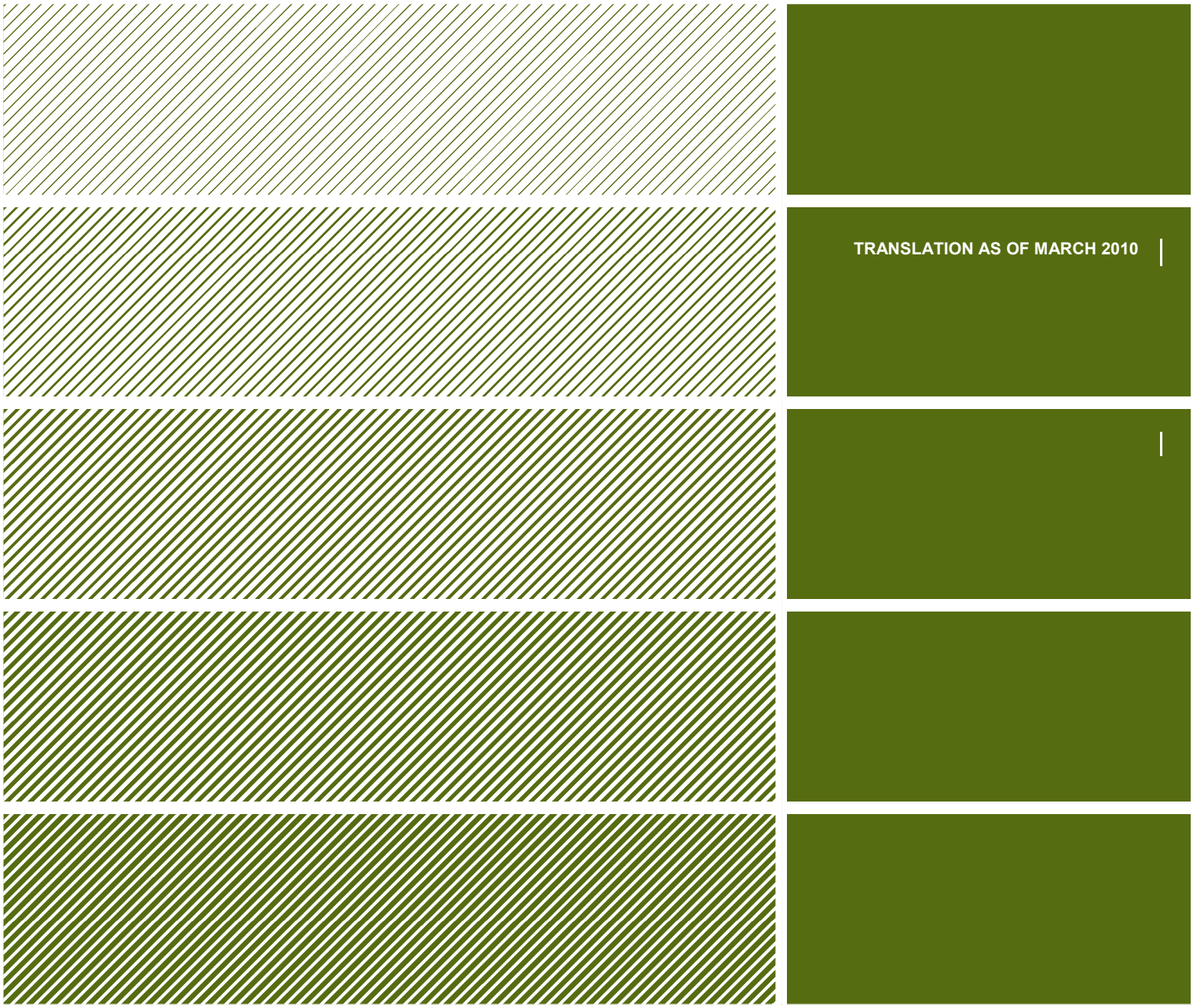
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Report

Risk and Vulnerability Analysis (RAV) 2009

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



TRANSLATION AS OF MARCH 2010

Contents

1 Introduction

Finanstilsynet (the Financial Supervisory Authority of Norway) performs an annual risk and vulnerability analysis (RAV analysis) of the financial sector's use of information and communications technology (ICT).

The objective is to be able to see the entire financial sector as a whole, based upon data from the information that Finanstilsynet has acquired from the individual institutions throughout 2009. The information has been acquired via inspections, interviews and event reports. In addition, national and international sources have been utilised. Through the analyses and the data that Finanstilsynet has access to, the trends in the risks associated with the financial sector's ICT systems are being followed over time. This makes it possible to identify problem areas and to initiate measures transverse to any individual institution.

The report aims to give a picture that is as correct as possible of the risk situation and thus be a useful source of information for individual institutions that are working with their own risk situation. One important goal in this context is the use and presentation of quantitative data as useful information when it comes to being able to see both the scope and the trends of identified problem areas.

The RAV analysis can also give indications of how the sector complies with applicable laws, regulations, industry-related codes that have been adopted and the relationship to the use of standards and industry-related norms.

Event reporting, which was established in a voluntary arrangement beginning in November 2007, has as at 1 December 2009 started being obligatory reporting through changes in the ICT Regulations.

In the RAV analysis for 2009, we will also present the results from Finanstilsynet's work with ICT infrastructure and analysis of sets of problems related to the moving of ICT tasks outside of Norway. The intent of this work is to identify possible deficiencies in administration and control and to identify areas of risk and vulnerabilities in technical infrastructure that require measures to be taken.

2 Technology and trends

There are many general trends in the financial sector that influence the use of ICT by institutions. The FSA has identified the following areas as being important for understanding their effects on operational risk.

2.1 Cloud Computing – ICT operation in the network cloud

Cloud Computing (CC)[1] is a new way of conducting the operation of Internet-based services. CC supplies the computing power, bandwidth and storage capacity somewhere in the network cloud as opposed to traditional data centres that manage operations for different customers divided into separate partitions. The CC supplier provides access to a server farm that can perform parallel processing, multiplexing and data storage for many different customers on an order of magnitude that ordinary data centres find difficult to compete with. The sum of the computing power makes it possible to scale the use of the computing resources more appropriately, with the customer paying according to the so-called *pay-as-you-go* principle. By paying for the actual use, it may be less expensive for the customer to use CC than to scale their own capacity as per the peaks, possibly running the risk of underdimensioning their own capacity and experiencing displeased customers. Similarly, the financial risk may be reduced when new services are offered that have usage patterns that one is not acquainted with in advance.

Three different models are differentiated between for CC, each with different degrees of standardised services. At one end of the scale, CC is offered as almost pure computing power in the form of a CPU, storage locations and IP network (*Cloud Infrastructure as a Service*). The model places no limitations on the type of application or software that can be operated in the cloud since the customers look after this themselves. On the other hand, CC cannot fully offer automatic solutions for scalability and reserve capacity solutions because the replication and consistency controls for the data are application-dependent.

On the other end of the scale, CC can be found based on web applications built on a traditional 3-layer model with clear separations between the layer for processing and the layer for data storage (*Cloud Service as a Service*). The customer uses the applications through a thin client, often a web browser, and the customer only has control of this layer. The model actually poses stricter requirements for application standardisation, including data storage. In contrast, this brings about a predictability that makes it possible for CC to offer advanced mechanisms in order to ensure scalability and availability.

In the middle of the scale, there is another model that is a cross between the two models mentioned above. The user can to a certain extent select the programming language and tools for the applications, but cannot control the underlying operating system or the environments the applications run in. CC can offer automatic configuration and scaling in the cloud, however the user must provide some specifications with the applications in order for this to be possible.

[1] National Institute of Standards and Technology (NIST): http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

CC can contribute to transferring risk from the owner of a service to the supplier of the service, because users of CC are able to secure predictable operation by relying on the elasticity in the accessibility of resources and adaptations to capacity that CC offers. Furthermore, CC can provide economies of scale in the form of special competence in machines, software, networking and security that it may be difficult for a smaller company to have by itself.

The European Network and Information Security Agency (ENISA) has issued a report in which they assess the risks of using CC[2]. The first risk they address is the risk of a loss of governance, i.e. administration and control. This is a risk that one must be willing to assume to a certain degree if one wishes to reap the benefits of CC.

The next risk ENISA addresses is the risk of *data lock-in*. The issue is what guarantee customers have of being able to retrieve their own data when they wish to switch operations service suppliers or if their operations service supplier goes bankrupt or is affected by other events that knock the operations service supplier out of operation. In order to compensate for the risks, customers must initiate measures to secure ownership and control of their own data. As the technology appears at the moment, there are a number of risk areas that are relevant if financial institutions are to begin using it. Finanstilsynet is not aware of any financial institution in Norway that has placed this technology into service.

CC is viewed as becoming one of the great innovations in computer science in the next few years. The technology is still not mature and substantial development remains. Finanstilsynet is not aware of institutions in the financial sector that have implemented this concept. Since the concept is not mature as a technology, this is also an area that poses challenges in relation to institutions carrying out RAV analyses. Furthermore, compliance with present regulations with respect to CC can also pose a challenge to these companies.

2.2 Infrastructure

2.2.1 Introduction

Financial services are to an increasing degree automated and taking place in real time in an end-to-end electronic interaction between the parties involved. This is made possible through the technical infrastructure.

The electronic transaction chains are characterised by their being automated and occurring in real time – the customer is serviced completely ”then and there”. The electronic transaction chains are continually becoming more comprehensive and it appears that this trend will continue in 2010. One example of this might be the use of BankID when signing electronic documents, together with offers to the customer for the preservation of documents in electronic archives. Many of the transactions are handled in real time with the consequence that if systems are not available, such becomes quite visible to the users.

[2] ENISA: Cloud Computing: “Benefits, risks and recommendations for information security” http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/

Because the automated, electronic financial transaction chains are becoming longer, the complexity and thus risks are increasing that errors will arise in one of the many links during the process. Errors in a link may cause a transaction to be unable to be initiated or further processed, and cause it to be declined. The customer is unable to execute the payment transaction in a timely manner and is entirely beholden to the supplier of financial services and its ability to re-establish the service.

2.2.2 Maintenance

The global financial crisis may cause a dearth of investments in critical infrastructure in individual sectors. Critical infrastructure is being impaired due to age and ”wear”, while requirements for services and performance are increasing. Outdated systems are being ”bandaged”, which can lead to further weaknesses. Experience indicates that access to power, water supplies, older generations of computing systems and transport infrastructure are vulnerable areas.

2.2.3 New channels

Growth has been seen in 2009 of new channels for financial services. Mobilbank and BankID on mobile telephones are examples. Due to a number of reasons, this is a positive contribution to the distribution of such services.

Firstly, the services become more robust in that there are now more ”paths” from the customer to the bank. If the landline telephones fail, customers can in certain instances use mobile banking instead.

Secondly, this gives the possibility to secure authentication from the customer. The risk of so-called phishing can be reduced. An example of phishing is a fraudster presenting a bank customer with a false login page, in order to then steal the customer's identity attributes. Such a procedure is not possible if the identity attributes are sent over the mobile telephone network. For the thief to be able to acquire the customer's electronic identity attributes, the customer must then be able to eavesdrop on both the Internet session and the information that goes over the mobile telephone network. This is a significantly more complicated attack scenario.

New possibilities, such as direct mobile telephone banking, SMS banking, payment cards with RFID technology, general authentication and signing of documents, may present new vulnerabilities. The complexity will be increased with several of the services being able to make use of multiple channels, for example SMS, bluetooth and RFID technology, multiple operating systems and new protocols.

Standards are lacking for mobile services in general and for mobile banking in particular. ISO is working with defining requirements for mobile banking in relation to the work of other standardisation organisations and in relation to services other than payment, however this is turning out to be challenging. Chips are currently perceived to be a secure technology, however the chip must communicate in unsecured mobile telephones for new, relatively untested channels and user interfaces. In addition, there are the contractual challenges of responsibilities for different services from different suppliers on the same mobile telephone.

2.2.4 Operation

In the area of ICT development (design, prototyping, coding, test) efficient and secure methods and tools have been introduced in recent years, for example .Net and working methods such as Scrum and Lean.

A number of new, customer-operated services have been produced and the expectation is that these will be available at all times (24 hours / 7 days / 365 days). This stream of newly developed services must be operated with high requirements for availability and with many interdependencies, long continuous process chains and likewise for the dependencies. In the area of operation, the possibilities for rationalisations have been more limited than in the development area. Due to this, ICT operation has become a much larger challenge in relative terms than in previous years. The challenges are multifarious.

The long transaction chains make for dependencies. With one link in the chain not functioning as presumed, the result can be the entire service becoming unavailable.

A number of programmes and operating services comprise the execution environment that the service is dependent upon: operating system, web server, application server, certificate services, network services, etc. The programmes have a number of parameters that must be properly set, maintained, renewed and tuned in light of changes in loads, operating environments, new versions and security updates. This jigsaw puzzle requires meticulous follow-ups and a good overview. Hence it is important to the extent such is possible to be thorough in the development, maintenance and operation in order to ensure availability, confidentiality and integrity in the solutions.

2.2.5 Protection of customer data

The customers will to a continually increasing degree be gaining access to banking support systems. In this context, the banks have an increased focus on protecting and controlling data within the domains of the banks. IPsec is a tool for achieving this. IPsec is a protocol that, among other things, is utilised to protect insight into the machine-to-machine communications with the use of encryption. Individual banks have plans to introduce access controls for machines in the network with the use of the IEEE 802.1X protocol.

2.3 Internet crime

Several areas of Internet crime have increased in 2009. In recent years, the number of vulnerabilities in applications has been far higher than for operating systems. The attacks that attempt to exploit these vulnerabilities follow two paths – password breaking and attacks on web applications. SQL Injection, Cross-site Scripting and PHP File Include attacks continue to be the three-most common as regards compromising websites and their applications. Automatic programmes cause it to be relatively simple to identify and exploit vulnerabilities in web applications on a large scale.

In the autumn of 2009, the American organisation named the Center for Strategic and International Studies published an updated version of Twenty Critical Controls for Effective

Cyber Defense.[3] In it, cyber criminals and security experts provide a collective expression of important control measures.

2.3.1 Client programmes that are not security-updated

So-called ”Drive-by downloads” are comprised of malicious code that is downloaded via websites that the user visits. One example of this is an advertisement that sits on web pages and contains malicious code.

The code infects the user's PC and exploits vulnerabilities in the programmes that are executing there in order to acquire increased privileges. Some are such that the user does not even need to open the document that has been downloaded. The user's infected PCs are used to spread the infection and compromise other internal computers and sensitive servers that are believed to be protected against unauthorised external access. The attacker's goal is to steal data. Within this context, the attacker installs backdoors that the attacker can use to enter the PC on later occasions.

The attackers continue to exploit the vulnerabilities by tricking the user to open documents sent by e-mail or by infecting web pages with links to documents that exploit the vulnerabilities. By exploiting vulnerabilities in the website's web content management system, the attackers can automate the infection process and impact an extreme amount of systems in the course of a few hours. Attacks that exploit vulnerabilities in Adobe have increased in 2009 after it became clear to the attackers how easy it was to exploit the vulnerabilities in order to gain control over a machine.

Java scores quite high on the list of vulnerabilities. Java is widely utilised in web pages as applets or as applications, and Java traditionally has been tardy with security updates. And until recently old, vulnerable code was not removed, with the consequence that malicious software was able to make use of it, even after updating had been performed.

For a more comprehensive list of the relevant vulnerabilities in widely used software, refer to Qualys’ list of the top 30 current vulnerabilities,
see http://www.sans.org/top-cyber-security-risks/.

2.3.2 Websites that are vulnerable

Attacks against web applications comprise more than 60 % of the total attacks. The vulnerabilities are exploited to turn websites that the user perceives to be secure into malicious websites. Web pages from these websites will then contain code that exploits vulnerabilities in programmes that run on the user's PC. Vulnerabilities in web applications such as SQL injection and Cross-Site Scripting in open source code as well as specially developed applications comprise more than 80 % of the vulnerabilities that are detected. Despite a large number of attacks and much coverage in the press, it is very far from all websites that actually scan for common vulnerabilities. They thus can easily become tools in the hands of criminals, and indirectly harm the website and customers, who at the point of departure trust the website.

[3] http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

The media has focused on credit card and national identity numbers being disclosed. However still more valuable data is being stored and can also leak out. The significance of protecting web applications against SQL attacks is quite important.

Cross Site Scripting is a recurring error in web applications. The pages for a website that the user has defined as secure turn out to contain a malicious Java Script from external websites that the trusted website co-operates with. The pages have functions that reflect code from such external websites, or they have links that fetch pages which in turn contain malicious code. Websites should to an increasing extent take the total responsibility for all code that, directly or indirectly, runs in a user's browser in consequence of the user fetching a page via a website.

2.3.3 Session security

Access to online banks is predicated upon the users identifying themselves and being authenticated before transactions may take place. One of the large challenges with respect to communications over the Internet is maintaining the connection between the merchant and the authenticated user during the entire session, such that transactions that the user performs during the course of the session may be uniquely associated with the individual concerned. Advanced trojans exist that are capable of altering the data a user registers on their PC and at the same time changing ”receipts” that come from the bank in a manner such that the false transactions do not become visible.

The merchant has the responsibility for programming its service such that session security is looked after. A number of techniques are used in this regard. Many banks require re-authentication in connection with each transaction. A number of banks utilise sequence numbers; if traffic comes out of sequence, then there is a reaction.

2.4 Methods for theft of personal information

Identity theft is increasing both nationally and internationally. Organised criminals are behind many of the thefts. The problem is being addressed from a number of quarters. Finanstilsynet is co-operating with other organisations both in Norway and abroad in order to survey how operational risks are affected by identity theft.

2.4.1 Where personal information is found

Identity theft is to steal, copy or in some other manner acquire personal information for later exploitation. On the Internet, with the assistance of some types of personal information, one can acquire information that is more payment-related such as a national identity number. Access to customer information of financial institutions may occur via vulnerabilities connected with:

1. Information that is shared between a customer and bank, for example a PIN or fingerprint.
2. Input equipment such as PIN keyboards and payment terminals
3. Protocols for transferring confidential information
4. Networks into merchants and financial institutions

5. Servers and computers at merchants and financial institutions
6. Procedures connected with the implementation, operation and use of systems and applications.
7. Acquiring sensitive information by manipulating people into giving it voluntarily
8. Disloyal operators internally within the companies

Fraudsters who do not have the expertise to exploit a person's or company's online bank have other possibilities, for example via access to servers at websites where information is stored about customers. Such websites, for example hotel chains, have agreements with credit card companies enabling them to insert reservations into their customer accounts after they have ordered an overnight stay. Finanstilsynet has seen examples of companies also retaining payment information after a purchase has been carried out. There are often limited controls on the security of the servers for websites, even if these must be encompassed by relevant PCI standards. Fraudsters thus often have ample time to research such servers where they may acquire information necessary to conduct transactions at sites where the card number, expiration date and CVC code are sufficient information for making payment.

Identifiers closely associated with the payor, such as a national identity number or fingerprint, strengthens the probability that it is the proper person who is initiating a payment. At the same time, it creates greater problems for the victim if these identifiers are abused than if a PIN code falls into the wrong hands.

Identity theft in 2009 has been particularly associated with different types of *skimming* (equipment for reading magnetic strips). In addition, information tapping from networks and bank data centres is a real risk.

2.4.2 Attacks against bank data centres

Previously, it was thought to be very difficult to steal encrypted PIN codes from a *hardware security module* (HSM) and decrypt the codes[4]. Such attacks can now be carried out in practice.

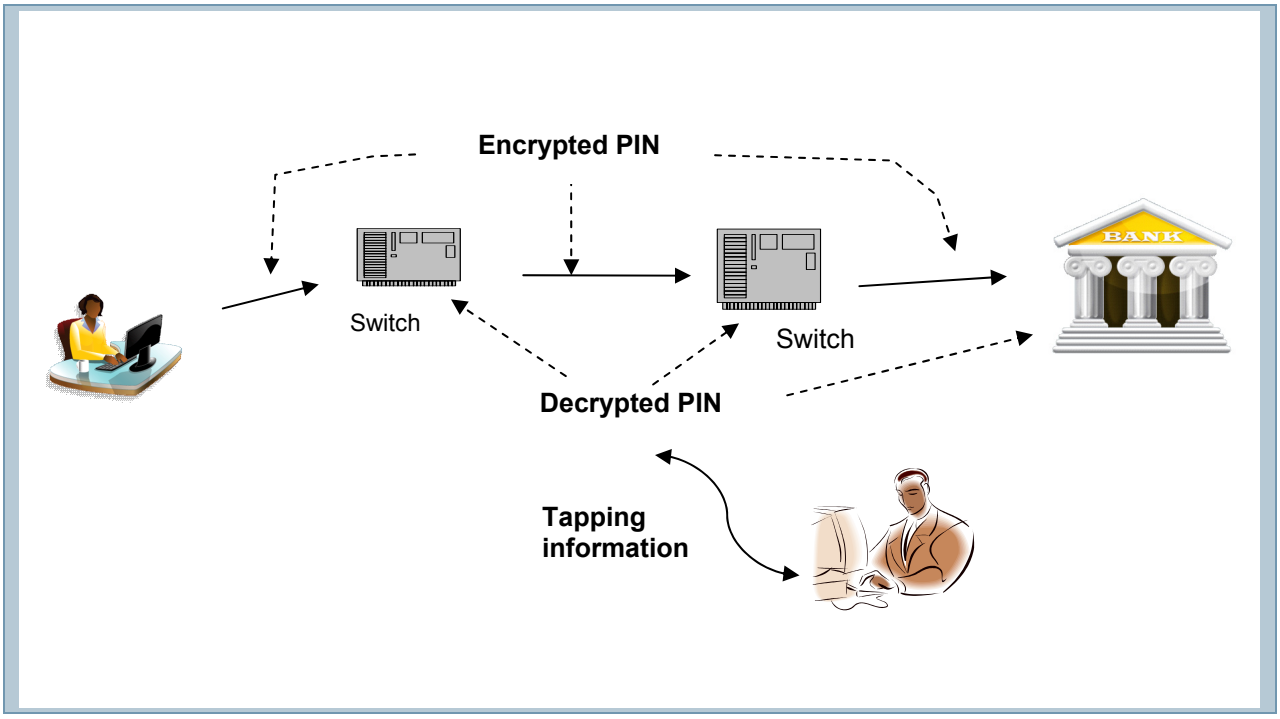
An HSM is a physical unit, and this often is the core of a company's secure infrastructure. It stores and processes, among other things, encryption keys with associated certificates, PKI and passwords. HSMs were developed in order to be able to be used by many types of customers in many countries. This means that they are all made with a number of functions that not everyone needs. A poor implementation of an HSM may be exploited by an intruder to bypass the security barriers.

HSMs are configured and administrated differently, often by suppliers who are not directly related to a bank. With respect to the PCI standard, PIN codes must be encrypted during transfer. However, a PIN may pass through many HSMs across several types of networks. At each switch, the PIN code must be decrypted and re-encrypted with the right key for the next step towards the destination location. With the manipulation and exploitation of vulnerabilities in standardised programmes for user interfaces, Financial PIN Processing API and poor implementations, fraudsters can fool an HSM into producing master keys for the

[4] The unbearable lightness of PIN Cracking, http://www.arx.com/files/Documents/The_Unbearable_Lightness_of_PIN_Cracking.pdf

system. When central components have been compromised, it becomes trivial to decrypt a PIN or password.

Chart 1: Encrypted and decrypted PIN



Vulnerabilities in the configuring of HSMs are also relevant in Norway, and especially where this is performed by suppliers who perform work for many companies with different requirements.

3 Findings and observations of Finanstilsynet

3.1 Important findings from IT inspections

In 2009, 22 on-site inspections were performed, 21 document-based IT inspections and 165 ICT events were reported about, where subsequent follow-up meetings were conducted. Furthermore, a total of 16 interviews were conducted with participants in the financial sector. In addition, Finanstilsynet has continued the work that began in 2008 with surveying the ICT infrastructure in the financial sector. Extra attention has been dedicated in 2009 to outsourcing in countries outside Norway.

3.1.1 RAV analyses

Finanstilsynet has pointed out deficiencies in the risk analyses by companies of their own ICT activities. The risk analyses often do not entirely cover a company's ICT activities. This is often due to deficiencies in the manner of approach by the companies in ensuring that the RAV analyses are complete. The analysis must encompass application development, operation, security, organisation and procedures, and in addition have participants who have competence in these areas. Furthermore, risk analyses should encompass assessments of suppliers with agreements and deliveries and the suppliers' own RAV analyses. Some RAV analyses lack adequate follow-ups. It is important that the RAV analysis be a living document where identified risks are regularly followed up.

3.1.2 Outsourcing

As mentioned above, many countries have outsourced operations to an ICT supplier in Norway or another Nordic country. The trend is for the ICT suppliers to further outsource certain services to suppliers in low-cost countries far away, so-called *offshoring*. The companies are to a varying degree and in different manners informed of such outsourcing to third-party suppliers. Plans may be presented as internal changes to an enterprise and in certain cases not show the actual content, namely that data is being processes in other countries with other legal codes, which may have an effect on the Norwegian operation. Financial institutions in Norway are responsible for their own activities, however they often become a passive recipient of information from the operations service supplier concerning plans for outsourcing to third-party suppliers. It is the financial institution that is responsible when the services are outsourced, ref. among other things the ICT Regulations. Such situations require the attention of the institutions and it is natural that the conditions would be reflected in the institutions' own RAV analyses. Finanstilsynet has devoted attention to the same situations in its supervision of the ICT suppliers.

3.1.3 Disaster recovery solutions and the testing of such

Disaster Recovery (DR) solutions and the testing of such continue to be a relevant area. Many institutions prioritise the establishment of alternative operating locations, however some companies are lacking sufficient testing of their DR solutions. This is an area where an institution's own solutions cannot be assessed in isolation from the solutions of the ICT suppliers. The institution must ensure the total preparedness of reserve solutions both for

operations that are handled in-house as well as operations based upon deliveries from the ICT suppliers. The DR solutions will thus require tests many different places in the chain. Even with smaller institutions, it is important to test the DR plan in order to detect defects in the planning and to bring about remediation of the defects before an actual disaster occurs.

3.1.4 Configuration overview

In the large institutions, through the IT inspections, questions are posed concerning whether they have a satisfactory plan for securing updated overviews of all configuration elements and their interrelationships. Such information is often collected together in what is called a Configuration Management Database (CMDB). A CMDB can be labour-intensive to establish, but it gives back benefits once it has first been established. Automated coupling between elements that in one or another manner are dependent upon and can affect each other can contribute to making it possible to perform change management with fewer errors. However, such overviews must be continually updated in order to have a reliable effect. Many events continue to be caused by unanticipated side effects of changes.

3.1.5 Administration and control of ICT activities

Finanstilsynet's remarks from an IT inspection performed in 2009 are related to the administration and control of the institutions of their IT activities. The ICT strategy of an institution should support the institution's business strategy, simultaneously with the ICT strategy is being operationalised through the ICT processes and defined measures. The strategy often seems to have become detached from how the ICT work is actually performed. It is not of much help to have a long list of security requirements when a fundamental security architecture has not been implemented in the organisation.

The business operations of the financial institutions rest upon extensive use of ICT systems, both administratively as well as for the execution of all types of financial transactions. This brings about a high level of fixed costs, where cost reductions must to a large extent occur by reducing unit transaction costs, which in turn increases the interest in participating in larger operating units. This trend gives rise to increased organisational and technical complexity that can cause new risk areas to have to be developed.

These problems have emerged in, among other things, on-site inspections through the detection of sometimes lacking competence and emphasis on central areas within the administration and control of ICT activities. At the same time, organisational areas of risk have been detected in how the relationship between the business strategy and ICT strategy must be implemented and function in the best manner possible operationally.

Such areas of risk may have their causes in the following:

- The business areas and ICT areas of the financial institutions have different drivers. The former is income and customer oriented, whereas the latter is production and cost oriented. In order to be able to detect areas of risk, it can be necessary to allocate resources for investments that will not necessarily show themselves to be income-related in either the short or long run. This form of self-insurance by being able to avoid future operating problems will not be visible because alternative costs will not arise in the future. In consequence it is necessary to have developed and visible

competence in operational risks on all levels of the organisations of these institutions.

- Financial institutions that have entered into strategic co-operation agreements with operating units that in turn have outsourced the operation and administration to specialised ICT companies have a potential operational risk. The responsibility for maintaining the requisite order-placement competence always lies with the institution that has the licence. Nevertheless, it is being detected that critical competence is not being maintained in the belief that such is being covered by the co-operating operating unit and due to goals for reducing costs internally.

- For the financial industry in Norway there is a clear concentration risk connected with industry having few data centres to choose between when alternatives for ICT-related issues have to the assessed. This in itself can contribute to selecting suppliers that make use of offshore resources to deliver ICT operations. In addition, the different institutions are to a large extent tied to established, older core systems with histories dating from previous co-operation structures, and which the data centres now own. This can affect the possibilities of the institutions to change suppliers for these types of services.

- In connection with the predominant use of payment cards and the associated payment terminals we have in Norway as well as the increasing threats of criminal attacks on such, it is purposeful to have a central register for payment terminals. The banking industry has established such a register in 2009 containing as much information as possible in order to be able to impede future criminal attacks in this area. If attacks will be made on such terminals, it will be significantly easier to diagnose measures through the use of such a central register.

3.2 Self-assessments of the institutions

Finanstilsynet conducted interviews with 16 institutions in 2009. The purpose was to obtain the assessments of the institutions of their own security situations.

The questions that were reviewed are given below together with a summary of the answers.

1. What does the institution see as the greatest risk(s) in the institution's use of ICT?
Even though the angle of approach is a bit different in the different institutions, many of them mention that a lack of competence is one of the largest risks connected with their use of ICT. When a number of services and products are automated in consequence of new technological possibilities, the requirements for competency also increase in still new areas. This involves areas such as system development, both in their own as well as in the supplier's organisations, order-placement competence and competence in ICT operation. The automation of products and processes is causing a detailed understanding of the business to disintegrate. One trusts completely and fully in the ICT systems.

2. What have been the greatest problems in the ICT area during 2009? What is the basis for being able to identify them?
Many institutions have experienced customers being subjected to one or another form of ID theft in 2009. The most common has been the theft of card data. A large theft of card data collected in Spain in 2009 caused many cards to become compromised, including in this

regard also cards belonging to Norwegian customers. Many Norwegian banks have distributed new cards in 2009 to a significant number of customers as a risk-reduction measure. The institutions mention in this connection that getting information from the international card companies is a problem. Furthermore, cards with magnetic strips and PINs have been skimmed in payment terminals in Norwegian convenience shops. This manner of compromising payment terminals is new.

There have been a number of deliveries to ICT projects in the financial institutions that have not been of a satisfactory level of quality. It is often the case that the same ICT supplier is used for operations, application development and as a contributor to internal ICT projects. For development projects, the deliveries are often not precisely on time and not of a sufficient level of quality. It is not just the suppliers who are the cause of the projects not being delivered as agreed, cases also exist where a lack of order-placement competence is mentioned as a cause.

3. What does the institution see as its greatest challenges in 2010 with respect to the risks of ICT use?

The institutions give the highest priority to secure and stable operation, as well as to the protection of data and personal information against unauthorised access. It is important to ensure high availability of the services. By adding more services to the portal solutions, for example in the online banking portal, the complexity increases. The challenge thus also increases of ensuring the stable operation of solutions that are expected to be available around the clock, seven days a week.

Performing security tests and continual improvement of an institution's security solutions are important to securing their own infrastructure against penetration. Sufficient testing prior to placement into production of new and altered solutions is a challenge. The quality of test systems and test data is absolutely crucial to the ability of the tests to detect defects in solutions before they are placed into production.

Regulatory requirements are also a challenge to ICT activities of the financial institutions. Examples of this are the new Money Laundering Act, the Payment Directive that has the potential to cause changes to a number of statutes, the implementation of Solvency II and the new Pension Reform. These will all bring about changes in the ICT solutions of the institutions.

Bankruptcy or other difficulties with business-critical ICT suppliers as a relevant threat.

Motivated employees are important. An emphasis is desired both on looking after key competencies and following up on the development of the employees as well as on measures to increase the strategic understanding of the employees.

4. What does the company see as important problems that must be addressed (through specific measures) in 2010 with respect to ICT security?

Increasing understanding and awareness of ICT security among the employees is a prioritised area. Along these lines, it is specifically mentioned that access control to systems and data on all levels must be reviewed such that security-related conditions will be surveyed and arranged in relation to this.

Protection of card data is an area that is mentioned by a number of institutions. The work by the institutions with the PCI standard will continue in 2010. The purpose of incorporating the PCI standard in internal solutions is increased security for the use of cards, but it is no guarantee that card data cannot fall into the wrong hands. The banking sector in Norway has, through the Banks' Standardisation Office (BSK), defined its own requirements for security with the use of cards and these requirements may in some cases be stricter than the PCI requirements. The BSK has initiated work on ensuring that the security requirements are sufficient and in compliance with relevant standards as they were prepared by PCI.

Upgrading of catastrophe solutions is in the plans for a number of companies. Some institutions have been lacking redundant solutions at a geographical distance and will be establishing such in 2010.

ICT projects are taking place to a greater or lesser degree in nearly all financial institutions. Within the area of securities, it is particularly relevant because new trading systems and settlement systems are under development. This affects all the members of Oslo Børs (the Oslo Stock Exchange) who will have to adapt their solutions to the new trading system. Managing deliveries from the projects in parallel with daily operation is mentioned as being especially demanding. For any institution with larger ICT projects, it is a new experience to be using many resources that are contracted in and a challenge to manage the external consultants correctly. In the area of securities, mention is made of the risk posed to the Norwegian securities institutions that is connected with a dominant supplier of ICT. This may place the institutions in an unfavourable situation with respect to price, quality and the timely execution of the deliveries.

5. Are there other sets of problems that the institution is concerned about and which may be significant to the enterprise's use of ICT and operational risk?

Keywords for what the institutions mention as areas they are emphasising are standardisation, quality of risk assessments and internal controls. An emphasis is being placed on implementing operational risk management in a number of processes in order to ensure an objective and conscious relationship to risk as well as a focus on overall risks in processes rather than just ICT risk viewed in isolation. A number of institutions have undertaken acquisitions and mergers in order to procure synergistic effects. The institutions are having the experience that the synergy that may be procured from the ICT area is difficult to realise. Often, it takes a long time before resources are brought in to integrate the solutions of entities that have merged. In the meantime, parallel systems live side-by-side, which involves duplicated operation, administration and development, as well as dispersed competence.

3.3 Analysis of reported events

3.3.1 Reporting of events to Finanstilsynet

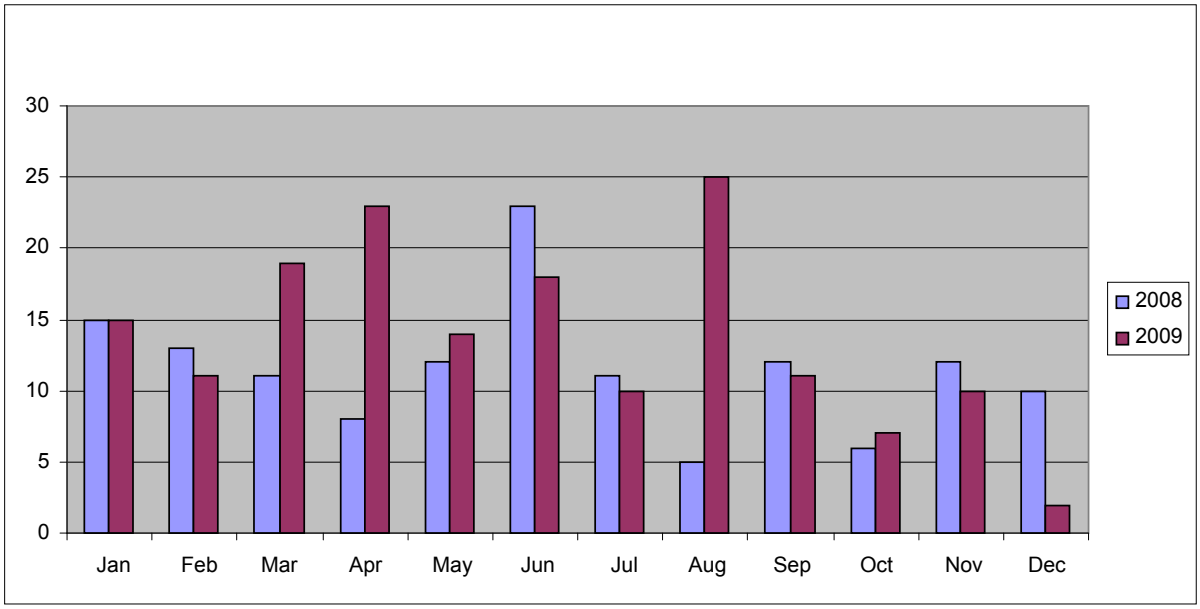
Event reporting to Finanstilsynet became subject to regulations as at 1 December 2009 through an expansion of the ICT Regulations. At the same time, the scope was extended to encompassing all financial institutions that are subject to the ICT Regulations with the exception of real estate brokerages, collection companies and pension funds.

Since branches of foreign banks and insurance companies are not subject to Norwegian regulations, Finanstilsynet has inquired of the branches whether they could participate in the

reporting on a voluntary basis. Some of the branches have chosen to follow the save arrangement for event reporting as the Norwegian institutions. Underreporting on events may be particularly noticeable in areas where foreign branches comprise large parts of the Norwegian market.

In connection with the use of payment terminals, attempted frauds have been detected using stolen cards and PIN codes. In this respect it has been possible to withdraw large amounts of cash in connection with purchases of goods. It appears that no blocks are built into such cash withdrawals like those that exist in cash points. Finanstilsynet wishes to make an assessment of this area of risk in 2010.

Chart 2: Events reported per month



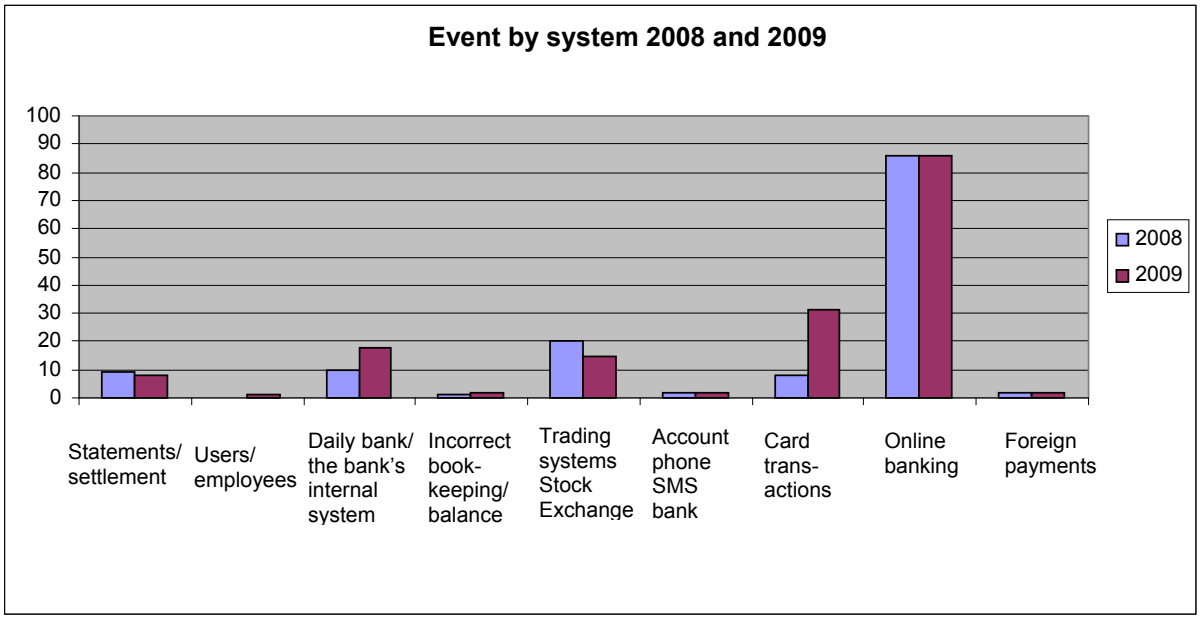
Source: Finanstilsynet

In 2009, more events were reported in connection with card transactions. For other areas, the number of events was around the same as in 2008.

In 2009, Finanstilsynet has attempted to structure the follow-ups to reported events.
Each quarter, an updated overview of reported events is posted on Finanstilsynet's website.

3.3.2 Events in 2009

Chart 3: Events distributed by business area



Source: Finanstilsynet

The events that received the most attention in 2009 were associated with skimming of shop terminals. The skimming attacks, which peaked in the late summer, caused a number of risk-reducing measures to be introduced, including an increase in the pace of replacement of cards with magnetic strips by cards with chips and the replacement of terminals with terminals that can read chips.

In general, it is the operating events that have dominated in 2009 – as in prior years. There have also been events connected with card transactions here. Events that cause the rejection of cards at retailers quickly result in substantial consequences. On Saturday, 24 October 2009, the system for using Norwegian payment cards with BankAxept was out of operation for13 minutes. This affected all merchants and all cards with BankAxept and occurred in the morning during the best shopping hours. BBS received an avalanche of inquiries during this short interruption for the cards.

Missing balance checks are most often the cause of problems with the use of cards at payment terminals and cash points. Most often, such events are limited to certain types of cards, certain types of cash points or certain types of merchants. The cause can be network problems or different problems connected with the operation.

The number of events associated with online banking is around the same in 2009 as in 2008. Total downtime for online banking appears to be somewhat lower in 2009 than in 2008. The picture for the causes is the same as previously. Insufficient capacity planning either as regards full disks or other boundary values that are exceeded without prior notice, and complications connected to a complex operating configuration. There have been some occurrences of programming errors related to session management that have resulted in a

customer being able to see another customer's data. When such errors are detected, the service is shut down until the error is identified and corrected.

3.4 Assessment of other relevant areas

3.4.1 ICT infrastructure

Financial services are to an increasing degree automated and taking place in real time in an end-to-end electronic interaction between the parties involved. This can be called an ICT infrastructure.

Users adapt themselves to the increased availability of financial services that the ICT infrastructure provides. A day-trader of shares buys shares trusting that the electronic share trading system will provide the possibility of exiting the position at the proper point in time. If the system goes down, it may involve a financial loss. Society is dependent upon the ICT infrastructure functioning well and being accessible.

As the automated, electronic financial transaction chains become longer, the complexity increases and thereby the risk of defects in one of the links. A defect in a link may cause the transaction to be unable to be executed and it being declined. The customer is unable to manage to execute the payment transaction in a timely manner and is entirely beholden to the supplier of financial services and its ability to re-establish the service.

In Finanstilsynet's experience there is a higher risk of defects in the connection between the participants in the transaction chain than with the individual participant. This has a natural context with increased innate risk connected with changing ”zones” from one participant to the next. In this exchange, decryption/re-encryption, reformatting, protocol conversion, address translation, version checks, sequence checks, etc. all take place. Such connectivity tasks have shown themselves to give rise to defects.

Hence it is useful to analyse the entire transaction chain as a whole for important financial services and in such case with a special focus on the interconnections. The financial service will be an object for processing in different systems along the transaction chain. Each system will be delivered by a participant in the ICT infrastructure. The work involves surveying the entire chain and all financial institutions and other infrastructure suppliers as well as their systems that are a prerequisite for the service to be able to function.

On this basis, Finanstilsynet has attempted during 2009 to survey the technical infrastructure that carries important financial transactions. In summary, the goal was to survey and assess the following for each system:

- Where does the system get its data from and in what manner is the data transferred to it?
- What does the system do with the data?
- Who does the system send its data to and by what manner does this occur?
- What security measures have been implemented?

What is meant by participants, for example, are BBS, EDB Business Partner ASA, the banks, VPS, Oslo Børs, Oslo Clearing, securities institutions, providers of networks for credit card transactions (VISA, MasterCard, etc.), payment processors for credit card transactions (Teller, Nordea), Telenor/other line suppliers and ISPs.

Among the main conclusions of the survey:

- In a number of areas, banking activities are dependent upon one or only a few large suppliers of services. This applies for example in ICT operation, system administration, share trading systems, investment systems, systems for validation of one-time codes and systems for reservation inquiries for cards/accounts. If the service is down, many of the customers in Norway are affected.

- The long transaction chains make it complicated to test end-to-end. It turns out to be difficult to maintain a production-like test environment. This gives rise to defects while in production.

- It turns out to be a challenge to get reserve solutions, in particular reserve lines to function as presumed.

- The operating environments have become extremely complicated and difficult to control, which makes for defects and downtime. Monitoring both of processes as well as systems is required.

- The online banks have been programmed such that all services in the online bank share central resources. Because of this, outage in one of the services will affect access to other services.

3.4.2 Outsourcing and offshoring

The nature of ICT operation resembles factory production. Among other things, automation and integrated operational monitoring see to this. Profitability in ICT operation is often a question of volume, and the trend is going in the direction of global ICT megacentres, typically in low-cost countries in order to obtain economies of scale, assure core competence and increased quality. Global competition causes financial institutions to desire to expand and operated in more countries in order to have larger volumes and to gain access to new and additional markets. The largest financial institutions are establishing centralised ICT solutions for their global operations, and arguing that centralised ICT operation is a prerequisite for rationalised operation.

Today, there are different requirements of financial enterprises with respect to outsourcing. For the Norwegian Central Securities Depository and Oslo Børs here are strict limitations where requirements are posed for approval by Finanstilsynet, whereas banks in Norway may perform outsourcing of their services without being subject to corresponding requirements. Sweden has introduced requirements for banks to submit their outsourcing agreements to Finansinspektionen (the Swedish Financial Supervisory Authority) for review when they have plans and agreements for outsourcing ICT services.

For the financial industry, as for other industries, reducing the costs of their ICT activities is important to being able to achieve the best possible results. This is a challenge for the in-house ICT activities of the financial institutions, and particularly for their ICT suppliers. With the complexity of the ICT solutions of the institutions, both in terms of technical infrastructure as well as applications, it can be difficult to secure sufficient competence in the different areas. This provides the driving force for a permanent process involving outsourcing and cost-reductions. ICT normally represents between 15 and 25 % of a bank's total costs and hence constitutes a significant sum. There is extreme pressure on IT suppliers to contribute to the necessary cost-reductions. One consequence of this will naturally be suppliers assessing offshoring as a means for achieving efficient cost reductions.

3.4.2.1 Principles and regulations

The Joint Forum was established in 1996 by the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS) in order to address challenges common to the banking, securities and insurance industries. The Joint Forum has prepared 9 principles for outsourcing. The first seven address the area of responsibility that the enterprise subject to supervision has in relation to outsourcing and its own activities. These principles have been incorporated into Finanstilsynet's ICT Regulations. The two remaining ones address the role of the authorities, and have been incorporated into Finanstilsynet's supervisory methodology.

Developments in technology, developments in the financial sector and events that have occurred in recent years pose new problems associated with risks, legal interpretations and the needs of the authorities for measures.

The current body of regulations provides individual provisions as regards individual companies, but little guidance when it comes to the assessment of risks for the entire financial sector as a whole, and how such should be evaluated on the basis of being activity crucial to the society.

In Norway, in connection with the Norwegian Official Report NOU 2006:6 “When security is of the highest importance – Protection of critical infrastructures and critical societal functions in Norway”, an assessment has also been made of the financial sector and it has been defined as a critical societal function. It is unknown whether, on the basis of the official report, further materials or bodies of regulation have been made other that the preparation of national guidelines to strengthen information security 2007-2010. In chapter 3.4, it points to the need to carry out risk and vulnerability analyses when a supplier has deliveries to enterprises that are defined as critical to the society.

In the BAS5 (Protection of Society) research project, an emphasis has been placed on the risks associated with critical societal functions. The authorities responsible for the project were the Norwegian Defence Research Establishment (FFI), the Directorate for Civil Protection and Emergency Planning (DSB) and the Norwegian National Security Authority (NSM), where Finanstilsynet was among the participants. The project carried out a delivery associated with ”Method for identifying and ranking critical societal functions”. It was assumed that several of the suppliers and a number of the tasks they are performing can be defined as being critical societal functions.

The following risk elements are of significance in the assessment of offshoring:

- The need of the financial institutions for their own administration and control of their own ICT activities. It must be presumed that this will be weakened over time if the company and/or ICT supplier are not sufficiently close to the tasks that are being performed.

- The need for instructional possibilities and control in catastrophe situations, by both the company and the authorities.

- Diminished national control if large parts of the ICT activities for the financial sector that are defined as being critical to the society are operated outside the country.

- Lack of overview of the legal code in the country that carries out the ICT tasks and which may cause unintended effects, particularly in a preparedness situation.

- Management of and secure storage of personal data where local statutes may cause unintended effects for compliance with legally mandated requirements. This applies in particular outside the EEA area.

- The relationship to activities subject to licensing and what can be defined as core activities, which cannot be outsourced without further consideration.

- Whether the body of regulations for outsourcing is sufficient viewed in relation to the different parts of the financial sector.

- Diminished possibility to perform supervision of the ICT activities of the companies.

3.5 Results from questionnaire-based studies performed

In September 2009 Finanstilsynet undertook a questionnaire-based study involving questions connected with the outsourcing of ICT and testing of catastrophe solutions for ICT activities. The questionnaires were sent to 144 banks (savings banks, commercial banks and branches of foreign banks in Norway). Finanstilsynet received 126 responses.

In addition to these five main questions, the questions were differentiated by which parts of the ICT activities were being outsourced (support, operation, administration, development, other) and whether the outsourcing was for suppliers in Norway, in the Nordic countries or in countries outside the Nordic countries.

Most of the savings banks in Norway belong to a banking group. There are more than 80 savings banks that belong to the Terra Group, where ICT activities are centrally administrated by the Terra Group with the operation being outsourced to Scandinavisk Data Center (SDC) in Denmark. Furthermore, there are between 40 and 50 savings banks that belong to the SpareBank 1 Group, where operation is primarily outsourced to EDB. EDB is also the most central operations service supplier for a large number of independent savings banks. The responses to the questions concerning outsourcing from savings banks in the same group are to a large extent identical.

The largest range in the responses came from the branches of foreign banks in Norway. These often have based their ICT activities on outsourcing to their parent company's ICT supplier.

The majority of banks are aware that their supplier company has agreements with and even have outsourced parts of the deliveries to third party suppliers. Outsourcing to third party suppliers in countries outside the Nordic countries was answered with a Yes by some banks and with a No by other banks based upon the latter not deeming it to be a third party supplier when the Norwegian supplier is an owner of the company in question in these countries.

There are relatively modest plans for changing the outsourcing arrangements that individual banks have established. There are few banks that are planning to outsource more parts of their ICT activities or to switch outsourcing suppliers, and there are extremely few that are planning to bring ICT activities back in-house.

Most of the institutions confirm in their responses that risk analyses are being performed and that notifications are sent to Finanstilsynet when changes are made in outsourcing situations that affect payment systems. However, a number of comments were made about these questions. Typical and pervasive comments were that the Terra Group and SpareBank 1 Group were performing risk analyses on behalf of the bank in questions concerning outsourcing or that the supplier was doing this. The same applied for outsourcing that may trigger the reporting obligation for new or altered payment systems.

The questions concerning tests of the catastrophe plan were directly aimed at the individual banks with questions on whether the bank had performed tests of its catastrophe plan and whether the bank assessed that is was fulfilling section 11 in the ICT Regulations. In response to the question regarding whether the bank has carried out tests of its catastrophe plan, many answered Yes and added the comment that it was a desk test. Many of the banks that responded with a No to the same question indicated in comments that a test would be performed later in 2009, possibly in the first quarter of 2010.

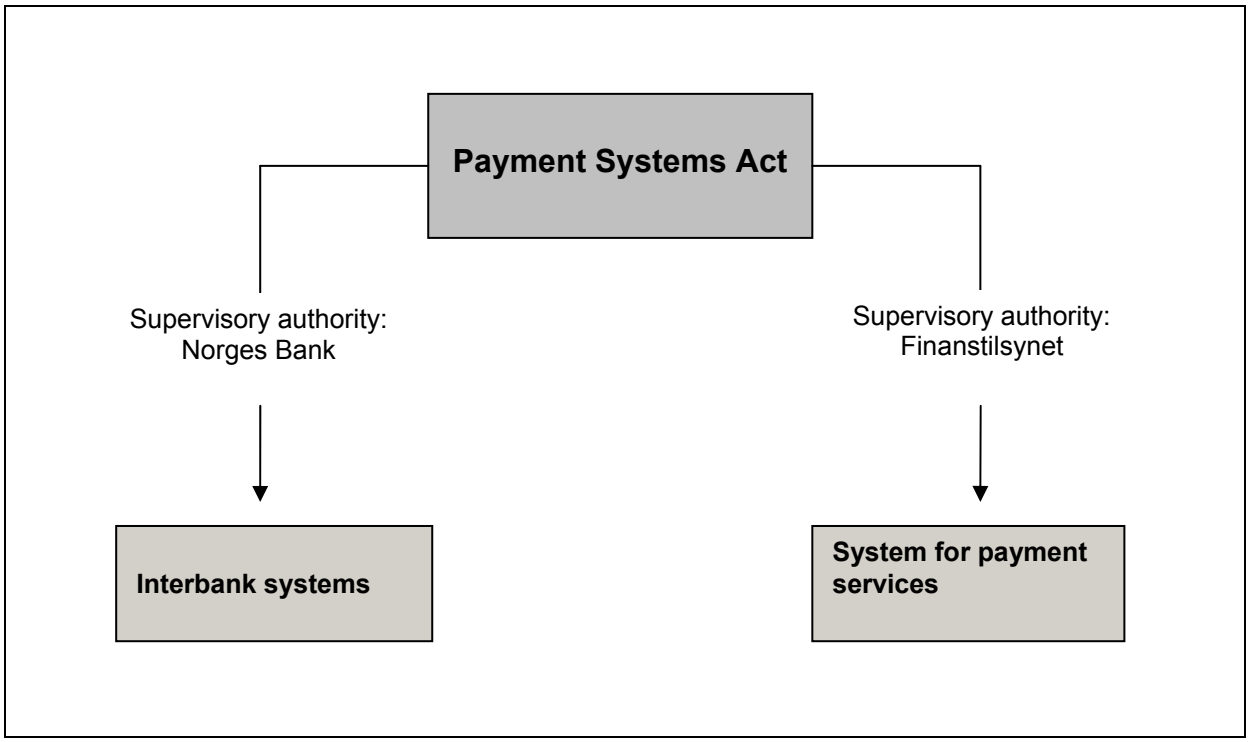
The many different answers show that there is some way left to go before well-defined and well-tested procedures for testing catastrophe plans are in place in all the banks. Furthermore, there are differences in how literally the banks interpret the requirements in the ICT Regulations. Part of the purpose of the questionnaire-based study was to draw attention to the operationalisation of testing the catastrophe plan. The catastrophe plan is a combination of reserve solutions inside the bank and with the operations service suppliers. In order to ensure that all parts function in a crisis situation, regardless of whether this arises in the bank, with the supplier or a combination of both places, the total catastrophe preparedness must cover all parts and the catastrophe plan reflect such.

4 Systems for payment services

4.1 Payment systems in general

In the Act of 17 December 1999, No. 95, the Payment Systems Act, the terms “interbank systems” and “systems for payment services” are used for systems that together ensure the transmission of monetary transactions/messages between customers of financial instructions and between banks in the interbank market. Examples of interbank systems include NICS (Norwegian Interbank Clearing System) and NBO (Norges Bank's settlement system). Systems for payment services include online bank solutions, mobile bank solutions and merchant solutions for payment cards. ‘Payment system’ can be used as a generic term for interbank systems and systems for payment services.

Trading goods and services in a modern, well-regulated society functions optimally through the use of efficient payment systems. The financial crisis has shown that despite the major turbulence in the global financial markets, the payment systems have functioned satisfactorily, nationally and internationally. In connection with this it is important to emphasise that the payment systems consist of both transaction information and monetary settlements.



In general the Payment Systems Act covers all systems that enable customers of financial institutions to transfer money from their own account to other accounts using the various payment instruments. The administration and control of payment systems is an important element of the assessment of operational risk based on the rules in Basel II and which have been incorporated into Norwegian financial legislation. For competition-related reasons, all payment systems and all lawful providers of payment services are required to ensure access to each other's payment systems under certain conditions.

4.2 Risks and vulnerabilities

The financial sector and the solutions that are offered are to an increasing degree vulnerable to attacks from different criminal groups. This is not a new situation, but it is worrying that there appears to be a gradual increase in attacks from internationally organised criminality. It is a challenge for an individual country to stop this type of trend on the Internet. Countermeasures will thus require measures that to a higher degree include risk analyses and international co-operation in order to identify vulnerabilities and to initiate risk-reducing measures.

If we look at the trend in Norway, we can surmise that there is intensive use of electronic solutions in payment transmission services that cover nearly 100 % of the needs for payment solutions. Volume development and innovation show that Norway lies in the uppermost stratum in this area in an international context. Volume figures measured against population size as described in Norges Bank's Annual Report on Payment Systems, dated May 2009, reflect this.

Experiences up to now have shown that it is the digital channels in the outermost link to the individual user, or individual link in the management of payment transactions, that are most vulnerable.

Based upon the experiences that Finanstilsynet has had, it is the following that have been the subjects of attacks:

- **Use of payment cards in cash points**
  In Norway there has been a problem with equipment being mounted in the equipment of the banks' cash points that was able to copy the content of the magnetic strip without the cardholder detecting this. The banks have implemented effective measures such that the remaining problems today are filming of the entry of PIN codes combined with theft of the card and subsequent misuse.

- **Use of payment cards at automated petrol stations**
  One consequence of reduction of the risks at cash points has been that some of the criminality has moved over to automated petrol stations where similar types of equipment are used for the unlawful copying of the content of the magnetic strip on a payment card. At present, it appears to be a manageable situation, and different measures will be initiated.

- **Use of payment cards at merchant terminals**
  It is the so-called payment terminals, where the cardholders enter their PIN codes, that have been vulnerable to modification for illegal copying of the content of the cardholder's magnetic strip. This has been a completely new threat situation in

Norway in 2009. It appears that the attacks have been well-prepared and organised in order to obtain the greatest possible returns. There are many shops that have been subjected to this, especially in the eastern part of southern Norway. The number of cards that could potentially have been subjected to skimming is estimated to be more than 10,000. The attempted misuse of the cards has primarily occurred in automated payment terminals outside Norway. The information is most probably sent out of Norway with using the Internet to a recipient who is working with them. We assume that there actually have been more cards that have been copied, but that attempts to misuse them have either been stopped due to various reasons or they have not been used.

- **Illegal copying of card information at collection and card processing centres outside Norway**
  Another increasing problem is that criminals, through different techniques, have acquired unlawful access to information from payment cards at collection centres in countries outside Norway. In this manner, they have acquired illegal access to the card information of Norwegian cardholders in connection with the payment card for the Norwegian customer having been utilised outside Norway. Norwegian banks have as a general procedure, when they became aware of this, seen to it that the card is blocked, contacted the customer and issued a new payment card. This type of illegal access to payment card information has greatly increased outside Norway. It is in particular the US, the UK and Spain where we are familiar with this having occurred. In practice, there have been limited losses in Norway, but it has been a great inconvenience to the customers and much work for the banks. We are unaware of this having occurred in Norway on a larger scale. The last time Finanstilsynet registered such leakage was in 2004, and even in that case it was very limited in scope. There are however all reasons to continue further work with measures in this area in order to ensure as best as possible that information on payment cards does not fall into the wrong hands.

With respect to an overview of total losses in Norway in the different service areas, Finanstilsynet has in connection with the event reporting and the follow-ups on such, commenced work with obtaining more precise figures from individual organisations of losses. This is important information, allowing Finanstilsynet to follow developments over time. For 2009, Finanstilsynet has procured estimates that provide a relevant picture of the losses. The work with this will continue in 2010 such that the 2010 report may contain more verified data about total losses in the service areas concerned.

4.3 Reporting obligation – Systems for payment services

Finanstilsynet has the supervisory authority for systems for payment services. The purpose is to contribute to systems for payment services being organised and operated such that regard is paid to secure and efficient payment and to the rational and co-ordinated execution of payment services. The institutions that are covered by the Payment Systems Act must without undue delay notify Finanstilsynet when they establish operations and systems for payment services. The notification must contain information on:

- The agreements between participating institutions and the transfer or withdrawal of means of payment.
- The agreements involving the affiliation of merchants.

- The agreements between systems for payment services.
- Use of payment cards, numerical codes or other forms of independent user identification that will be utilised when making payments.

The notification duty gives Finanstilsynet information that can function as a basis for risk assessment and checks of compliance with the law. With a basis in the relatively low number of notifications that have been received, it is presumed that some underreporting may be occurring. On the basis of the experiences that Finanstilsynet has had, it has turned out in many cases that the requirements that are being posed for the submission of notifications have not been adequately carried out, for example the execution of tests prior to placement into production, and that in many cases it also takes a long time to procure supplemental information on new or altered systems for payment services.

5 Identified areas of risk

5.1 Skimming

In 2009, a number of payment terminals were stolen from shops in Norway. The terminals were then furnished with equipment to be able to copy the content of a payment card's magnetic strip (skimming) along with the PIN code for the same card. Based on the information that Finanstilsynet has received, these thefts are related to the skimming of more than 10,000 cards, however losses have been incurred by only a small number of these. This type of fraudulent method has not been seen in Norway before, however it resembled attempts that were previously tried in, for example, the UK.

In Norway, standards and requirements for security have been established that correspond to the requirements for security that the card companies pose of solutions for the use of the cards issued by the companies. The standard being referred to is the PCI standard. This standard is updated regularly, however delays of several years are often granted before old products have to comply with the new standards. The Norwegian Banks' Standardisation Office, established under the auspices of Finance Norway (the FNO), has the responsibility for setting standards and requirements for security in the Norwegian payment systems.

The scope of the skimming has been limited so far. The reason for this is probably that it is a relatively difficult way in which to defraud people, since components from several terminals are required in order to be able to make one that functions. Furthermore, one must have detailed technical expertise concerning the technology in the payment terminals.

So far, the risks with payment cards have been the relatively simple task of copying information from a payment card's magnetic strip in order to then copy it again onto a new, false card.

With the transition to the use of chips, this risk has been reduced. The industry and Finanstilsynet thus recommend that all users of payment cards make use of the chip and not the magnetic strip for payments in payment terminals.

5.2 Identity theft

According to the Data Inspectorate, identity theft is defined as all situations where a person, without the consent of the proper individual concerned, either:

- in full or in part is in a condition to perform one or another form of undesired transaction in the name of another person,
- acquires access to resources belonging to others, or
- illegally acquires rights that belong to others

According to the Federal Trade Commission, identity theft is one of the fastest growing crimes in the US.

The most common methods the criminals utilise in order to acquire information about for use in identity thefts are:

Phishing and fake web areas. Pretending to be well-known organisations through fraudulent e-mail messages (phishing) and fake web areas.

Personal presence. Eavesdropping or spying on people during financial transactions.

Hacking. Breaking into databases where personal data is stored in order to then retrieve requisite information. Examples of this are data thefts at payment card processors such as Heartland Payment Services and RBS Worldpay.

5.3 Offshoring

Based upon information that Finanstilsynet has received from individual companies, and through Finanstilsynet's internal project for surveying and assessing risks connected with outsourcing in general and the moving of ICT tasks out of Norway in particular (offshoring), Finanstilsynet has identified this as an area with increased operational risks. This is grounded both in the current scope as regards outsourcing and offshoring, but also in the on-going processes and plans of individual companies and ICT suppliers in this area, which can give rise to increased risks.

One approach is to assess the risk that applies for an individual financial company, both with respect to the probability and the consequence of the individual risk element and on this basis to evaluate whether the risk is acceptable. Another approach is to view the entire financial sector as a whole, with respect to both the probabilities and the consequences. The consideration may then be made of whether the overall consequences give too high of an operational risk when weighed against a critical societal function.

It will thus be necessary for Finanstilsynet to follow this trend carefully, particularly when it concerns operational risk weighed against critical societal functionality. Some guidelines do exist in this area through: Norwegian Official Report NOU 2006: 6 - “When security is of the highest importance – Protection of critical infrastructures and critical societal functions in Norway” in which parts of the financial sector are defined as a critical societal function. And similarly through the “National Guidelines for Information Security 2007-2010”. The primary basis for a risk assessment in this area at Finanstilsynet will, regardless, be an assessment of compliance with the Financial Supervision Act and other relevant laws and regulations that apply to the different parts of the financial sector.

5.4 Rapid pace of change

In the area of securities, large projects have been initiated that will change the infrastructure. Oslo Børs entered into an agreement in 2009 with the London Stock Exchange on the purchase of trading platforms for derivatives and securities. The platform for derivatives was placed into service on the first weekend of December 2009. The trading solution for shares is planned to be placed into production in February 2010, however by far the majority of the work was performed in 2009. The changes that are being carried out in the securities area are

large and comprehensive, with follow-ups to the risks that the projects are running being extremely important.

As a consequence of new trading solutions being placed into operation, the members of Oslo Stock Exchange will have to make changes to their internal systems. To a large extent, the members of Oslo Børs utilise deliveries from one and the same supplier. As a point of departure this can be viewed as an advantage where the implementation of changes to be carried out could be performed by all the members at the same time. On the other hand, the members use the solution differently, so some tailoring must be reckoned on regardless. This could cause an increased delivery time. Out neighbouring countries carry out corresponding projects where they are also dependent upon deliveries from the same supplier. With substantial pressure on deliveries from all parties involved in the securities infrastructure, this could increase the total operational risk of the securities activities and lead to delays.

5.5 Catastrophe

Section 11 of the ICT Regulations, Operating interruptions and disaster preparedness, poses requirements for training, exercises and tests to be performed at least once annually of a scope that provides sufficient assurance that the catastrophe solution will function as presumed. The results of the test must be documented in a manner that makes it possible to check.

Finanstilsynet's experiences from the documentation it has received shows that performing and documenting catastrophe tests is an area that must be focused on in the future. Experience shows that a number of institutions are basing their own catastrophe tests on their solution being tested only at the operations service suppliers, and not as an integrated part of the institution's catastrophe solution. Functioning catastrophe solutions are often a prerequisite in order for institutions to be able to be operate in a defensible manner if a catastrophe situation arises.

5.6 Complex infrastructure

The increasing complexity of the ICT infrastructure is challenging. Traditionally, the data centres have been divided up into three primary groups having the responsibility for development and maintenance of computing equipment, systems applications and deliveries. The groups cover server farms, storage and networking. The different environments that have such responsibilities build up their own environments in order to protect the own areas of competence. This takes place at the cost of the requisite communications, which ought to be open and unhindered between all these three primary groups. A lack of co-ordination with the other groups and the protection of one's own areas increases the complexity, makes for worse administration and control of operational risks and causes unnecessary co-ordination expenses.

This picture will become still more complicated when all the minor subcontractors are taken into consideration that for example supply applications that are only concerned with delivering minor parts of the entire ICT infrastructure to an already fragmented ICT environment.

With operational risks being connected to an increasing degree to reserves for equity capital under Basel II (ICAAP), the continued ability to accept an opaque ICT infrastructure will be limited in time. Hence a further emphasis will be placed on the institutions themselves being able to document all the elements in the ICT infrastructure and on them also understanding how the individual elements function together. This must in turn be built into the strategic and operational plans and management control systems of the institutions.

5.7 Transaction chain

Financial services are to a continually increasing degree being automated and occurring in real time in an end-to-end electronic interplay between transacting parties within what we can call an ICT infrastructure. A number of suppliers of ICT services are involved. Along the way, a transaction may be transported in networks that have different protocols. At the nodes where the transaction is delivered from one supplier to the next, the transaction must be opened and reformatted so that it is suitable for the transport protocol of the next stage. A hypothetical example is a service that is delivered via the mobile telephone channel. The transaction is transported using the mobile telephone network and its associated protocol (GSM) and security (GSM encryption) to the telecommunications supplier's server, where it is unpacked, reformatted (typically to IP), re-encrypted and forwarded to the service provider. At the reformatting point, the transaction is ”vulnerable” to, for example, unauthorised disclosure. In order to compensate for the uncertain security, performing end-to-end encryption at the application level is recommended. Such encryption involves challenges both technically and logistically that are connected to the securing of keys and the administration of keys (key exchange). The risk will increase in step with the transaction chains becoming longer and further automated.

6 Finanstilsynet's further follow-ups

6.1 Current measures

Only after a risk has first been recognised is it possible to commence appropriate measures. When one's own understanding of the risks is small, it often becomes the events that drive the work with security. It is not always possible to detect all vulnerabilities in advance, but it ought to be a goal that all vulnerabilities that can be detected through systematic work with risks as well as other planned measures will be what collectively form the basis for risk-reducing measures. We also know that it is often the case that repairs cost significantly more than if the relevant problems were taken into account in a planned manner. In its supervisory work, Finanstilsynet places an emphasis on the preventive security work of the institutions.

The measures that Finanstilsynet can undertake in the risk area primarily are:

- Seeing to the carrying out of IT inspections of a scope and level of detail that allows Finanstilsynet to obtain a realistic picture of how the institutions are taking care of their ICT activities, managing their risks and complying with the body of regulations.

- Administrating the event reporting system and ensuring that information from the reporting of ICT events to Finanstilsynet is utilised for preventive measures and simultaneously contributing to ensuring that fault situations that arise are handled appropriately and that normal operation is re-established as quickly as possible.

- Through, among other things, the work with RAV analyses procuring necessary information so as to have as correct as possible an understanding of the risks the financial sector as a whole is facing.

- Keeping the focus on the payment systems through proactive measures, but also through supervisory activities and other follow-ups, in order to ensure compliance with the regulations and that payment occurs in a fast and efficient manner.

- Contributing to establishing arenas for co-operation connected with problem areas where it is important to share information and discuss joint measures.

Monitoring of processes and resources is a prerequisite to being able to predict bottlenecks and trends in time so as to react and avert an undesirable situation. Finanstilsynet's event statistics for 2009 indicate that the institutions can focus more on monitoring. Good monitoring is not just a question of good tools. Placing monitoring at the right location, setting the right threshold values and creating and implementing good procedures for reacting and reporting all require personnel with a high level of competence. Finanstilsynet recommends that the institutions give priority to this important area during 2010.

An explanation is given below in some added detail of how the use of relevant measures is organised and utilised to contribute to the responsible management of operational risks.

6.2 Increased focus on the merchants

A lack of understanding of security at the merchants can lead to implementations that are encumbered with security defects that are vulnerable to fraud and misuse. Events in 2009 indicate that there is a need for the individual responsible for service to improve the controls at the merchants. The controls can be envisioned as taking several forms.

As PKI services are now gradually being use more, it may be desirable for the individual responsible for the PKI service to take responsibility for the merchant approving the ID having implemented this in its service in a manner that gives the merchant sufficient security that unauthorised parties cannot make transactions in the proper user's name after such has been authenticated. For example, the user ought to be able to expect that the merchant has implemented the ID service in its infrastructure in a manner such that the ID cannot be easily misused. Such misuse may for example occur through the unauthorised party ”hooking into” a logged-on session, ”picking up” a session that the proper user believes have been terminated but which is ”hanging” and which continues to be open on the merchant side, and so on. The ID service has little value if it is implemented in the merchant's service in a manner that leaves it vulnerable to such misuse.

The ID supplier ought to demand that the merchant perform quality assurance for the integration of the ID service into the merchant's service as per rules defined in further detail by the ID supplier.

6.3 IT inspections

Performance of IT inspections to a sufficient extent is a fundamental manner by which to carry out ”temperature-taking” of how the financial sector is managing its use of ICT and the risks associated with such. It thus is important to continue to give priority to increased IT inspections, while at the same time it is a challenge to further develop the supervision planning such that relevant problems and vulnerabilities can be identified.

Further development of the planning of the supervision continues to be on-going as regards improvements to existing arrangements and the establishment of new supervisory modules. Similarly, continuation of the work with implementing a methodical grading of the level of maturity of an institution's ICT organisation is on-going. The conceptual work with establishing a separate module for so-called transaction testing is also on-going, and this will be the last primary module in the total IT inspection architecture. We are projecting that the methods will gradually be placed into use and that some practical experience will be gained during the course of 2010.

6.4 Further development of the plan for reporting obligations for systems for payment services

Finanstilsynet will continue the work with self-reporting as a basis for looking after its responsibility for the reporting obligation for payment services as regulated in section 3-3 of the Payment Systems Act. Considerations involving risks will also be used as a basis in this work. Finanstilsynet will give priority to preventive measures for improving the security of

the payment services that have electronic channels directly to customers. Electronic payment services represent an important societal function. At the same time, these types of services are under attack from organised criminality. The work in this area will take place in close co-operation with industry organisations and the joint institutions that the banks have established in this area. A new supervisory module has been made for systems that are utilised in connection with IT inspections.

The standard form of 19 questions (circular 17/2004) that the reporting obligation is now based upon will be reviewed during the course of 2010. The objective is to obtain a more detailed description from all the participants of what new or changed systems for payment services contain, as well as precisely which links are the critical links in the production process.

6.5 Risk and vulnerability analyses (RAV)

Performance of RAV analyses that cover the entire financial sector are important, both in order to ensure sufficient on-going understanding of the operational risks with respect to the use of ICT as well as to ensure that it is possible to compare results between years and between different parts of the financial sector. The knowledge that Finanstilsynet receives through the RAV analyses represents an important basis for prioritising future supervision, and for determining risk-reducing measures and/or quality improvements.

6.6 Event registration and reporting

An arrangement was established in 2007 for event reporting to Finanstilsynet. This was a trial arrangement for banks, Oslo Børs, the Norwegian Central Securities Depository and Bankenes BetalingsSentral (BBS). On the basis of the results from the trial arrangement, Finanstilsynet concluded that this was an appropriate manner to ensure timely and correct information on serious ICT events in the financial sector. The data from the event reporting is utilised as a source for risk and vulnerability analyses and comprises a contribution of quantitative data to the report. The reports are also used as a basis for addressing relevant problems directly with the institutions concerned. In 2009, Finanstilsynet thus decided to regulate event reporting in the form of an administrative regulation that will apply as at 1 December 2009. Finanstilsynet will devote substantial resources to its follow-ups on the arrangement and the use of the data in its work. Plans are to establish a user forum for the participants in the event reporting.

6.7 Information and communication

As an element of its work with ICT in the financial sector, Finanstilsynet is participating in a number of different forums. Some of the more important ones are: the Information Security Coordination Council (KIS) and the Contingency Committee for Financial Infrastructure (BFI). There is also direct co-operation with Norges Bank, the Norwegian National Security Authority (NSM), the Norwegian Post and Telecommunications Authority, the Data Inspectorate and industry organisations. Finanstilsynet also co-operates closely with the other Nordic supervisory authorities, participates in international IT inspection 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 group for security.

Finanstilsynet is participating in an EU project associated with Internet security and notification (Communication Middleware for Monitoring Financial Infrastructures). The project is supported by the EU's seventh framework programme for research and development and has a duration of two and a half years (to 2011). The purpose of the project is to arrive at measures that can make the financial sector's use of the Internet more secure (European measure). Finanstilsynet is participating in the project by defining requirements that supervisory authorities wish to pose for a monitoring/notification system. A reference group has been established with representatives from banks. At the end of 2009, Finanstilsynet participated in a new project application for the EU’s seventh framework plan in the area, a monitoring system as a measure against money laundering, which has been given the designation OMAS (Online Money Laundering Report and Analysis System).

FINANSTILSYNET
P.O.Box 1187 Sentrum
NO-0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO