutions used in the banking and financial sectors in Norway originated at a time when IT architecture and programming languages were different from those used in development today. As a result, a large part of the portfolio of applications used by the financial sector is managed and operated by personnel who will be approaching the end of their working career in a few years' time. Few or none of the newly trained informaticians in Norway are interested in working with old, possibly dying, technologies and programming languages. Finanstilsynet has therefore seen a tendency for a growing number of companies to outsource these services to countries where there is better access to this type of personnel than in Norway. This could entail a considerable risk since the institution's responsibility for the services is weakened, while the operations are carried out by other personnel, who are often located far away and have to communicate in an unfamiliar manner. In the long term, this may increase the level of risk.

4.1.4 Risk and vulnerability (RAV) analyses

As in earlier years, Finanstilsynet sees that the quality of risk and vulnerability analyses is a recurring issue. Since Finanstilsynet introduced the current ICT Regulations in 2003, the industry has made great progress in terms of carrying out such analyses. A consistent problem in 2010 was the poor quality of RAV analyses dealing with companies' desire to outsource ICT services to countries outside the regions where such services have traditionally been outsourced, such as Sweden and Denmark. On several occasions in 2010, Finanstilsynet pointed out to supervisory units the importance of carrying out good, adequate RAV analyses. Finanstilsynet strongly emphasises that it is the responsibility of the individual supervisory units themselves to prepare good, comprehensive analyses.

4.1.5 Institutions' ICT expertise

As a result of outsourcing, institutions' own IT departments have gradually been changed, and expertise in the field of IT has been concentrated in a smaller number of human resources. The result in many cases may have been that it is the service provider who largely controls and determines the development of solutions and services for the institutions' portfolio of applications. This procedure can be appropriate if the service provider and the institution exchange information on and coordinate their strategies. Through its inspections, Finanstilsynet has ascertained that many institutions lack sufficient procurement competence to define requirements for and check the ICT products and services supplied by the service provider.

4.2 Interviews –institutions' own assessments

Finanstilsynet interviewed representatives of 13 financial institutions in 2010. Some of the interviews covered several institutions in the same group. The interviews were based on questions regarding what the institutions considered to be an ICT risk in the current year and in the future. When the replies were summarised and compared, it was evident that several of the institutions point to the same areas of risk.
The following is a summary of the institutions' assessments:

What does the institution consider to be the greatest risk(s) in connection with its use of ICT?

Logical errors in applications that result in an incorrect balance or accounting entry is one of the worst things that can happen.
Vulnerability in open networks and infrastructure is a risk. The threat of malware or viruses and online payment service fraud is a constant concern.
It is hard to find sufficient qualified personnel. Key personnel with a combination of specialised IT and business skills constitute a bottleneck and are used again and again in every project.
Mainframe expertise may become scarce as many IT staff approach retirement and new staff leave the company more quickly than was normally the case before. This poses a problem in terms of requisite skills.
Banks divide tasks up by entering into agreements with several different suppliers, and following up on agreements and coordinating deliveries is a demanding task, both administratively and technically. From the supplier's standpoint, multi-customer connections requiring the delivery of secure services to customers located in many different places presents a similar challenge.
Many financial institutions have a Nordic platform, and ensuring that IT applications are compliant with the rules in all the Nordic countries is a challenge.

What were the biggest ICT problems in 2010? And how were they identified?

Disruption of operations due to errors in applications, system software or infrastructure was a recurring problem in 2010. As a result of mergers, financial institutions have largely been forced to use a single supplier. Many institutions experience delays in deliveries from suppliers. Due to organisational changes and associated "noise", the quality of deliveries is poorer. There is a lack of expertise on Norwegian payment infrastructure among system developers in other Nordic countries who are responsible for managing applications for the Norwegian market.
Card skimming has been a problem. Offline payment terminals are used to procure cardholder data. Merchants and their service providers in Norway and abroad still do not comply adequately with PCI requirements.
Vulnerabilities in software products such as Adobe and Windows, and the requirement that it be possible to upgrade them rapidly by means of patches, constitute a risk.

What does the institution view as the biggest challenges in 2011 in terms of risk related to use of ICT?

For commercial reasons, high priority is given to accelerating the development of new products and meeting expectations as regards the delivery of new digital customer solutions that include services on mobile units. At the same time, information security related to these solutions must be safeguarded.
Dealing with structural changes and reorganisations while advancing product development is a challenge. Resources have to be shared between development and operations. Quality and security must be safeguarded. When projects are carried out, their potential effect on the infrastructure must be ascertained. Testing methods, including regression testing, must be refined.
Trojans posed a growing threat at the start of 2011. Organised crime targeting electronic payment systems must be monitored.
In many institutions, national and international activities are becoming increasingly integrated. This gives rise to a complex situation since systems must cover payment processes and account reporting for many countries with different sets of rules.
It is important to secure the stability and capacity of WAN networks between Nordic countries.

What does the institution consider to be important issues that must be addressed (by implementing measures) in 2011 with regard to ICT security?

Measures to prevent Trojan attacks have high priority.

Solutions to reduce payment card crime are important. Measures include preventing the misuse of stolen and counterfeit cards by reducing the number of offline terminals, improving communication with customers who may be potential fraud victims so as to block their cards more quickly, establishing even better teams of analysts, improving merchant training and promoting compliance with PCI standards (international card company standards).
Increasing the security of mobile units is high on the agenda. PCs can be encrypted, but that is not as easy to do with a mobile telephone. At the same time, more data is being collected on mobile telephones. A review is needed of possible security measures such as anti-virus tools, centralised administration, etc.
Parallel projects/system releases must be coordinated and quality-assured by means of improved testing and follow-up. Successful development and management require human resources who possess both business expertise and specialised IT skills. Communication between the commercial staff and the development staff regarding the interpretation of requirements as to format, coding, etc., is crucial. Global projects and ensuring a common Nordic level of security pose a challenge.

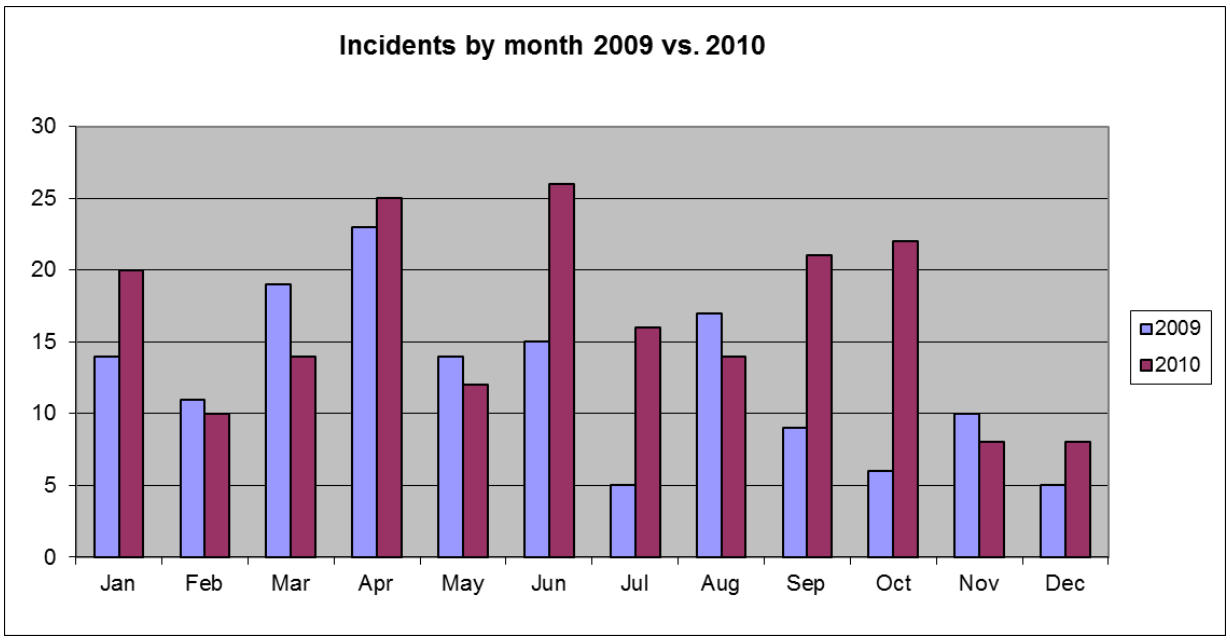
Other issues of concern to the institution and which may be of relevance for the institution's use of ICT and operational risk?

Security measures must be understood, followed up and actively supported at management level.
The complexity of market information is steadily increasing, in part due to the growing number of marketplaces (see more on this subject in section 2).
It will be important to develop a global understanding of local differences.
The backbone network (the institution's primary communication system) has to be replaced.
Real economic and political conditions can cause international unrest.

4.3 Reporting of incidents to Finanstilsynet

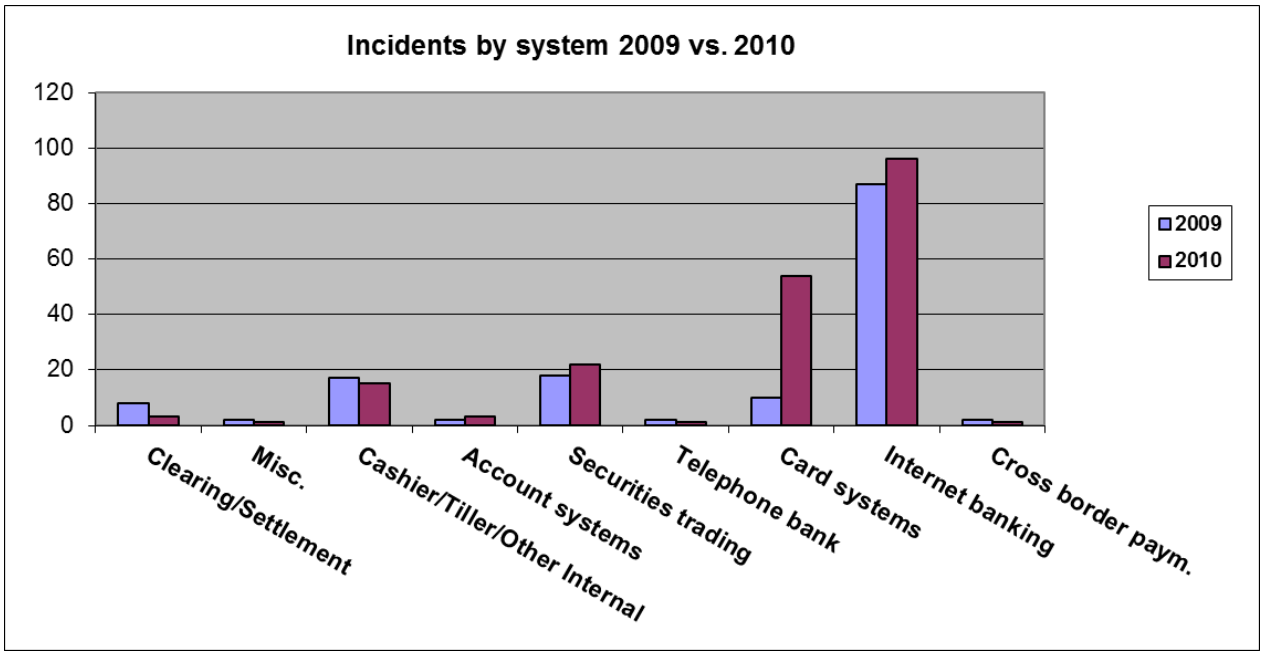
4.3.1 Incident reports in 2010

The number of incidents reported in 2010 rose by about 40 per cent compared to 2009. A total of 198 incidents were reported in 2010, 42 of which were related to ATM skimming. Banks still report the largest number of incidents.



Finanstilsynet follows up on incident reports in a variety of ways. In addition to the day-to-day follow-up, Finanstilsynet meets with major institutions to discuss nonconformity trends and the forms and level of reporting. Serious incidents are followed up particularly closely. These are often incidents related to fraud, new forms of security breaches or other incidents that have had especially serious consequences.

4.3.2 Findings from incident reports in 2010



The above figure shows the breakdown of incidents by business area/function.

Card transactions – vulnerabilities in banks' payment systems at merchants in Norway

The number of card-related incidents has increased. In 2010, Norwegian ATMs were subjected to serious attacks in which the content of the magnetic strip was unlawfully copied, a process called skimming. Over 40 ATMs out of a total of 2 200 were skimmed, and many

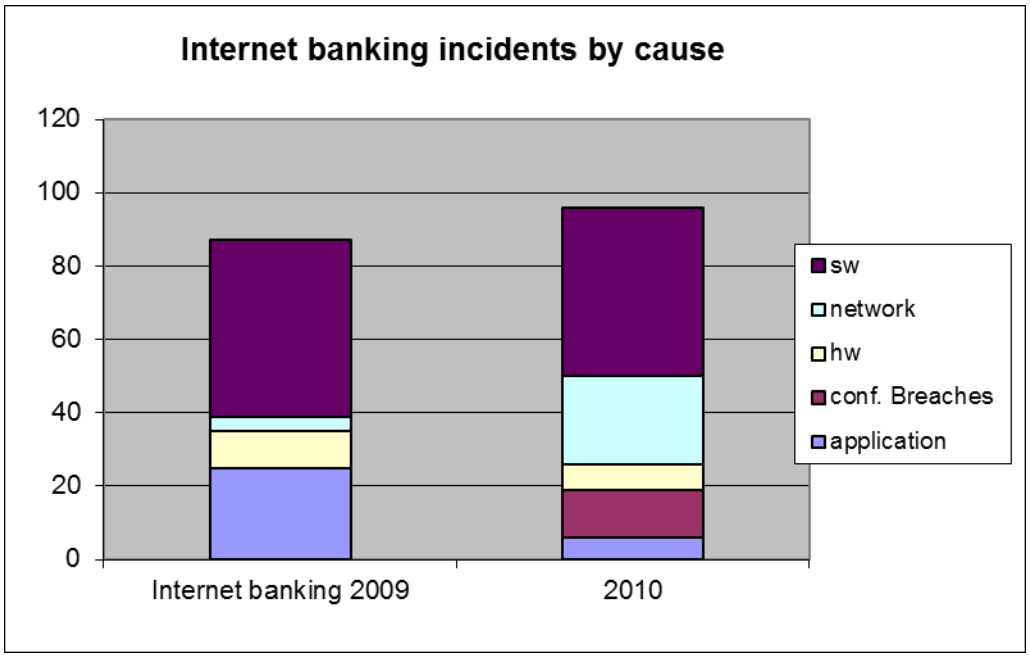
cards were exposed to potential misuse. The actual number of cards that were misused was far lower. New cards were issued to all the cardholders concerned. An important task in 2011 will be, in cooperation with BSK, Finance Norway and the banks, to ensure that relevant steps are taken to address this problem. A meeting forum has already been established for this purpose with the banks, both to secure relevant information and to discuss possible measures. The Oslo Police District has established a dedicated group at Sentrum Police Station, who are engaged in inter-county efforts to combat this type of crime.

Incorrect accounting entries/balances

In 2010 there were two incidents in which errors in the operational set-up resulted in duplicate transactions/reservations on customer accounts. These are serious incidents that it has taken considerable effort to remedy.

Online banking – vulnerabilities in the online banking service

The majority of incidents still occur in connection with online banking.



The above figure shows where the cause of the incident lies. In the case of SW, the reason for the fault is often that the SW has been set up 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 figure shows that system software is still the predominant cause of incidents. It still appears to be difficult to maintain a stable operating environment for online banking applications. The online banking services draw on the same limited pool of technical resources. Online banks are gradually providing a growing number of services that are usually connected to systems outside the online bank. A fault in one of the many services or in surrounding systems can reduce access to all or large parts of the online bank. Moreover, traffic and traffic patterns are changing, and SW parameters must be adjusted accordingly. This is a complex situation that requires a great deal of know-how and attention. Dealing with SW in complicated operating environments is a resource-intensive process in terms of both technical expertise, coordination and follow-up. This type of resource may become scarce. Traces of Trojan attacks on online banks in Norway were found in 2010, but no customers were defrauded. Large-scale attacks are taking place in many other countries, so it is important to maintain high focus on the online banking sector through inspections,

collaboration with industry organisations and individual institutions, and by implementing appropriate measures. A collaborative project has also been established with the National Bureau of Crime Investigation (KRIPOS) in this area. Trojan activities appear to be on the rise, and focus on this area was intensified somewhat at the start of 2011.

Incidents leading to breaches of confidentiality

There were several cases of confidentiality breaches in 2010. A total of 18 cases were reported in 2010, compared to just three in 2009. This applies to all types of financial institution. These incidents are not due to fraud, but are caused by operational errors, often due to what institutions describe as "human error", which have arisen in connection with system modifications. As a rule, this is due to incorrect programming, as a result of which a customer may gain access in certain situations to another customer's account online or receive an account summary that contains information on another customer, or personal identity numbers may be printed visibly on letters/envelopes. This type of information leak must also be reported to the Norwegian Data Inspectorate.

4.4 Outsourcing to countries other than Norway

Finanstilsynet is aware that several banks and other financial institutions have outsourced all or parts of their ICT activities to suppliers outside Norway.

A new situation arose in 2010 when the IT company EDB moved some of its operations to a company in Ukraine that is partly owned by EDB. Finanstilsynet therefore investigated the situation more closely. This investigation showed that no full formal contractual adjustment had been made of the functions that had been moved to Ukraine. Moreover, many of the banks had not carried out the risk assessment on which such contractual amendments are supposed to be based. Some banks had based their assessments on risk assessments carried out by the supplier, which were inadequate. In Finanstilsynet's assessment, the risk related to the relocation of functions was too high, and several matters subject to regulation were in breach of the rules.

Finanstilsynet explained its assessment in greater detail in inspection comments to the banks. It introduced a general measure in the form of Circular 14/2101 on the outsourcing of banks' ICT functions, which sets clear restrictions on outsourcing to areas which are described as high-risk areas, and which apply to specific functions/areas of banking activity. The circular is an explanation of Finanstilsynet's definition of acceptable risk in this area. In Finanstilsynet's view, both the banks and the supplier have taken account of and complied with the circular.

4.5 Questionnaire surveys conducted in 2010

4.5.1 Duty of notification – Section 3-2 of the Payment Systems Act

In the last quarter of 2010, a survey was conducted among the largest financial institutions on vulnerabilities related to payment services. The reason for the survey was that Finanstilsynet assumed that financial institutions were not adequately complying with their duty of notification. The result of the survey confirmed Finanstilsynet's assumption.

Finanstilsynet received 19 new notifications from five financial institutions in this period. Three questions were answered, with the following results:

1. Has the institution established any new system(s) for payment services in 2010?
   12 yes and 7 no

2. Has the institution developed a new version of payment service systems in 2010 that significantly affects other parties involved in the system?
   12 yes and 7 no

3. Has the institution developed a new version of payment service systems with significantly modified or new functionality in 2010?
   13 yes and 6 no

All the institutions replied in the affirmative to one or more of the three questions. Finanstilsynet has concluded that this survey has made the institutions more aware of what is naturally subject to the duty of notification. This will enhance the quality of the reporting, and help to reduce the operational risk.

4.5.2 Regulations relating to requirements regarding the design of ICT systems for members of the Norwegian Banks' Guarantee Fund

On 19 May 2010, Finanstilsynet laid down the regulations relating to requirements regarding the design of ICT systems for members of the Norwegian Banks' Guarantee Fund. The purpose of the regulations was to describe how the administrative board of a bank that has been placed under public administration and the Norwegian Banks' Guarantee Fund can rapidly and correctly pay out amounts equivalent to the amounts guaranteed by the Guarantee Fund.
To ensure that the banks have implemented the requisite solutions in their own ICT systems, Finanstilsynet asked the largest banks and bank groups to make a self-assessment of whether their systems satisfy the requirements set out in the regulations.
Based on the feedback from the banks, Finanstilsynet can conclude that most of the banks largely consider themselves to be in compliance with the regulatory requirements. One reservation was notified, concerning the third requirement of being able to "show a subsidiary ledger of the claims paid with funds provided by the Norwegian Banks' Guarantee Fund and indicate that the Guarantee Fund has subrogated the original depositor's claim against the bank". More time was requested to be able to respond to this question.
Furthermore, some banks have indicated that they will satisfy the regulatory requirements by 31 March 2011. Projects are currently being carried out, and the solution supplier has set a date for the implementation of necessary changes.

4.6 Incidents culled from international sources

It is interesting to note certain incidents that have taken place elsewhere in the world. A number of incidents that occurred in 2010 are described below.

4.6.1 The theft of data from a testing system in Cleveland, USA

On a number of occasions in 2010, data was stolen from testing systems in which real production data was used for testing purposes. On one occasion, the Federal Reserve Bank's

branch in Cleveland, Ohio, USA was hacked, and information from 400 000 credit and debit cards was stolen and offered for sale. The person who stole the data was a resident of Malaysia, but travelled to the USA to meet a buyer. In this case, the buyer was a federal agent who arrested the man after he had sold data from 31 cards for USD 1 000 per card.

4.6.2 The National Bank of Australia

In late November and early December of 2010, the National Bank of Australia had extensive problems with its ICT systems. According to publicly available information, the problems were caused by human error. Due to the error, none of the bank's customers were able to access their accounts to pay bills or use shop terminals. Inter-bank settlements were also affected. The clean-up after this incident was a very costly, laborious process as over 60 000 transactions were corrupted as a result of the incident.

4.6.3 An incident in DBS Singapore

In 2010, an incident occurred at DBS, one of Singapore's largest banks, which resulted in loss of access to ATMs, shop terminals and online banks for several hours. For Singapore, this is a more serious incident than in other countries because official guidelines require that if a bank offers this type of service, the services must be accessible on a 24-hour, year-round basis and must have the requisite infrastructure.

5 Identified areas of risk

Based on findings in connection with inspections, incidents, interviews with institutions and external national and international sources, a number of areas stand out as areas of particular risk, to which special attention must be paid in 2011.

5.1 Skimming attacks on ATMs

The skimming attacks on Norwegian ATMs that took place in 2010 were based on a different technology from the type that was used for skimming in the mid-2000s. While "digital" skimming was formerly used, an analogue skimming technology is now utilised. Measures have been put in place to prevent the further spread of this type of skimming attack. Losses were limited, not least thanks to the fact that illegal transactions were rapidly discovered and cards suspected of having been skimmed were quickly blocked. Nevertheless, there is no reason to believe that new forms of ATM skimming attacks cannot crop up.
Measures to prevent skimming are implemented at two levels:

- Physical protection of the ATM technology and of the site where the ATM is located
- Monitoring and analysis of transactions

5.2 Attacks on online banking services

Online banking services are attractive targets for fraud due to the direct access to funds. At the start of 2011, preparedness for Trojan attacks on online banks was improved. Highly qualified hackers are taking attack methods to a new level of professionalism and finding new ways of "selling" Trojan services. To successfully attack an online bank, the fraudster must have a place to which the money can be transferred, i.e. a beneficiary account. Various scenarios are created to obscure the information regarding the person receiving the money. The recipient can be a customer who has also been attacked without being aware of it; his account is used as a transit account and the money is automatically sent on to an account abroad. Attacks on online banks become particularly dangerous when different attack methods are combined, such as when phishing is combined with Trojans. In Finanstilsynet's view, banks in Norway devote great attention to threats against online banking, and collaborate both nationally and internationally on appropriate measures. It is important to give priority to this area of risk, which is evolving so rapidly.

5.3 Inadequate testing and verification of disaster recovery plans

Under the current rules, institutions must test their disaster recovery plans at least once a year, and the results of the testing must be documented. Institutions in the financial industry use ICT solutions that are complex, composed of many layers and based on deliveries from several different suppliers. Carrying out disaster recovery tests calls for specialised knowledge and resources. It is important to involve all the participants concerned. It is a laborious process, but it is the only way to ensure that preparedness plans will function in a crisis. It is hard to say when a disaster recovery plan has been tested sufficiently, but in

Finanstilsynet's view, there is room for improvement in this connection. There is probably a need for guidelines on this topic.

5.4 Lower-quality operations due to organisational changes implemented by ICT suppliers

In 2010, several mergers took place between major ICT suppliers. These mergers mean that there are now fewer suppliers and thus a greater risk of concentration and less opportunity for the customer to exercise influence. Mergers create turmoil in the organisations while they adjust, and this affects their operations. The Nordic dimension is increasingly dominant. Nordic groups must supply services to financial institutions throughout the Nordic region. Each of the Nordic countries has its own payment infrastructure and regulatory framework. Expertise is relocated and can be lost in the process, and is difficult to build up again because a person's knowledge of the payment infrastructure in another Nordic country is weaker than the person's knowledge of the structure in his or her own country. Several institutions have pointed out that this is a challenge. There is also a potential risk in the fact that institutions which move their operations outside Norway then become a branch in Norway. The host country cannot apply exactly the same instruments to a branch, and rules may be different in the parent country.

5.5 Lack of management and control in connection with outsourcing

There are risks associated with outsourcing, whether to a supplier in Norway, the Nordic region or more remote countries. Generally speaking, the greater the distance to the supplier, the greater the challenges related to ensuring adequate management and control of the outsourced services. It is therefore essential that the institutions themselves carry out the necessary assessments of risks related to outsourcing ICT activities. The risk assessments must cover both the operational risk per se, but also the country risk related to the country to which the activity is to be moved. The institution's management must ensure that the risk situation is dealt with in a satisfactory manner. Institutions must take account of the possibility of increased operational risk as a result of outsourcing, and counter the risk by taking relevant action. These are areas in which Finanstilsynet, as part of its work, has made banks aware of deficiencies.

6 Further follow-up by Finanstilsynet

6.1 General

The main focus of Finanstilsynet's work on inspection of ICT and payment services is on risk and vulnerability. Follow-up of this takes the form of:

- ensuring that IT inspections takes place on a scale and level of detail that allows Finanstilsynet to obtain a realistic picture of how institutions safeguard their ICT activities, managing risk and complying with regulations.
- ensuring registration and follow-up of information from reporting on ICT incidents by e-mail to: hendelse@finanstilsynet.no and an overview of an area that is crucial to the stability of the financial market
- that through RAV analyses and other work, Finanstilsynet obtains information that enables the most accurate understanding possible of risk in the area
- to focus on payment systems through proactive measures, but also through inspection activities and other follow-up, to ensure compliance with regulations and that payment takes rapidly and efficiently
- to ensure compliance with existing rules and regulations and ensure appropriate development in the light of the risk situation
- contribute to establishing areas for cooperation on problem areas where sharing of information and discussing of joint efforts is important

6.2 Current efforts focused on risk areas

6.2.1 Skimming

Finanstilsynet is monitoring banking organisations' work on skimming and keeping up to date with technological developments, threats and vulnerability in the area. Finanstilsynet aims also to secure necessary information on incidents and losses as a basis for assessing potential consequences and measures to ensure acceptable risk management so as to limit any consequences for society. Confidence in payment services is important.

6.2.2 Online banks

Finanstilsynet is monitoring online banking systems closely. It is important that banks have new security measures available when the consequences of attacks become too great. Close contact has been established with BSK, collaboration with BSK's Online Banking Committee (Nettbankutvalget) and individual banks. Finanstilsynet has also established close collaboration on the Nordic and international level with other supervisory authorities in this area. This helps to ensure a broad range of information on criminal attacks against online

banks in other countries and about the methods that are used. Formal collaboration has also been established with NorCERT, which assists in monitoring of the internet and is an important partner when it comes to measures in networks outside Norway.

6.2.3 Disaster recovery plans

It is essential for society to have faith in disaster recovery plans. Sufficient testing to verify that the contingency system functions is necessary. Finanstilsynet will therefore follow up this important area through its supervisory activities, direct contact with individual institutions and a new questionnaire survey in 2011.

6.2.4 Management and control in connection with outsourcing

Work is in progress on this issue, which covers both outsourcing generally and offshoring in particular, both through possible regulatory amendments and the drafting of special guidelines to Section 12 of the ICT regulations on outsourcing. Finanstilsynet will monitor developments closely through 2011, and at the same time cooperate with industry organisations and authorities in other countries to ensure harmonising on best practice and international standards in this area.

6.3 IT inspections

Finanstilsynet continues to give priority to IT inspections. At the same time, further developing the inspection system so that relevant problems and vulnerabilities can be identified remains a challenge.
In 2010 the existing inspection system was improved and new inspection modules established. Finanstilsynet is engaged in implementing a methodical classification of the grade of maturity of institutions' ICT organisation. Work to establish a separate transaction testing module is also in progress.
In 2011 guidelines to the ICT regulations will be drawn up, for example for Section 2, Planning and organisation, Section 5 Security, Section 10 Continuity requirements, Section 11 Disruption of operation and disaster preparedness and Section 12 Outsourcing.

6.4 Handling emergencies

As from 1 June 2010, Finanstilsynet is responsible for the secretariat and chairmanship of the Contingency Committee on Financial Infrastructure (BFI). Finanstilsynet will work actively to maintain and further develop this committee in collaboration with Norges Bank and the other participating organisations. Important responsibilities are on-going follow-up of incidents, financial infrastructure stability and holding of appropriate emergency preparedness exercises.

6.5 Handling of ID theft

The Data Inspectorate and Finanstilsynet will continue their collaboration on ID theft. The Norwegian Centre for Information Security (NorSIS) is also taking part in this work, so that future work can build on the studies already made in this area. The work is aimed at identifying leakage sources, analysing how the information can be used in attacks on the

financial sector, and on finding effective means of stopping leakages and reducing opportunities for misuse of stolen information. There will be increased attention to and follow-up of merchants' compliance with the regulations. An inadequate understanding of security by merchants generally may lead to security deficiencies in connection with the execution of payment services. Finanstilsynet will also follow up the new merchants offering banking services to help impart a better understanding of law, liability, security, communication and training.

6.6 Information and communication

Interaction and trust between Finanstilsynet and the institutions that are subject to inspections is essential. A day seminar is planned in 2011 on risk management associated with ICT-vulnerable areas and payment services that are subject to attack from criminals.
Finanstilsynet is participating in a number of different forums as part of its work with ICT security in the financial sector. Some of the more important ones are: the Information Security Coordination Council (KIS) and the Contingency Committee for Financial Infrastructure (BFI). Finanstilsynet also cooperates directly with Norges Bank, the Norwegian National Security Authority (NSM), the Data Inspectorate, the Norwegian Post and Telecommunications Authority and industry organisations.
Finanstilsynet also co-operates closely with the other Nordic supervisory authorities, and participates in international IT supervisory co-operation (Information Technology Supervisors Group) with a European sub-group. There is similar participation in the work on international standardisation in the groups for banking and security standards, standardisation of electronic signatures (ETSI ESI) and in the International Federation for Information Processing's (IFIP) security group.

6.7 CoMiFin

CoMiFin is a research project financed by the Seventh EU Framework Program. Deliveries from CoMiFin may help banks to link together in a practical manner IT resources among a collaborative, distributed network of agents. The system contains functions for defining and measuring service quality, resource measurement and allocation/release of resources, and for analyzing large quantities of data. The system has been fully developed and tested. It can be used to detect threats and vulnerabilities (Denial of Service attacks, Man in the Middle attacks etc.) The system can also be used for joint development and testing platforms for banks wanting to cooperate in systems development, for example a joint application for reporting to the authorities. However, it will be up to banks and other financial institutions to independently adopt a system such as this. In the meantime it is positive that research and development is being carried out in this risk area.

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