Risk and Vulnerability Analysis (RAV) 2008

Financial institutions' use of information and communications technology (ICT)

Kredittilsynet, 17 February 2009

Contents

1 Introduction

The financial system is a great contributor to efficiency in a modern society and the national economy. Today, the use of information and communications technology (ICT) in the financial sector is all pervasive, and serious breaches of confidentiality, integrity and availability in this sector have a very negative impact, and can have serious negative social consequences. The recognition of this is one of the main reasons for the increasing focus on operational risk in the financial sector: internationally and nationally, in industry organisations, in consumer protection agencies and in individual financial institutions. There are many examples of this trend. Some important driving processes behind this are listed below:

- Internationally: through cooperation programmes such as the new capital adequacy regulations (Basel II), which for the first time provide guidelines for managing operational risk. A similar process is underway in the insurance sector through the work on Solvency II, which has adopted many of the elements of Basel II. These are just a couple of examples of a multifaceted process that is focusing in particular on the risks associated with socially important areas. Several other measures are in progress in this area, initiated by the OECD, the G8 countries, and the UN, which address the risks associated with ICT and the financial sector.

- Nationally: through NOU 2006: 6 *"When security is of the highest importance – Protection of critical infrastructures and critical societal functions in Norway"* in which the financial sector is defined as a critical social function. There are wide-ranging discussions of ICT security in Report to the Storting No. 17 (2005-2006) "*An information Society for All"* and in the "*National Guidelines for Improving Information Security 2007-2010"*. It is also discussed in Report to the Storting No. 22 (2007-2008) "*Societal Security – Cooperation and Coordination"*, which provides an account of a number of security measures that affect the financial sector. The following research project should also be mentioned: *"Protection of Society 5"* (BAS5), which particularly examined risk and vulnerability analyses as a method, and delivered the reports "*BAS 5 Case study – risk analysis of a financial institution's ICT system*", *"Inspection methodology and measurement of information security in the finance and energy sectors"*, and its final report, *"Protection of Society 5: Vulnerability in critical ICT systems – final report*"[1].

[1] http://rapporter.ffi.no/rapporter/2007/01204.pdf (downloaded Feb 2009)

The financial sector in Norway has always been an early adopter of ICT in new areas, and this is part of the reason why such emphasis is being placed on ICT security and risk in this sector. Cooperation forums and common organisations for standardising ICT security and risk requirements have been established in a number of different areas. This system now faces challenges due to demands for European harmonisation. One of the tasks in this will be to maintain the national level of security in European solutions. The authorities have drawn up regulations for this area due to the financial sector's advanced use of ICT. The ICT Regulations stipulate that institutions must conduct risk and vulnerability analyses at least once a year and document the results of these. Risk can only be managed in an acceptable manner when individual institutions themselves focus on risk and get to know their own risk situation.

Kredittilsynet's annual Risk and Vulnerability Analysis (RAV Analysis) summarises the work done on ICT security in the financial sector in the preceding year, and the individual institutions' and industry's compliance with the regulations. This makes it possible to see trends in the financial sector over time. The results provide part of the basis for implementing measures in particularly vulnerable areas. Norges Bank's *"Annual Report on Payment Systems"* should also be mentioned here. This is a collaborative effort with Kredittilsynet aimed at coordinating the focus on areas associated with ICT security and risk in payment transmission services.

It is a long time since people became aware of risk and the difficulties associated with recognising in advance every problem that could arise:

> *"It is probable that something improbable will happen."* Aristotle, 384-322 BC

If this quote is to be taken seriously, it underlines the importance of risk prevention work which in practice is a never ending task. Therefore, it is important that risk prevention work never becomes purely routine, but is instead afforded sufficient attention, priority and weight to achieve its aim, namely to make it possible to discover problems and implement measures before they materialise.

2 Technology and trends

2.1 Technological trends in general

There are many general trends in the financial sector that influence the institutions' use of ICT. In Kredittilsynet's opinion the following drivers are important for ICT development and affect operational risk.

- The area of electronic communication is developing rapidly. The various communications networks can increasingly be used in combination with each other (convergence). The use of telephony in combination with the Internet is one example of this. The networks have become multimedia carriers, i.e. they can transmit text, audio and images. The electronic communications networks will be accessible everywhere at any time. This means the same electronic banking services can be used from Norway and from Australia. All that is needed is access to an Internet terminal or a mobile phone with a web browser.

- Mobility has increased in line with the development of the mobile phone and the opportunities the mobile phone's interface can offer its users. As mobile devices steadily gain more functions and greater capacity, the devices will not only largely replace stationary office PCs, but also laptops. This type of advanced mobile phone has personal support functions, traditional PC features, and enables high-speed Internet access.

- So-called contactless payment methods are an emerging trend, especially in areas where cash handling still dominates. Technically speaking a contactless payment is completed without physical contact between the reader and the card. Several technologies can be used for this, including Bluetooth, infrared or radio frequency identification (RFID).

- Unlike wireless devices based on Bluetooth or infrared, RFID transmitters do not need batteries. Instead they respond to interrogation signals sent by a RFID reader. This makes it possible to embed a RFID transmitter in a chip and makes the technology very flexible. RFID chips can be embedded in key rings, mobile phones, credit cards, watches, letters and other ID chips. This great flexibility may result in lower unit costs and make their use simpler for users.

- Many consumers are already familiar with the use of contactless payments. In Norway, one of the most commonly used types being the Autopass chip. The USA has had solutions such as ExxonMobile's Speedpass and a number of other tollbooth solutions for a long time. In the UK the best-known project is the Oyster Card, which is used to pay on London's public transport system. Major market players such as American Express, Visa and MasterCard have made RFID cards available to consumers since 2005.

- As mentioned, the above RFID payment solutions were particularly developed for the traditional cash segment within payments. This is a positive development for merchants and banks with respect to handling cash. Handling cash represents a major cost for the banks. Reducing the quantity of cash also reduces the banks' costs.

- Online banks are by far the dominant channel Norwegians use to manage their own finances. The desire for new services and ways of using them is increasing as solutions steadily become more advanced. Therefore, there is reason to assume that today's online bank solutions will change. As a rule, most of the solutions offered to Norwegian customers are designed along the same lines. The biggest difference between the solutions is not their content, but what it costs consumers to use them. Future solutions will probably allow for customization, meaning users will be able to personalise their own interfaces. Changes will particularly be seen in areas where the communication with the bank is more direct. Chat and direct contact functions between the customer and bank could be used to improve customer relationships. In this way providers of online banking solutions can help increase the range of services on offer and consequently also the competition between the banks.

- A large proportion of Norwegian online bank users today depend on security devices such as DigiPass or code cards to log into their online banks. New solutions are continuously being developed to simplify the customers' use of financial services. Security services that were previously implemented with the aid of traditional security devices, as mentioned above, are instead being implemented using mobile phones. This makes the services more available since people "always" have their mobile phone with them.

2.2 Infrastructure

2.2.1 General

Infrastructure encompasses physical components, operating systems, networks, standards, monitoring systems, organisation, agreements, follow-up, documentation and control with respect to the operation of an institution's ICT, whether this takes place in-house or is partly or wholly outsourced, e.g. as part of a partnership constellation.

A number of current initiatives are also increasing the attention being paid to securing vital international and national infrastructure.

2.2.2 Networks

Individual institutions are themselves responsible for ensuring the availability of their own infrastructure. National prioritisation in the telecoms network is addressed by the Norwegian Post and Telecommunications Authority (NPT). Market players responsible for tasks of national importance can receive funds through the so-called assistance programme, which is administered by the Norwegian Post and Telecommunications Authority.

Beyond this it is the individual service provider that has to ensure that the institution's requirements when it comes to availability, back-up copies, redundancy, etc, are met.

During 2008, many financial institutions analysed vulnerabilities and threats in their network infrastructure in detail with a view to finding solutions that could provide a higher level of confidence that the institution's services could continue despite the occurrence of unplanned events.

A number of institutions report that in many cases it can be difficult to obtain an overview of the network infrastructure. Getting telecoms operators to describe the topography of networks has proven to be difficult. In some cases it appears as though there is a lack of willingness to provide the customer with the necessary insight. In other cases it appears as though the network operators do not have an adequate overview themselves.

Kredittilsynet considers it unacceptable for financial institutions not to be provided with an overview of this important part of their business critical infrastructure. The alternative is the Norwegian Post and Telecommunications Authority or the telecoms operator formally having to confirm redundancy in the infrastructure.

2.3 Integration between central and local software

Financial services are becoming increasingly automated. The scope and use of online financial services are increasing strongly. The increased use of electronic services is making society increasingly dependent on the quality of the services – there is less room for downtime and errors.

Today many services have a central (server) and a local (client) software component. The client may be transient, e.g. a programme ("applet") that is downloaded every time the service is used, or it can be persistent, e.g. software components installed on the customer's hardware. The customer wants integration with his or her own systems, and this is often resolved by a persistent component installed in the customer's systems. Developing an interface with the customer's systems is often a major challenge, not least because the technical environments vary from customer to customer. Customers have different portal configurations, firewall configurations of different kinds, differently configured software, and so on. The variations are manifest and suppliers have problems maintaining functions to secure the interfaces with the many different configurations. Suppliers resolve this problem by offering open an application programming interface (API) in which it is the customer who has to configure the security parameters and turn on security features according to on his or her specific infrastructure. This entails a major and increasing risk. The customer may have inadequate understanding of security and the level of security he or she achieves may thus also be inadequate. Suppliers have many different customers and cannot check that every customer has set-up his or her security properly.

Some services are designed such that measures on the client side are administrative in nature meaning that security is dependent on the client side following instructions for security configurations and procedures. Other measures are "hard coded", i.e. the client has no options and the security configuration is therefore forced.

The so-called PCI (payment card industry) requirements apply in the area of credit cards. These measures are administrative in nature. Despite the requirements there have been a number of accidents in which large quantities of card data have gone astray. There may be reason to believe that the PCI requirements have not been adhered to by the merchants who have "leaked" card data. Checking that the PCI requirements are adhered to at all merchants at all times is a major challenge for the card companies.

2.4 Testing

At the same time as ICT infrastructure is becoming more complex and various parties are having to cooperate, ensuring adequate testing before changes and new systems are put into operation is a major challenge.

Bank transactions used to be divided into separate 'legs'. A giro transaction, for example, involved the "user", Posten Norge AS, OCR Giro at BBS AS, settlement in the Norwegian Interbank Clearing System (NICS) and bookkeeping in the "Bank AS" in isolated and separate processes. An error in one link did not mean the transaction had to be started from the beginning (by the user) again, and it was not given that the error would even be visible to the user. Today, these services often take place online and in real-time. The user sits at his or her PC and sees everything that happens from registration until the amount is reserved on the account. The transaction is completed in one integrated operation. An error in just one of the links means the entire transaction has to be done again. The error is immediately visible to the user and harms the bank. The risk and harm to the financial institution from the system failing in one link is therefore much greater today than it was before. Therefore, an institution's management should have a policy of developing systems that ensures testing that reflects this (IT governance standards).

2.5 Effects of the financial crisis

Today, all financial institutions have technical infrastructures that include deliveries from a series of ICT suppliers. The global financial crisis gives rise to the question of whether the ICT suppliers are in danger of going bankrupt or having to suspend their activities for other reasons. Many suppliers may have made loan-financed purchases. Difficulties in the credit market may result in higher interest rates and strains on liquidity, and consequently reduce freedom of action. If the purchase is a part of a business amalgamation, it may be difficult to achieve the desired benefits in the short-term, and in times of crisis turnover could fall.

In such a situation it is important that the financial institution (the customer) takes a closer look at their suppliers. It may be relevant to improve one's control over the delivery with a view to, in the worst-case scenario, having to take over further development or hand this over to a new supplier. Appropriate questions in such a situation would be: "What are the statuses of documentation, source code, training and so on?" Moreover, it may be relevant to check ownership rights, i.e. intellectual property rights (IPR), rights of use, resale rights, the right to develop the product further, and other relevant factors. If the institution contributes to the completion of the product itself without having the necessary ownership rights, this may have unfortunate consequences.

2.6 Replacement of systems

Given the extensive cooperation that has taken place in the Norwegian financial sector and through the establishment of joint solutions in many areas, today joint infrastructure also exists to support this. This is particularly true in the areas of payment systems, securities, clearing and settlement, and in special service areas such as public key infrastructure (PKI). Moreover, various joint solutions and infrastructure have been established. The Norwegian infrastructure is interconnected. Many key systems that form part of the cooperation are going to be replaced in 2009 or in succeeding years (Norges Bank, the Norwegian Central Securities Depository, the Oslo Stock Exchange, NICS/BBS, and Teller). The systems are central to the Norwegian financial infrastructure and there are interfaces between them. The fact that many interlinked systems are to be replaced around the same time poses a risk in itself.. This will present major challenges with respect to testing, quality assurance and risk management.

2.7 Internet crime

2.7.1 General developments in Internet crime

Many countries report an increase in the number of attacks on online banks. This also includes successful attacks, i.e. attacks that have resulted in losses. Many banks are worried and have established taskforces to find countermeasures quickly.

Internet penetration has increased in many countries since 2006. The USA and China have around 200 million Internet users. Instances of attempted fraud and the number of fraudsters on the Internet have increased correspondingly. Some countries are believed to have a disproportionately large number of fraudsters, but these can often be difficult to identify since the relevant server that transmits the transactions is often controlled in another country. Nonetheless, it is believed that Russia, Nigeria, China and Ukraine are examples of countries that are sources of major Internet crime.

Phishing, i.e. malicious software that secretly collects identity information from customers, is a serious threat. The threat sets limits with respect to which services it is defensible to offer via the Internet given that the known ID solutions require the user to register a password and user ID on their PC.

2.7.2 Possible future forms of attack

2.7.2.1 Attackers penetrating enterprises' internal networks

Attackers have succeeded in penetrating enterprises' internal networks. Kredittilsynet believes that this problem will increase. These attacks open up a number of opportunities for the attackers.

- The attackers can carry out unauthorised banking transactions from inside the enterprises
- The attackers can close down the system (operations) and blackmail the enterprise for money.
- The attackers can steal customer information and blackmail an enterprise for money or sell the information.
- The attackers can plant software that feeds them information from the system or gives the attackers control over the system.

One example of this was the penetration of the World Bank, which is a thought provoking event that took place in this area in 2008. The attackers successfully penetrated the bank's network and gained access to passwords that, with a high level of probability, could be used to extract sensitive information, see the article "*World Bank Hacked, Sensitive Data Exposed*"[2] published on 10 October 2008 on the website, Darkreading.com.

2.7.2.2 More advanced forms of trojans

[2] http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201265 (downloaded February 2009)

Several examples of attacks have been reported, in which malicious code (trojans) “hides” fraudulent transactions from the user. The technique is known as persistent MitB (man-in-the-browser).

The user is presented with pages showing only the transactions that the user has authorized, and corresponding account balance. The user does not see the fraudulent, unauthorized transactions and therefore does not raise the alarm. This gives the attacker more time to transfer the money before the fraud is discovered.

None of the known attacks were discovered by antivirus software. This concurs well with the results of a government survey conducted in Spain.

2.7.2.3 Distributed denial of service (DDoS)

DDoS[3] (distributed denial of service) is still considered one of the biggest threats on the Internet.

A DDoS attack involves attacks from a large number of infected PCs that are connected in a so-called botnet. To start with the PCs in the network are unknown to the victim. The attacker can activate/deactivate the PCs, meaning that the PCs that have been used in the attack and which the victim eventually blocks via his or her firewall are replaced by other PCs activated by the attacker. It is difficult for the victim to differentiate between real traffic and malicious traffic before the malicious traffic has caused damage. Continuously blocking PCs in a firewall is a major job for the victim as is requesting the web host of the attacking PCs to block these from accessing the Internet. Some web hosts are known not to comply with blocking requests – these are popular among DDoS attackers.

Of greatest concern is the fact that little can be learned from being attacked. There is a limit to what victims can do to prepare for the next attack and to protect themselves. Nonetheless, it is still important that institutions think through the situation that would arise were their institution subjected to a DDoS attack. Continuity and contingency solutions must be in place.

2.8 Web application development

The use of web applications is probably the area that presents the greatest security challenges. There are many reasons for this. The threat picture is very dynamic. It is more the rule than the exception that Internet software contains serious security holes. The Internet attracts attackers. An increasing amount of useful traffic is transmitted via the Internet and many financial institutions report their exposure to the Internet will increase.

Even reputable software developers appear to be incapable of developing code without security holes, and we have become used to accepting a large number of security updates. In light of the risks on the Internet, it is strange that applications are not, to a greater extent than they are, subject to independent security testing and security reviews before they are put into production. Risk analyses often are conducted on a general level, if at all.. In a few cases the analyses do reach down to the application and operating environment and analyse the application’s ability to protect against threats.

Kredittilsynet has pointed out vulnerabilities with respect to web development in earlier RAV analyses. Terms such as ‘SQL injection’, ‘header poisoning’, etc, are familiar terms in development departments. Over time best practices have been developed for the area of web development.

[3] Distributed denial of service (DDoS) is a technique in which an attacker sends a large enough number of queries to a service to cause it to go down, or in which the attacker conducts many logging in attempts with the wrong combination of user ID and password resulting in the user being shut out.

Organisations that develop and administer these have emerged. The Open Web Application Security Project (OWASP) is one such organisation and opened a Norwegian branch in 2008.
The OWASP Guide is a document of more than 300 pages and provides guidelines on how to develop secure web applications and web services. This is a continuous project that is updated all the time. It covers 'rich applications' such as asynchronous JavaScript + XML (Ajax). This covers the entire development process from policy, secure coding, threats and risk modelling to configuration, rolling out and maintenance, and covers many topics in detail such as authentication, authorisation, session management, data validation, etc.[4]

The vulnerabilities discussed make it harder for the user to discover the threats on the Internet and correspondingly more difficult for them to protect themselves against them. Even reputable websites have proven to contain one or more of the discussed weaknesses, which means that the user, without him or her discovering it, may have malicious software installed on his or her PC.

Creating security in every link is a challenge with respect to web development, especially in those cases where the services include software installed on the client ("thick client"). In these cases a supplier must take many different client configurations into account. Some client configurations have their own DNS[5], others do not, some are behind firewalls, others have different forms of portal solutions, and so on. It is too extensive a task for the supplier to produce bespoke versions for every variant. Instead the supplier delivers standardised security APIs[6] and facilitates the customer's use of as many of these as possible.

2.9 Identity theft

Identity theft via the Internet is growing, and securing systems that enable interacting parties to identify themselves is becoming more important.

Financial institutions currently offer various forms of online identity control. All involve customers having to provide secret codes. The customer registers the code via his or her PC and the codes are transmitted to the institution and verified there. It is well known that a PC can be infected with malicious software, software that enables an attacker to get his or her hands on such codes. This allows an attacker to then misuse these codes.

[4] Source: OWASP, http://www.owasp.org/images/7/76/20080528_hva-er-owasp.pdf

[5] A domain name system (DNS) is an Internet name service that translates names into a computer number (IP address) and makes it possible to send information to the correct place on the Internet.

[6] Application programming interface (API) is the term given to an interface that enables communication between different software.

None of the identity controls used by financial services via the Internet today effectively protect against the biggest identity thief on the Internet, namely phishing.[7] This is a topical risk since attacks on online banks that result in losses are growing in other countries.

Given this there is reason to question whether or not current identity solutions are secure enough to justify their use in connection with transactions, agreements, etc, on the Internet. In particular this applies to transactions that by their very nature could have significantly negative consequences if an identity thief executes transactions and agreements, etc, in another user's name.

2.10 Regulations associated with ICT security

Much of the development taking place in Norway associated with information security is steered by international decisions and affected by regulations developed outside Norway. Below we provide some important examples of the developments that are helping to improve risk management, but which at the same time also require potentially demanding changes.

Basel II

The purpose of Basel II was to establish an international standard that banking supervisory authorities could apply when laying down regulations that determine the banks' capital adequacy requirements as collateral for financial or operational risks that may arise. Another aim of this type of international standard may be to protect the international financial system from experiencing problems if one or more major banks are no longer capable of fulfilling their obligations.

Given the experiences we have already seen, there is reason to believe that another look will be taken at the Basel II regulations to ensure that the regulations do not reinforce the crisis (procyclical) in a crisis situation, but instead help to minimise the scope of the damage if one or more banks fail.

Solvency II

Solvency II is a set of regulatory requirements for the insurance industry established within the EU and EEA. Solvency II is based on economic principles that enable the measurement of values and obligations. This will also be risk-based such that the risk is measured on the basis of stipulated principles and that the capital adequacy requirements will directly reflect this. The work on Solvency II has been going on for some time and the directive is expected to be implemented in 2012.

The data storage directive

In February 2006, the EU Parliament adopted a new European framework for storing telecommunications and Internet information as part of the work to combat crime.

[7] A technique for stealing identity codes that consists of an attacker impersonating the bank by presenting the customer with a copy of the online bank's logging in page and fooling the customer into providing his or her identity codes.

The directive is regarded as EEA relevant and thus binding for Norway. The directive covers storage of a range of information associated with data and telecommunications such as telephone numbers or user IDs, the names and addresses of those who are calling and the people being called, dates, times and the duration of the communication, as well as where the equipment was located. The information can be stored for between six months to two years.

The directive has generated a great deal of debate in Norway, and there is a great deal of scepticism about the directive. The Norwegian Data Inspectorate is one of the strongest critics of the directive and claims that introducing the directive will result in a number of changes that may threaten privacy protection.

National guidelines

The *"National Guidelines for Improving Information Security 2007-2010"* were drawn up in 2007. The guidelines are intended to create a common understanding of the challenges we face and identify areas in which there is a need to make an extra effort. The guidelines are intended to promote a better understanding of how all users, developers and suppliers of ICT can contribute to the development of, and benefit from, a culture of security in this area.

Report to the Storting No. 17 (2006—2007) points out the need to ensure good protection of the Norwegian information infrastructure through preventive measures. This involves being prepared for ICT security events with contingency measures and ensuring that security work is maintained and strengthened through measures such as competence training and standardisation.

Europe/EU

Several measures have been implemented that will also apply to Norway. These include the establishment of a European strategy group within security research (European Security Research and Innovation Forum – ESRIF), which is expected to have a positive effect in the long-term. ESRIF was both established and supported by the EU, and Norway is represented in the forum. ESRIF was established to contribute to the cooperation on security related research and preparation of strategies and policies – and the implementation of measures. The goal is to ensure the general level of security in Europe is improved, as well as the security associated with ICT. The security threat in Europe is becoming increasingly complex and European countries are having to increasingly trust each individual country's security regime.

3 Kredittilsynet’s findings and observations

As in previous years, this RAV analysis is based on the knowledge and information Kredittilsynet gained through its IT inspections, interviews with key players, reports about ICT events, and the follow-up of the notification duty on systems for payment services. Information from national and international organisations and bodies also made an important contribution to this RAV analysis. The greatest risks are discussed in more detail in chapter 5.

3.1 IT inspections executed in 2008

20 on-site IT inspections were conducted in 2008. In addition to this, 35 institutions submitted self-evaluation forms covering the institution's IT activities in connection with ordinary inspections and were assessed in accordance with the procedure for simplified IT inspections.

Over a period of five years of intensive supervisory activity all of the major institutions and many of the smaller institutions have undergone one or more IT inspections. Kredittilsynet has accumulated considerable experience in on-site IT inspections through these, and we have noted a development in how the institutions organise their IT activities. The ICT Regulations are now well known in the finance industry and institutions are increasingly able to point to processes that support the regulations’ requirements. Meanwhile, unfortunate events do occur in the area of IT in the finance industry, which sometimes few people foresee despite the institutions’ own RAV analyses and other preventive measures. These are events that could have been avoided had relatively simple preventive measures been implemented. Established and documented processes are not always sufficient. The processes must be constantly evaluated and improved and, not least, they must be complied with.

The following are important findings from the IT inspections conducted in 2008:

1. Inadequate configuration management
2. Incomplete implementation of continuity and catastrophe tests
3. Inadequate or incomplete RAV analyses
4. Inadequate compliance with own change processes

In addition there are also other findings, which are relevant, but which are not discussed in more detail here. These include inadequate quality goals and quality monitoring, insufficient resources, competence back-up that is too weak (key personnel risk) and inadequate basic documentation, inadequately documented IT strategies, RAV analyses in institutions that are not fully carried out, and inadequate or insufficient security policies. The main findings are discussed in more detail below:

3.1.1 Configuration management

The institutions' ICT infrastructure encompasses all physical components, operating systems, networks, and systems for monitoring and operation. The technical infrastructures of large institutions in particular are complex and extensive, meaning that maintaining an adequate overview of the entire infrastructure at all times is a major challenge. Despite this the institutions need this overview to ensure good, stable ICT operations. From experience it is known that most errors occur due to errors that arise in planned changes. If institutions do not have an adequate overview of their own infrastructure, every change represents a major risk since many of the infrastructure components are mutually dependent. Therefore, the components' compatibility must be ensured by maintaining an up-to-date overview of the configuration of the institution's ICT infrastructure.

3.1.2 Catastrophe tests

Catastrophe testing is a vital element in ensuring that an institution has the ability to continue its own operations in the event of a catastrophe situation. Testing plans can in particular reveal deficiencies and weaknesses.

Section 10 and 11 of the ICT Regulations require training, exercises and the testing of contingency solutions to be carried out at least once a year and of a scope that provides confidence that the contingency solutions function satisfactorily. The tests must be documented so that their execution and results can be assessed afterwards.

Kredittilsynet's findings from the IT inspections that have been carried out may indicate that not all institutions carry out tests that can be regarded as adequate. This especially applies to the extent the results of the tests are documented. In Kredittilsynet's opinion a failure to document the results can make it difficult to monitor and improve the catastrophe plans on which the testing was based.

3.1.3 Risk management

Risk assessments have increasingly become tools that enable institutions to uncover vulnerabilities in IT systems and in the use of ICT. Risk analyses and the measures that follow from these may enable an institution to make IT systems more robust. This will help to reduce the probability of unwanted events occurring. The primary purpose of risk assessments is first and foremost to become aware of one's own risk situation and, based on this knowledge, implement risk reducing measures or in some other manner ensure one's own risk is properly managed. It is important for the institution to clarify what is an acceptable level of risk based on the institution's business strategy and the scope and importance of the activities.

One desirable effect is that the risk analysis 'protects' against losses and damage to reputation. Risk analyses are important tools for ensuring that the institution's goals are achieved and should form an integral part of day-to-day operations. One prerequisite for ensuring the quality of risk analyses is that they must be conducted by personnel who are in a position to assess risk at an adequately detailed level.

In Kredittilsynet's experience the inspections it has conducted indicate that many unwanted events could probably have been avoided if the institution had conducted a risk analysis of adequate quality. This is particularly true with respect to risk assessments linked to changes.

3.1.4 Change management

Kredittilsynet has seen a clear improvement in the institutions' work on improving processes and routines that support change management in the institutions. In larger organisations in particular in which the pace of change is very high, the processes and routines are well established. The risk process has also been assigned a key position in change processes. It is well known that "little strokes fell great oaks" and this also applies to changes. Small changes that it is assumed cannot affect other systems have resulted in long-term situations with inadequate availability.

The causes of the errors Kredittilsynet found were twofold: Firstly, the risk process had not been sufficiently thoroughly executed when a change was introduced, meaning they did not possess the knowledge necessary about the risk the change entailed to make the right decision about whether or not the change should be executed. Secondly, the established processes and routines were not adequately complied with. In Kredittilsynet's opinion these are the two primary reasons why changes go wrong and they particularly affect changes in technical infrastructure.

3.2 The institutions' assessments

In 2008, 12 interviews were conducted with key personnel in important financial institutions, primarily people who represent the area of ICT. These types of interviews provide a good picture of what an institution considers the greatest challenges and risks in the area of ICT. Interviews in institutions work especially well in those cases where the interviews have become regular annual features.

Further processing of the results of the interviews reveals the following main traits:

1) What does the institution regard as the greatest risk(s) with respect to its use of ICT?
Many institutions report of an intense pressure to deliver. The demands come from customers and from authorities. Many institutions think their IT department is going to great lengths, and that over time the customers' expectations have risen too high. For example, today customers expect banking and share trading services to be available 24 hours a day. Banks used to be open from 09:00-15:00 (15:45). The fact that such opening hours are expected makes significant demands on the operation and development of IT systems. In addition to this, IT departments in practice often have to take responsibility for phases that are supposed to be handled by others, e.g. in the specification, definition and prototyping phases, as well as during the development of user documentation. The consequences of unrealistic delivery demands and expectations are a major risk associated with ICT.

Given the public's expectation of services available around the clock, the time available for software maintenance, hardware maintenance and implementing changes is correspondingly short. This means changes should be subjected to greater testing and quality assurance before they are implemented. There is simply not enough time to make errors and possibly roll back to older versions within the implementation window.

The management and control of outsourced IT is an increasing challenge in light of the increase in outsourcing and the subsequent reduction in in-house competence.

2) What were the biggest problems associated with the area of ICT in 2008?
Many of the institutions think maintaining and controlling the basic platform, i.e. the basic infrastructure, is a challenge. The platform has become too complicated to maintain. This results in a lot of errors and downtime. If this involves an online service, the error can cause serious damage to an institution's reputation.

Monitoring and capacity planning are also reported to be major challenges. This applies to, for example, disc space, space allocated in databases, the number of threads in the application server, the number of simultaneous users, communications units' time-out parameters, etc. Everything has to work together and be tailored to the installation and loads at all times. Controlling this complicated interaction is a challenge.

The pressure to deliver mentioned in point 1 was intense in 2008 as well. The pressure contributed to systems that had been put into production proving to be of inadequate quality. This resulted in a large amount of maintenance, which in turn was at the expense of new development and improvements. This propelled some institutions into a vicious circle of maintenance and new implementation attempts. Genuine new development thus suffered.

Achieving a good dialogue and interaction between the business side and the IT side is always a challenge.

3) What criteria do you use to be able to identify these?

Events in institutions provide a good basis for identifying the biggest problems. The challenge lies in analysing an event and finding the root cause. In the absence of thorough analysis, the visible factors are often 'blamed' for an event. A typical statement we heard from customers in 2008 was: "There is something wrong with the online bank again." A more detailed analysis may reveal that the online bank application is in fact working normally, but that a software component or a hardware component 'further back' is failing. It is very important to conduct a thorough analysis so that one finds the real cause.

4) What does the institution regard as the greatest challenges in 2009 with respect to the risks from using ICT?

Satisfying the public's demands with respect to the availability of the systems is a major challenge. A high degree of uptime is expensive. To increase uptime by 0.2% from 99.6% costs significantly more than to increase uptime by 0.2% from 99.4%.

High uptime demands challenge the change management function, cf. point 1 above. Creating an operating environment (test environment) for quality assuring new services is regarded as one challenge for 2009.

Almost all the institutions report that the lack of integrated IT architecture and infrastructure is a challenge. The core systems may date from the 1980s. The system produces data for a data warehouse that was implemented in the 1990s. The core systems no longer receive data in files, but from web-based real-time systems that were developed after 2000. The systems reflect the architecture, etc, that was current at the time they were developed, and can differ substantially. Middleware has to be created that ties the whole thing together. This results in risks and maintenance in the middleware components. In addition to this, many of the institutions have merged and become part of a group. Other group companies may have made different choices to those made by merged institutions over the years. Seen from the standpoint of a group, IT is an extensive and multifarious collection of systems. Controlling systems portfolios and getting systems to integrate in a good way is a major challenge, and a risk that will be further addressed in 2009.

5) What does the institution regard as important issues with respect to ICT risks in 2009 that require the implementation of special measures?

a) Change management linked to implementation of new systems

Many important finance players plan to replace key systems in 2009. Because the systems are interrelated, there is a strong demand for quantity assurance and control at all stages.

b) Architecture
Almost all of the institutions plan to document their architecture in more detail and try to simplify the architecture such that it converges towards something more stable. Almost all of the institutions have recently established special positions and/or functions, and projects, within this important area.

c) Testing environments
Many institutions report challenges linked to testing. Today financial services are real-time and integrated, end to end, hence even small functional changes must be subject to regression testing against the entire function chain. Achieving this is a challenge, especially in those cases where the service has a (thick) client component that tests have to be carried out against. Adequate testing is one of the prerequisites for achieving the uptime goals.

d) Risk associated with deliveries from suppliers
Many institutions face challenges associated with the quality of deliveries from key suppliers. Many go so far as to say that it is unusual for a delivery not to contain errors. Some feel that they are, once the service has been put into production, almost part of the supplier's testing of the service.

Most of the institutions have outsourced IT services to a handful of suppliers. This results in concentration risk. The institutions' in-house IT knowledge is degrading due to the increase in outsourcing, which means that suppliers may not be properly followed up. Some institutions have initiated measures to attract and retain capable employees, not least within the area of IT security.

Follow-up in this area is a prerequisite for achieving the uptime goals, cf. point 4.

e) Access control
Many institutions report 'wear and tear' with respect to access controls and an inadequate overview of access controls. This has several aspects.

Access controls are spread out: in code, in access control systems, in software, as keys in software, etc. Many institutions report that they do not have a total overview and control.

Personal access rights are not always tailored to the individual employee's actual tasks and responsibilities. Many institutions have identified challenges within this area. Many also report that far too many have been assigned administrator rights in a system. The institutions have initiated projects to improve controls, and will continue this work in 2009.

The reason why many institutions want to focus on access controls now may be that increased disquiet at work may erode employee loyalty. An employee facing termination may wish to take information with him or her about customers, etc, so they have something to live off in the future. We have seen examples of this happening. However, protecting individual employees against suspicions of irregularities is just as important – it is difficult for an employee to commit irregularities within an area to which he or she does not have access.

f) Cessation of activities at one or more key suppliers
Many financial institutions fear the situation that may arise if an important supplier has to cease or suspend his activities for a shorter or longer period. This may happen as a consequence of the financial crisis. We know that many major suppliers have made loan financed purchases and that the financial costs have increased significantly and are straining liquidity. Activities may also be halted due to labour conflicts.

g) Network hardware
Many of the institutions report fewer periods of downtime due to errors in one or more network components than in previous years. Continuing this good trend in 2009 is an important goal.

h) Risk of viruses spreading
The increasing mobility of users also increases the risk of being infected by a virus or other malicious software. There are many sources infection and many institutions see this as a threat they will continue working on preventing in 2009. Among other things, the use of home offices is increasing, and laptops are perhaps not regularly in contact with the network and thus do not receive the necessary security updates. Moreover, there is a risk of being infected by a virus or other malicious software via memory sticks and email. The use of Facebook and other social sites is increasing, and with this so is the risk of viruses spreading.

i) Internet
Virus production has been industrialised. Attacks are increasingly targeting users and not hardware. English language services used to be the target of the attacks. This has changed. Attackers can now choose the language used in the malicious software they purchase. Many of the institutions regard securing online banks and other important web-based services as a priority task for 2009.

Many institutions report increased Internet exposure.

j) Process compliance and culture
Unwanted IT events are often caused by inadequate compliance with established processes. Many of the institutions are going to address this in 2009.

Some institutions have programmes aimed at creating a culture in which risk and vulnerability become more addressed.. Discovering and reporting vulnerabilities will be rewarded. In many cases, these programmes include improving risk analysis processes.

3.3 Reporting events to Kredittilsynet

3.3.1 Reported events and their categorisation

In November 2007, a voluntary reporting routine was established for events in Circular 31/2007 "Reporting of ICT events to Kredittilsynet". At the end of 2008 we can summarise the experiences gained after approximately 13 months' of reporting. Savings banks, commercial banks and branches of foreign banks in Norway, the Norwegian Central Securities Depository, the Oslo Stock Exchange and BBS have participated in the reporting, and EDB Business Partner ASA joined the reporting from September 2008.

Kredittilsynet received reports of 136 events in 2008. This is five times the number from the year before. Kredittilsynet was also informed about events earlier in the process than before, and principally by institutions themselves rather than the media or customers. In around 80% of the cases Kredittilsynet was informed via an email being sent to hendelse@kredittilsynet.no. In the rest of the cases Kredittilsynet was notified via telephone or letter by an institution or was informed about the event via the media or emails directly from customers. In those cases where Kredittilsynet became aware of an event via other channels, Kredittilsynet has routines for demanding a report about the event.

Kredittilsynet carries out an initial approximate categorisation of events using the loss event types in Basel II (the so-called 7 exposure factors). The events were categorised as follows:

1. Basel II: Internal fraud	1
2. Basel II: External fraud	5
3. Basel II: Employment practices and workplace safety	–
4. Basel II: Clients, products and business practices	–
5. Basel II: Damage to physical assets	–
6. Basel II: Business interruption and system failure	124
7. Basel II: Execution, delivery and process management	6

It is important to emphasise that the table only shows ICT related events. It is clear that most of the events fall under business interruption and system failure. This means that there is a need for a further categorisation in this area. Event reporting provides us with basic facts that are significantly better than in previous years and provides a basis for measures.

When distributed by business area it is not surprising that by far the most events are linked to online banks. Online banks for paying bills, securities trading, etc, are end services for customers that are open 24 hour, 7 days a week. These immediately represent a problem for customers when the services do not function.

The card payment system in shops and cash points is also services that are open 24 hours, 7 days a week, but these are more stable with fewer events reported. In the case of cash points the events often occur locally, and customers can use another bank's cash point instead.

In many cases the event picture is complex. The reported event may impact several services at the same time.

3.3.2 Further details about events linked to online banks by cause

Kredittilsynet has produced a system for analysing and categorising the underlying technical causes of events in order to enable more standardised assessments of the causes of events linked to online banks. The picture of causes behind online bank events (85 of our 136 events) has been broken down by the following categories:

Online bank – SW: Software errors (operating systems, database software, monitoring software, firewall software, communications servers, network software, application server software, etc).

- Faulty operation (programming error)
- Parameters: incorrect/inappropriate values
- Software located on disc instead of in local memory – results in long response times
- Insufficient capacity: Software is not programmed to handle the traffic
  (number of simultaneous users/threads)

Online bank – HW: The hardware the bank operates the online bank on, and the hardware in the bank required to reach the online bank, i.e. networks/communications hardware in the bank.

- Hardware has insufficient capacity to handle the traffic (e.g. too little memory)
- Faulty operation and full stoppages (e.g. due to power failures)

Online bank – network: Communications lines, routers and other communications equipment (hardware and software) outside the bank which the customer uses to reach the online bank and the software used in connection with the communications lines.

- Telecommunications lines fail (e.g. due to digging accident).
- Telecoms operator's equipment fails.
- Fire at Oslo Central Station means that Tele2's and Telenor's lines fail.
- Equipment's capacity is inadequate.

Online bank – application: The bank's network applications.

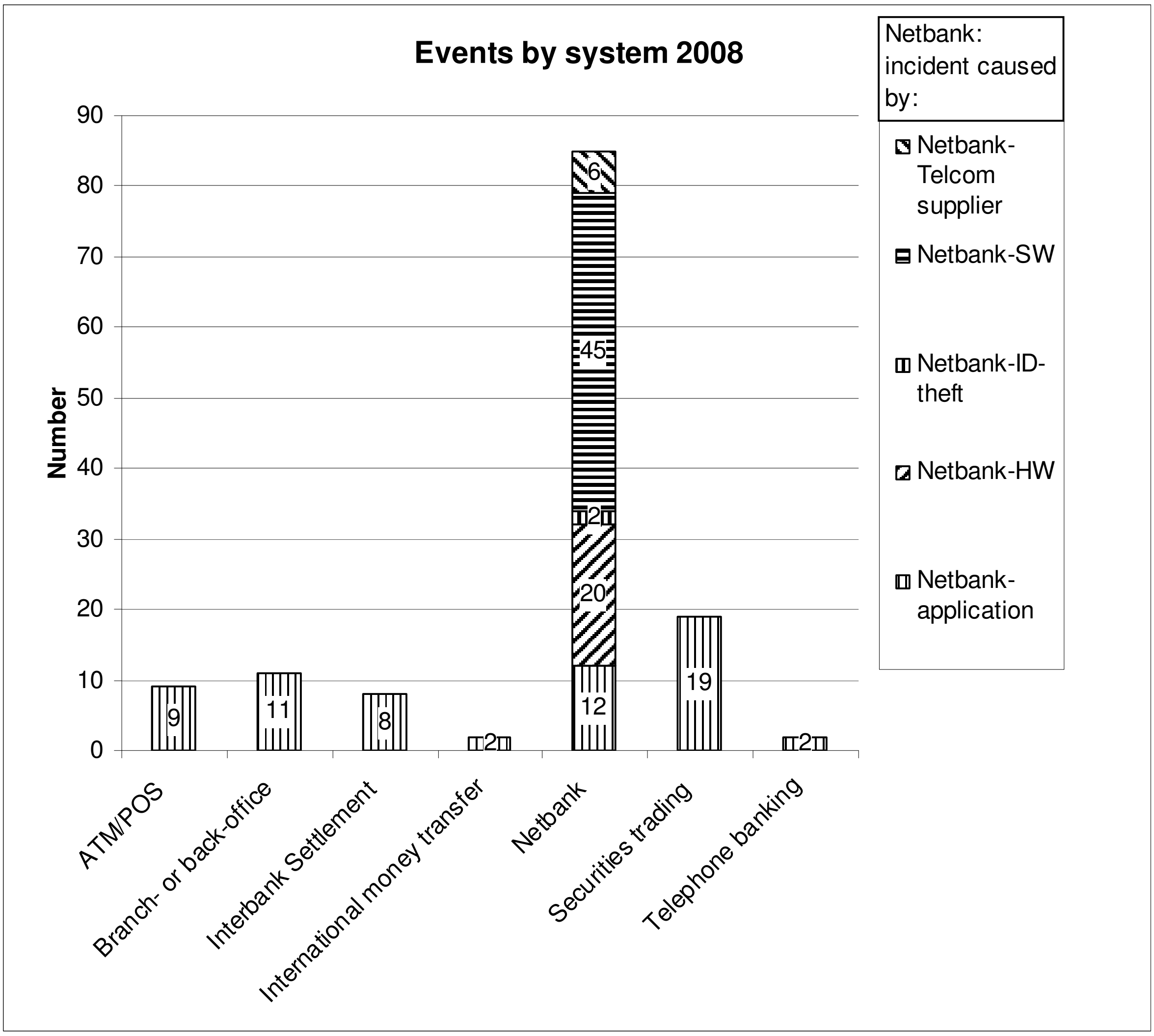
- Insufficient capacity: Application is not programmed to handle the traffic
- Faulty operation

- Error in an application outside the online bank has consequences for the online bank.
- Error in BankID application(s) means the online bank is unavailable.

Online bank ID theft:

- Man-in-the-middle attack (MITMA)
- Phishing
- Combination of phishing and MITMA
- Trojans
- The bank disseminates customer data by accident

Relevant events linked to online banks can thus be categorised as follows:



The reports show that greater attention should be paid to the online bank's technical environment and not only to the online bank application. This is new knowledge based on the total event reporting from 2008.

3.3.3 Number of reported events versus number of actual events

Often several different institutions report the same event at about the same time and these prove to be events that are rooted in the same technical error at the same supplier. In other words, in reality there were fewer events than the 134 events that were registered. Nonetheless, we chose to register every individual institution's event report as a separate event (except in those cases where the same error impacts all banks in one banking group such as the Terra Group or the SpareBank 1 Group, but these also report jointly for the group). The reason for this is an assessment based on the fact that the suppliers have bilateral agreements concerning the delivery of IT services with the individual bank or banking group, and that despite the fact that the same technical error caused the events, the events can impact the services differently at the various institutions. During the trial period we saw the same technical error at a supplier impacting more than one institution on around 10 occasions. Of the 134 event reports we registered, between 30 and 40 of them can be traced back to these 10 actual events. Most of these occurred at IT suppliers, but errors at network operators also caused events that were reported by multiple institutions.

3.3.4 General experience of event reporting

Kredittilsynet observed major differences in the number of events reported by the institutions, which cannot just be ascribed to the institutions' size or number of IT systems. Producing a description of which events should be reported was a challenge during the preparatory work on event reporting, and there is no set answer with respect to this. The circular came closest to defining this by stating that: *"The reporting shall normally cover events that institutions themselves categorise as very serious or critical, but can also cover other events if they reveal especially vulnerable points in applications, architecture, infrastructure or defence systems."* (Kredittilsynet's Circular 31/2007). This must be taken into consideration when the frequency of reporting from the individual institution is assessed. The institutions may have different scales against which they measure whether or not the event is serious enough to qualify for reporting to Kredittilsynet.

Some institutions have managed to put in place a well-functioning event reporting routine, while others appear to lack this. Our overall experience is that Kredittilsynet has a relatively up-to-date and correct picture of IT activities in the institutions Kredittilsynet receives regular and routine reporting from, while Kredittilsynet lacks an equivalent picture of the IT activities in institutions it lacks reporting from. Most of the institutions find themselves somewhere between these extremes.

The total volume of event reports, including underlying documents containing descriptions of the cause of the event, is a useful source for understanding how systems and networks interconnect. This is true for internal systems, systems that connect financial institutions, and systems that connect suppliers and financial institutions. Even though the individual event report only provides a fragmented picture, every report is one piece of a large jigsaw puzzle. As mentioned, many of the events stem from the same technical error at the same supplier. Kredittilsynet has observed, among other things, that the same technical error can impact different business areas in different institutions. For example, an event can impact online banking services in one bank and cash point services in another. The same event can be described differently by different institutions, which also fills out the overall picture of the situation. Together the information from the event reports functions as a source for mapping the infrastructure of the financial sector in Norway.

One important part of the follow-up of event reporting is the handling of events that are assessed as especially serious. Event reporting acts as an information channel for continuous status updates concerning the situation and provides a basis for Kredittilsynet's assessment of whether or not a contingency situation should be identified. Kredittilsynet will use data from event reporting as a basis for reporting to other government agencies such as the Contingency Committee for Financial Infrastructure (BFI) and the Ministry of Finance.

3.3.5 Events in 2008

The events were relatively evenly distributed over the year in 2008 with a slight peak at the end of June, beginning of July. The event that gained the most attention in the media in 2008 was the problems with the Oslo Stock Exchange's trading system on 2 June and 3 June. In this case Kredittilsynet was notified via the event reporting system on the mornings of both 2 June and 3 June. Kredittilsynet was kept continuously up-to-date on the status of the error handling via subsequent reports on both days. Immediate measures were initiated which later revealed the root cause of the event.

There were many cases of unavailable online banks that impacted many banks at the same time. There were also repeated problems with the trading systems in some banks, which was particularly unfortunate given the major fluctuations in share prices in the autumn of 2008. There were instances of phishing and other forms of ID theft. However, no successful trojan or man-in-the-middle attacks were registered.

Events which result in balance errors are very serious. In 2008, such events were rooted in errors in applications or systems software after programming changes. Luckily only a limited number of customers were affected, and the banks managed to correct the balances afterwards. The correction work necessary after these types of events is very extensive and often requires a substantial effort to be made by both involved suppliers and banks.

As the figure on page 28 shows, most of the online bank events reported to Kredittilsynet can be traced back to software problems. Therefore, maintaining control of the operating environment applications operate in is a major challenge. Software contains a number of parameters that all have to be set correctly and which may have to be reset if the traffic pattern changes, the configuration changes, or the interaction with the environment changes in some other manner. Monitoring the traffic and configuration, and keeping the software up-to-date so it reflects these, is a major challenge.

The institutions report challenges associated with maintaining the basic systems. Many of the institutions have several generations of systems, from CICS/PL1, IMS/DL1 and Cobol to more modern systems. Many have to operate systems that span decades, each system reflecting on the technical prowess prevalent at the time of installation. Differences in implementation exist in most layers of the OSI model, with the exception of the physical layer, but the differences between older and modern technology are primarily expressed by differences in the stratification and in the user interface. Maintaining the systems is an extensive job. It requires broad competence and a good overview. In most cases modern systems need to talk to older systems. A typical example is an older customer account system that is fed with data by a modern Web-based system and which may report this to a data warehouse. This means that middleware must be created that ties the systems together. This results in risks in the middleware components.

3.4 Other findings

3.4.1 Basic systems

Many of the institutions report challenges associated with maintaining the basic systems (the enterprise's core systems) in their infrastructure. Many of the institutions have several generations of systems that reflect the level of development, methods, architecture, etc, at various times. Maintaining the systems and getting them to 'play together' is a challenge. The observations from the institutions concur well with the events reported to Kredittilsynet. Of the 85 events that impacted online banks, 45 can be traced to software.

The challenge of controlling an ever more complicated operating environment can be resolved by increasing competence and staffing until one gains control and/or by reorganising and simplifying the software portfolio.

Kredittilsynet notes that many of the institutions have aggressive reorganisation, amalgamation and simplification plans with respect to software. In some cases institutions only use a small proportion of an application's functionality. However, the maintenance the application requires is not correspondingly small. An application's parameters have to be set, security updates (patches) have to be applied, versions have to be updated, etc, as if it were in full-scale use, and applications require the environment to be updated to specific levels. Many institutions are therefore taking a critical look at their software portfolio. Kredittilsynet has seen many examples of institutions that have uninstalled 'marginally used' software and replaced the required functionality with their own code or a smaller middleware component specifically programmed for the purpose. In Kredittilsynet's experience these institutions have gained a much improved, more stable and more comprehensible operating environment. Kredittilsynet has great faith in the value of such reviews and reorganisation.

Dominant and comprehensive control software results in constraints and guidelines with respect to infrastructure development. The software reduces an institution's freedom with respect to future architecture. Software suppliers naturally want their software to have a major impact on an institution's infrastructure in order to bind the institution to the supplier's software. Reviews and reorganisation can, as previously mentioned, loosen these ties and give an institution more freedom with respect to future development.

3.4.2 Access control

Having one system for access controls that covers all systems and users is difficult in an institution of any size. The principles on which access control is based vary depending on whether one is talking about personnel access, process access, or database access, etc. Process access, i.e. access rights automated process need to run, maybe is defined with the aid of user IDs and passwords written directly into the software, digital signatures verified by software with the aid of keys that are more or less well protected, and possibly other solutions. Personal user rights can often be controlled more readily with the aid of suitable administration systems. However, personal user rights are often subject to erosion over time, which typically results in a user gaining more rights than are strictly necessary for his or her actual tasks. We have seen examples of administrator rights being assigned to far more users than there is a real need for.

Controlling user right, particularly process user rights is seen as a challenge by many institutions. Many of the institutions have identified this as an area of risk and have initiated processes to rectify the situation. Kredittilsynet will follow up the institutions' work on this in 2009.

3.4.3 Testing

In Kredittilsynet's experience many of the events that took place in 2008 were, to some extent, rooted in the fact that in practice it is difficult to conduct full-scale tests of new services. Full-scale testing and regression testing are particularly difficult to achieve in practice. However, some events resulted in major damage and better testing would therefore have paid off.

Many of the new or upgraded services in 2008 were central services that also required prior upgrading of the user's in-house software. End-to-end testing in such circumstances requires a lot of coordination and it may be the case that some institutions make do with a function/regression test and smaller scale testing. However, should the implementation go wrong, turning this around might prove difficult in practice. Asking all customers to roll back to an old version and coordinating a restart of the old version would be a pretty hopeless task.

Kredittilsynet recognises that achieving full-scale and production-like testing is not a simple task. Technicians who work on systems development and operations at a practical level understand how important this is, and also how difficult it is to test adequately.

3.4.4 Outsourcing

Kredittilsynet has discussed the relationship between financial institutions and ICT suppliers in previous RAV reports. In Kredittilsynet's opinion there remain major challenges and some direct misunderstandings associated with the allocation of responsibilities between institutions and ICT suppliers.

Kredittilsynet is aware of cases of network operators preventing financial institutions from gaining an insight into aspects of deliveries regulated by the ICT Regulations. This is unacceptable. It is the financial institution that must ensure compliance with the ICT Regulations with respect to the institution's use of ICT. Financial institutions have a special responsibility with respect to ICT delivered by subcontractors, cf. Section 12 of the ICT Regulations. If financial institutions do not have an adequate basis for assessing whether or not the provisions of the ICT Regulations are being complied with when it comes to services provided by subcontractors, then the financial institutions may not use the service.

4 Systems for payment services

4.1 Payment systems in general

The Payment Systems Act (Act relating to Payment Systems, etc – 1999-12-17 no. 95) stipulates that systems for payment services (Section 3-2) must be reported to Kredittilsynet.

When systems for payment services are developed, purchased or modified, Kredittilsynet must be informed via the “Self-certification for systems for payment services” (Circular 17/2004).

The reports represent an important source of information for the work on RAV analyses. In 2008, Kredittilsynet received eight reports of modifications to systems for payment services.

The Payment Systems Act uses the terms “interbank systems” and “systems for payment services” for systems that together ensure the transmission of monetary transactions/messages between customers of financial instructions and between banks in the interbank market. The same is true for the requirement concerning the functionality necessary to ensure this takes place in a satisfactory and efficient manner. 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.

The financial industry’s payment systems are transmission systems with monetary settlements that are always directly linked to a commercial transaction based on physical goods, services or securities trading. This is one of the financial industry’s basic functions, which in modern times has developed from purely manual operations to today’s electronic transactions based on advanced ICT and applied message standards under the administration of the UN, ISO and the Norwegian Banks' Standardisation Office.

Interbank systems and systems for payment services constitute two parts of a payment settlement between different parties. Norges Bank bears supervisory responsibility for interbank systems and Kredittilsynet is responsible for supervising systems for payment services. The operative supervision therefore involves close cooperation with respect to both the continuous activities in the payment systems and the duty to report triggered by changes to existing systems and services, as well as the introduction of new functions and payment services. The applied systems handle the necessary processes between the customer and the customer's bank and between banks either directly or via settlement centres and Norges Bank.

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 financial institutions' operation of payment systems is mostly based on the use of ICT, normally as a combination of in-house and outsourced processes. The rules relating to the operation and development of such processes are covered by the ICT Regulations (Regulations on the use of Information and Communications Technology (ICT) – 2003-05-21 no. 630).

The administration and control of payment systems is an important element of the assessment of operational risk based on the rules in Basel II, which has been incorporated into Norwegian financial legislation.

A new payment directive that covers the EU/EEA will, when it comes into force on 1 November 2009, also result in amendments to the existing financial legislation, including to the Payment Systems Act. Work on a proposal concerning how to implement the directive in Norwegian law is well underway under the leadership of Norges Bank.

4.1.1 Payment infrastructure

From a technical point of view, the payment infrastructure is based on ICT infrastructure (see chapter 2.2 Infrastructure) and various interacting institutions. This is key to a payment system functioning as intended.

The infrastructure can encompass an institution's own organisation, including outsourcing agreements (computer centres), and cooperation agreements with other institutions (e.g. other financial institutions, clearing houses for payment transactions, and central banks).

The infrastructure's various elements and players must cooperate to achieve cost-effectiveness and ensure the flow of transactions within the limits of satisfactory operational risk.

Payment channels, payment instruments, and message standards are elements of the payment infrastructure that form the payment services and which interact in the financial provider chain when payment services are executed in the payment systems.

The payment systems generally consist of three main elements as defined by the European Monetary Institute:

1) definition of participants in the payment system
2) a set of payment instruments
3) defined procedures that must be followed.

The part of the payment system defined in the Payment Systems Act as a system for payment services consists of:

Payment channels
a. Letter
b. Branch/bank in shop
c. Electronic payment terminal (online bank, mobile bank, shops' point of sale terminals, etc)
d. Electronically transferred data files

Payment instruments
a. Codes (in connection with online bank, mobile bank, shops' point of sale terminals, etc)
b. Debit card
c. Credit card
d. E-Invoice
e. Direct debit
f. Mail giro
g. Giro (single and mass mailings)

Overview of message standards in payment networks
a. Self-controlled message standards
b. Common controlled message standards

1. NIBE
2. SWIFT MT and MX
3. EMV (international payment cards)
4. OCR
5. BOLS
6. Telepay
7. EdiFact
8. ISO (8583, 20022 XML)

4.2 Risks and vulnerabilities in the payment systems

NICS functions as the only complete clearing system for customer-based payment transactions in NOK at an overarching level. All Norwegian financial institutions that offer payment services deliver transactions to NICS during the day. NICS in turn delivers cleared net transaction data to NBO for use in monetary settlements and entry against the financial institutions' accounts in the central bank. The individual banks then update the customers' accounts.

In addition to this, two Norwegian banking groups are licensed by Norges Bank to offer interbank system services to other banks. The structures of these payment systems function as a hybrid in that the transaction clearance is executed in NICS, while the monetary settlement is executed via interbank accounts outside the central bank. In these payment systems customer accounts are in some instances updated before the interbank settlement has been executed (crediting before settlement). This can result in both liquidity related risk and the potential for losses.

NICS is a robust system that functions very well within a stable infrastructure based on approved types of message standards. The risks and vulnerabilities in this clearing system lie in the individual financial institution's core and customer systems and in NICS Operations at BBS. Such systems are intended to ensure the correct transfer of payment information and receipt of information about executed transactions.

Kredittilsynet believes that when it comes to the so-called level 1 and level 2 banks it is important that the individual bank is properly classified with respect to NICS. If they are not, this may result in differing perceptions of their own responsibilities with respect to participating in NICS, resulting in the individual institution assessing operational risk incorrectly and having an erroneous perception of where ultimate responsibility for a transaction lies. Kredittilsynet believes it is necessary to conduct a new analysis and clearly define how the various payment systems should be understood and operated in relation to the Payment Systems Act.

An increasing risk has also been identified in the payment systems in that new, smaller banks especially have too simple a perception of their participation in payment systems. The belief that these banks' provision of payment services can be based on a 'plug and play' concept in which the bank can quickly connect to existing systems can result in inadequate management of the operational risk. A number of players in the payment infrastructure are responsible for this perception. Kredittilsynet will point out these weaknesses through contact with and inspections at various banking groups in order to help ensure acceptable management of the risk.

The increasing competition between the financial institutions and their offer to customers of electronic payment channels open 24 hours a day may result in increased risk in the payment systems. This arises from frequent conceptually based demands from the business areas concerning changes to products and services. Another factor is the ability to operationally implement such changes in an increasingly more complex ICT infrastructure in which making time for adequate testing represents a challenge. The risk picture can be reduced somewhat with a more formalised horizontal organisational focus through better coordination between the banks' income-focused business areas and the costs-based operational areas, particularly in ICT.

5 Preparedness – National ICT 08 Exercise

5.1 ICT 08 Exercise

The Norwegian Directorate for Civil Protection and Emergency Planning (DSB) and the Norwegian National Security Authority (NSM) conducted a national exercise in 2008 called the ICT 08 Exercise. The exercise focused on society's ability to be prepared for, discover and manage a massive attack on Norway's digital infrastructure and encompassed the financial, telecom, energy and oil and gas sectors. Enterprises in these sectors were invited to participate in the exercise. Kredittilsynet participated in the exercise along with eight other financial institutions. Kredittilsynet was assigned the role of coordinator of the financial sector's participation in the exercise. Institutions from the securities sector, banking sector and IT suppliers were represented. Besides the institutions that were directly involved in the scenarios, the banks' associations also participated in the planning and execution of the exercise.

The exercise was paper-based and did not involve technical encroachments on the systems. It had the following objectives:

- Understanding the various responsibilities and roles of the different decision-making levels before, during and after an event.
- Determining the usefulness of the established plans.
- Vertical and horizontal information sharing for the different decision-making levels before and after an event.
- Media management and crisis communication with customers/general public before, during and after an event.

The exercise was designed to be as close to reality as possible for the participants. An exercise team covered the events as journalists and produced various news items for a web-based media simulator.

The actual exercise took place between 1 December and 3 December 2008. A number of events impacted the financial sector during these days. These were dominated by distributed denial of service

(DDoS) attacks against the websites of financial services such as online banks, etc. There were also other forms of malicious attacks against electronic services.

5.2 Post-exercise summary

The financial institutions found it very useful to have an opportunity to exercise together with other institutions in their own and other sectors and with a scope that it would be difficult and complicated to organise alone. This provided the financial institutions with an opportunity to test their communications with external suppliers and authorities, as well as their in-house communications. Notification lists and liaison points/contacts were updated.

The exercise enabled the financial sector to train in handling a situation in which many financial institutions are impacted by the same events instigated by external attackers. The most important thing for financial institutions in a crisis situation is to provide correct information and avoid panic among the general public. The exercise showed that in a crisis situation one had to be able to quickly initiate continuous media monitoring and consequently increase staffing levels in the institutions' communications departments to handle the expected media pressure.

The exercise also showed that it is difficult to gain a consistent and correct overall picture of a situation in which many institutions are simultaneously impacted by the same events and the media provides substantially differing information. Underreporting to Kredittilsynet's event reporting routine was registered during the exercise. This was primarily due to technical exercise failures, but one cannot exclude the possibility of there being acertain sluggishness in the institutions' reporting to Kredittilsynet. Besides the event reporting to Kredittilsynet there is no automatic process that ensures information from one financial institution flows to other financial institutions or common bodies.

The financial sector handled the attacks themselves operationally, i.e. there was no need to ask the Ministry of Finance to initiate measures. Web-based services in the financial sector are not as critical as, for example, point of sale terminals and cash points. The financial institutions were able to practise bringing reserve solutions online in the event of attacks on their services. The scenarios in the financial sector triggered further exercise scenarios for NorCERT, the Norwegian Post and Telecommunications Authority, and telecoms operators who participated with respect to monitoring the attacks against the networks and implementing measures from their side.

6 Identified areas of risk

6.1 Execution of catastrophe tests

The importance of ICT in institutions' business critical processes steadily continues to grow. This combined with the fact that an increasing need for services demands 24 hour operations, year round, means it is important that organisations have control over their own data and ICT infrastructure in case a catastrophe situation occurs. Comprehensive, detailed plans are crucial with respect to how quickly one can re-establish the business critical processes. Such plans require the establishment of a process that ensures that relevant documentation is updated when changes are made to the ICT infrastructure, management, notification lists, purchasing processes and so on.

Section 10 and 11 of the ICT Regulations require training, exercises and the testing of reserve solutions to be carried out at least once a year and of a scope that provides confidence that the reserve solutions function satisfactorily. The tests must be documented so that their execution and results can be assessed afterwards.

Kredittilsynet regards testing catastrophe solutions as a vital part of ensuring that an institution has the ability to continue its own operations in the event of a catastrophe situation. Simply testing plans can reveal deficiencies and weaknesses. Conducting large-scale, comprehensive catastrophe tests in larger institutions can be resource-demanding meaning that 'live' tests are not conducted every year. However, those parts of the institution's plans that are not covered by the testing should be subjected to special risk and vulnerability analyses.

In Kredittilsynet's opinion documenting the results of catastrophe tests and accompanying risk analyses is vital with respect to following up and improving the tested catastrophe plans. The quality of the tests is determined by their level of detail. Sloppy and haphazard plans will not be adequate for institutions subject to strict availability and ICT infrastructure requirements. Kredittilsynet will pay particular attention to institutions' catastrophe plans and accompanying RAV analyses and test results in its IT inspection activities.

6.2 Configuration management

Financial services are becoming increasingly automated. The scope and use of financial services on the Internet is increasing. The increased use of electronic services is making society increasingly reliant on the quality of these services. This means various types of events can having major consequences.

An institution's ICT infrastructure includes all physical components, operating systems, networks, and systems for monitoring and operation. Even the technical infrastructure of smaller institutions can be complex and extensive. Increasing demands concerning the availability of institutions' ICT infrastructure also make stricter demands on quality, and configuration management is often associated with the term quality.

The purpose of configuration management is to maintain an overview of all the components in an ICT infrastructure, the connections between these, and which versions the components are. This information is important, especially for the organisation responsible for the operation of the ICT infrastructure, if one is going to be able to offer a high degree of quality in the execution of the change management and problem management processes. As a rule, institutions subject to high uptime demands have strict configuration management requirements.

From experience it is clear that most of the events that result in downtime in ICT infrastructure components arise due to errors in planning modifications. This may indicate that the ICT infrastructure has not been adequately documented. This means it is unclear which versions of various components are in use and how the various components depend on other components. In Kredittilsynet's opinion it would be an advantage if this area were paid greater attention. The framework laid out by IT Infrastructure Library (ITIL) is regarded by many as the best practice for deliveries of ICT services and customer support.

6.3 Networks

A network is an element of infrastructure that allows two or more computers to talk to each other. A simple network can consist of two PCs communicating via cable, infrared connection, Bluetooth or a similar method. Larger networks can have several hundred thousands computers connected to one and the same ICT infrastructure. The financial industry has traditionally outsourced large portions of its network deliveries to suppliers of network services.

In Section 3 of the ICT Regulations Kredittilsynet has stipulated a requirement that every institution must conduct RAV analyses of their entire ICT infrastructure at least once a year. This includes network deliveries. During 2008, a number of financial institutions analysed vulnerabilities and threats in their network infrastructure in detail, precisely with a view to finding solutions that could provide a higher level of certainty that the institution's services would remain available. Information about the institution's network solutions must be available in order to conduct RAV analyses that encompass the entire ICT infrastructure. A number of institutions report that in many cases it can be difficult to obtain an overview of the network infrastructure.

Kredittilsynet has been informed that there are cases in which it has been difficult for an institution to get the telecom operator to provide an account of the topography of the institution's network. In Kredittilsynet's opinion it is important that institutions have access to adequate information about their entire ICT infrastructure in order to assess their own exposure in relation to risk. As mentioned previously, this is about a customer's right and duty to examine the product they are purchasing.

6.4 Offshoring

Buyers of outsourcing services are increasingly moving ICT tasks to countries in which prices are lower. This trend can also be clearly seen in Norway at suppliers such as Accenture, EDB Business Partner ASA and Capgemini. Even though lower costs remain an important driver in the growth of so-called global delivery models (GDM), more 'mature' buyers are also seeking better coverage of their needs to obtain the labour capacity they need. GDM is still a new concept and there may therefore be reason to assume that delivering robust and consistent services via GDM may present challenges.

About ten years ago global market players such as IBM and Accenture commenced expanded activities in India. India will continue to be the most important GDM country in the medium to long term, but a number of countries are following its lead such as the Baltic States, Ukraine and the Philippines. Both IT service suppliers and customers of these have to some extent chosen to establish a presence in India and some other countries, often through the acquisition of local companies. In the last few years, Indian suppliers have increased their annual turnover by about 60% in Europe.

Application services were the first area that was outsourced and moved to a different country. The number of services that can be procured via GDM is increasing and, for example, testing services have become a standard offer. Some types of service are at an early stage and it could in the opinion of the Gartner Group take some time before they mature. Infrastructure services (technical operation) and business processes, among others, are still relatively immature areas compared with application services.

Varying quality, challenging personnel growth management, and a large through-flow of employees often create great challenges for both customers and suppliers. In Kredittilsynet's opinion strong cooperate cultures need to exist to tackle these types of challenges. The institutions that have successfully established a presence in India and other relevant outsourcing countries are primarily institutions that have traditionally had strong cooperate cultures and transfer this to the organisation in the "offshoring country".

6.5 Change management

The change management process is an important process that encompasses receiving change requests, categorising, assessing needs, planning, assessing costs, analysing risk, testing, approving, implementing and status reporting. The purpose of the process is to gain control of all the changes in the institutions' ICT infrastructure and thus also reduce the risk associated with changes.

Kredittilsynet has seen a clear improvement in the institutions' work on processes and routines that support improved change management in the institutions. This has also been necessary since the pace of change has increased. In Kredittilsynet's opinion it is vital to have adequate documentation and knowledge about the ICT infrastructure in order for the change management process to function as intended with satisfactory quality.

In Kredittilsynet's opinion there are two reasons why a relatively large number of changes fail. One of the reasons is the quality of the risk process and the activities that this process initiates from a change message being reported until the change is implemented. The second reason, and in Kredittilsynet's opinion the most common, is that the established processes and routines are not adequately followed. This can largely be traced back to the culture the institution's IT organisation has with respect to established processes.

7 Kredittilsynet's future follow-up

7.1 Topical measures

The most important measures that can be enacted to manage operational risk are measures that are addressed in the individual institution subject to supervision. It is first and foremost through this absolutely fundamental factor that we can achieve appropriate risk management. The measures that Kredittilsynet can address as a supervisory agency will primarily be:

- Ensuring the implementation of IT inspections of a scope and with a level of detail that means Kredittilsynet will receive a realistic picture of how the institutions use ICT, manage risk and comply with regulations.

- Measures that support the institutions and their own activities. For example, this could be training and guidance material. Kredittilsynet actively participates in international and national cooperation in areas associated with ICT risk.

- Contributing to establishing cooperation forums linked to problem areas in which it is important to share information and discuss common measures.

- Ensuring active administration of the regulations associated with operational risk in the area of ICT and at all times formulating relevant requirements for areas of activity and the use of ICT where this may be appropriate for ensuring satisfactory risk management.

- In 2009, Kredittilsynet will work to ensure that telecoms operators make the necessary and precise information available. At the end of the day this is about the customer's right to examine the product they are purchasing. This is a statutory right, cf. Section 3 of the Sale of Goods Act, which provides customers with a right and a *duty* to examine deliveries.

Kredittilsynet has established various means in its work on operational risk linked to the financial sector's use of ICT. Below we provide an account of how the future work on the means will be organised so that this can contribute to proper operational risk management.

7.2 IT inspections

The work of conducting an adequate scope of IT inspections will continue. This is an essential instrument and suited to ‘taking the temperature’ with respect to how the financial sector manages the use of ICT and the risk associated with this. The challenge will be to develop the supervisory system further so that relevant problems can be identified through the most rational use possible of resources, both in the supervisory units and in Kredittilsynet.

Kredittilsynet’s experience from IT inspections must be actively utilised as a ‘thermometer’ in order to implement suitable measures and as a basis for grading and comparing relevant institutions.

The work on developing the IT supervisory system further as separate modules will continue. This is the best way of ensuring the system enables appropriate modules to be picked and chosen for individually planned IT inspections.

One goal is to make the individual supervision modules available from Kredittilsynet’s website so they can easily be retrieved and used in the institutions’ own work on operational risk and ICT security.

7.3 Further development of the notification system for systems for payment services

Section 3-2 of the Payment Systems Act states that "*The Banking, Insurance and Securities Commission shall, without undue delay, be notified of the establishment and operation of a system for payment services.*"

The notification duty is discussed in Kredittilsynet’s Circular 17/2004. This emphasises that in those cases where the introduction of a new system or new versions of a system for payment services significantly affects related parties, or where new versions of functions and other functional changes are significant vis-à-vis established systems, this will trigger the notification duty. The circular and form are available from Kredittilsynet's website.

Kredittilsynet is working on a system that will better enable it to identify possible problems associated with systems for payment services, depending on the messages that are received pursuant to the law.

Similarly, a new supervision module has been created for systems for payment services that will be used in a combination of IT inspections and follow-up of the work on ensuring quality and risk management in the payment services. The plan is for this module to be available from Kredittilsynet’s website in the first half of 2009.

7.4 Risk and vulnerability analyses (RAV)

Conducting regular RAV analysis to secure an understanding of the existing risk and, on the basis of this, implement measures in the areas where these are necessary are important prerequisites for appropriate risk management.

This is the main reason why Section 3 ‘Risk analysis’ of the ICT Regulations stipulates that annual risk analyses must be conducted.

The most important measure Kredittilsynet can take is to ensure that institutions subject to supervision comply with Section 3. As mentioned previously, in Kredittilsynet’s opinion conducting RAV analyses is a demanding process and requires knowledge about the execution of such processes while at the same time one needs access to adequate competence in the business areas and areas of technology the RAV analysis is going to cover.

To help with this Kredittilsynet has prepared simple guidelines for compliance with Section 3. There are many relevant standards and methods for conducting RAV analyses. Therefore, it is important the institutions acquire the knowledge necessary to ensure the execution of RAV analyses, which is a management responsibility.

Kredittilsynet will on its part continue to conduct annual RAV analyses across the financial sector to obtain insights and knowledge that in turn can be used as a basis for following up the institutions further. Improving competence and techniques so RAV analyses can be conducted in the best possible manner will therefore be important.

The international institution ECM, one of whose important business areas is ICT security, has stated that the following is a problem: *“Organisations cannot secure what they do not manage”*. The statement is intended to address fundamental factors. If an enterprise has not ensured it has secured an appropriate administration, organisation, clarification of responsibilities, documented and written relevant processes and procedures, secured managerial capacity and competence, it will be difficult to establish security solutions and appropriate risk management. The fundamental elements need to be put in place first so one can then construct the necessary systems for managing risk and security.

Another important job Kredittilsynet started in 2008 is mapping the ICT infrastructure used in the financial sector. Important conclusions have already been reached from the work in 2008 with respect to management and control, technical problem areas and the supplier situation. A report from this work containing interim results will be prepared and followed up with the relevant individual institutions and cooperation structure, at the same time as the work in this area will continue into 2009.

7.5 Event registration and reporting

The event reporting trial was established November 2007. It has been decided to continue this. The evaluation has shown that this is a useful means of securing correct information about the event picture in the financial sector and that it provides a good basis for analyses and measures. In 2009, work will be started to incorporate event reporting into the ICT Regulations...

The event database was an important source in the work on the RAV analysis in 2008. Information from the event database will be used as a basis for analysis so that problems in ICT areas that require measures can be actively brought up.

7.6 Information and communication

The work of continuing forums and a close dialogue with industry organisations and other relevant partners will continue. Key reports and guidelines will be published on Kredittilsynet's website in order to help improve knowledge and understanding of ICT risk management and security in the individual institution.

In 2008, Kredittilsynet contributed in 30 external seminars on topics associated with ICT risk and security. We aim to continue along the lines we have kept to until now in which we, at the request of individual institutions, industry organisations and other relevant partners, are positively inclined to make a contribution.

The work on developing guidance material will continue. Important topics in 2009 will include ICT management and control, and contingency plans and catastrophe solutions.