

Risk analysis, controls and compliance

Atle Dingsør, Financial Supervisory Authority of Norway (FSAN), ICT-supervision dept.

The responsibilities of the Financial Supervisory Authority of Norway (FSAN) are defined in a separate law (Law on the Financial Supervisory Authority of Norway). This law also defines which Financial Institutions (FIs) are under supervision by FSAN. To this law there is a bylaw, or regulation if you wish, which sets requirements on the financial institutions when it comes to Information and Communication Technology (ICT) in particular. The bylaw has clauses on

- planning and organizing ICT
- risks analysis
- quality- how to set target levels, monitoring and reporting
- security and data protection
- development and procurement
- maintenance
- operation
- incident and change management
- continuity plans
- contingency plans
- outsourcing and offshoring
- documentation

FSAN uses the control objectives of ISACA, the Information Systems Audit and Control Association, as a foundation for its work. We have modified, tailored and added on to the COBIT questionnaires, so that we now have a number of self-assessment questionnaires which the FIs fill in. Based on the answers and supplementary documentation, we do interviews with representatives from the FI under supervision. This in turn may spark in-depth interviews and investigations into areas that we find are potentially not satisfactory. Add to this that we also receive information from customers who have experienced downtime or errors, which we use as input to the inspections. FSAN also is in close contact with academia, to which it may contract special investigations. As from November 2007, the Financial Institutions are obliged to report major incidents to FSAN. Taken together, we hope that FSAN has a solid foundation for its opinions.

What then, were the main discoveries of FSAN during the last period?

Before Internet-banking, transaction processing errors (e.g. errors with OCR-scanners, counting machinery, teller terminals etc.) most often were contained within the “back-office” of the bank, i.e. errors often were not visible to the customer. With Internet banking, the user is a real-time observer as to whether the processing is successful or not. Errors affect him instantly. To a day-trader in shares, downtime could easily translate into money loss. Hence the risk and cost of errors to the FIs is magnified, for example in the form of impaired customer confidence or litigation even. Add to this that with ever longer and more integrated transaction chains, with non-banks entering the service chain, the number of vulnerabilities over the length of the chain increases also, giving a higher risk of errors.

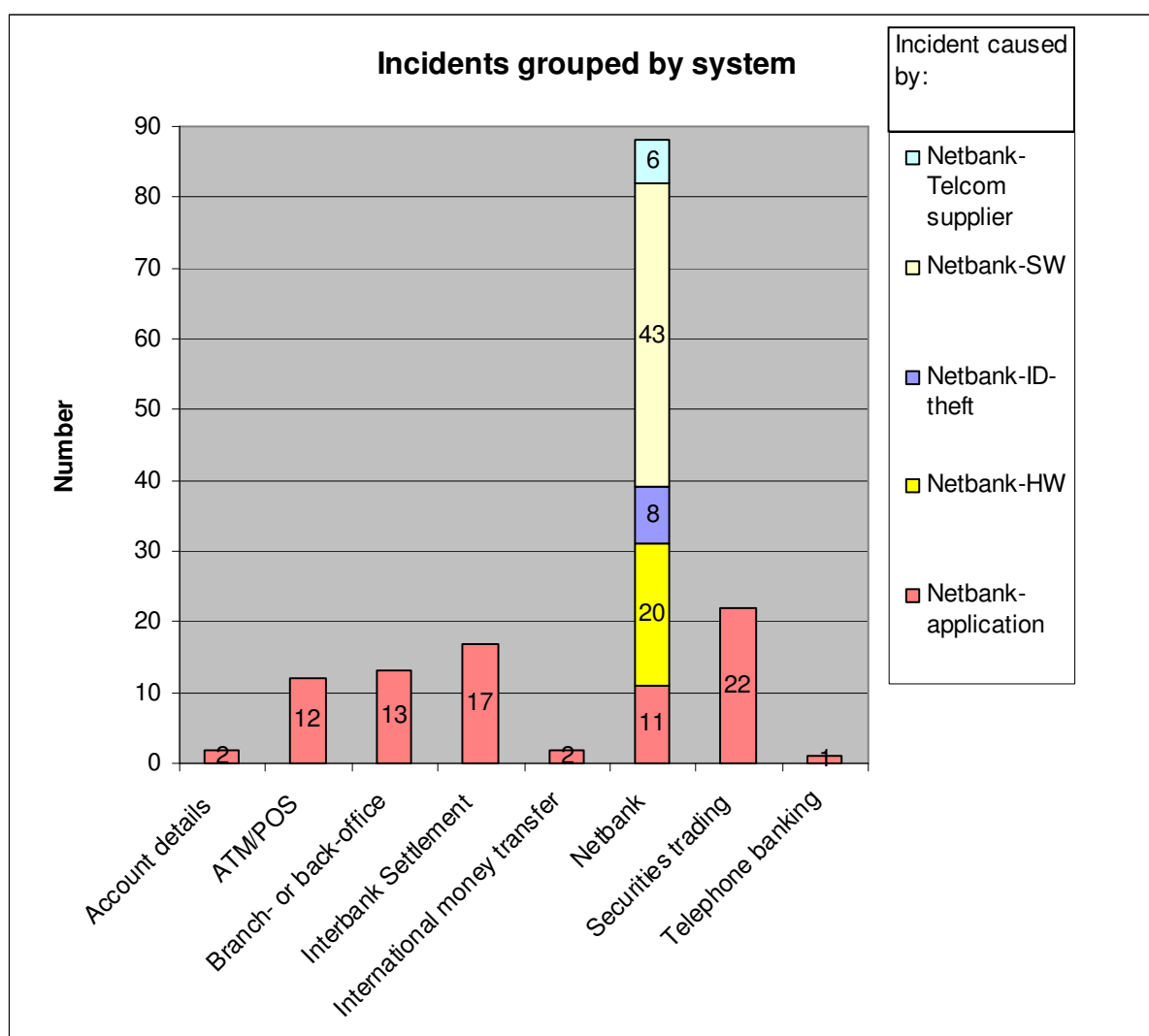
Many of the FIs report that the IT portfolio is getting dangerously complex. Many have a portfolio of systems that span decades, each system reflecting on the techniques etc. prevalent at the time of implementation. It takes a lot of resources and diverse skills to keep the systems

Risk analysis, controls and compliance

Atle Dingsør, Financial Supervisory Authority of Norway (FSAN), ICT-supervision dept.

running. The many different operating issues are thinly manned, maybe with one or a few persons responsible for a risk sensitive part of the operation. Being “thinly” manned, it is difficult to reap the security benefits inherent in “division of duty”. Many FIs are now attacking this problem head-on. Marginally used software is discontinued or maybe replaced by more targeted code, which might even be open source. Old mainframe based systems (e.g. Cobol/CICS) tend to become outsourced, to larger Cobol/CICS “factories”.

This observation tallies well with the sources of incidents that have occurred during the period. Complexity and mismanagement of the operating environment in which the applications run, seem to be by far the greatest source of downtime when it comes to Internet banking:



By SW we mean database servers, operating systems, applications servers, firewall software, other software used for operation, maintaining valid process users, certificates etc. It seems to be overly complex to keep track of all switches, parameters, variables, settings, expiry dates etc., their interrelationships and how they relate to changes in load and configuration.

Risk analysis, controls and compliance

Atle Dingsør, Financial Supervisory Authority of Norway (FSAN), ICT-supervision dept.

This again ties in with a clear trend towards operating issues becoming more focused. In their contractual agreements with suppliers, the FIs now have specific Service Level Agreements targeting supporting services like

- test environment
- monitoring (utilization, patterns of use/peaks)
- reporting
- log analysis
- audit
- control
- statistics
- follow up

and the like.

Several FIs are now into offshoring their ICT. ICT mega centres in low-cost countries serve several FIs from diverse countries, presumably giving cost savings for the FIs. When it comes to offshoring of IT-development, i.e. design and programming, to the best of our knowledge, there seems to be few outright successes among Norwegian FIs yet. Several offshore projects have been discontinued or brought “back home”.

When it comes to outsourcing of ICT operation, the picture is mixed, some are successes and some aren't. In this area several regulatory aspects have been identified and are now being looked into. Among these are privacy issues, data protection and contingency.

Several FIs have an uneasy feeling about user IDs. This applies in particular to process IDs, i.e. IDs that data programs use to log into other parts of the systems, e.g. to log into a database, or to open a file. Up through the decades, user IDs may have been set in clear text in the code, in clear text in parameters that are read on run-time or otherwise may not be sufficiently protected. Add to this that many process IDs have password set to not to expire, for obvious reasons, and you might have a problem.

On three major incidents that hit the Norwegian FI infrastructure the last 15 months, the contingency solutions turned out not work as expected. Additionally, FSAN has observed that on several incidents internal to the FIs, contingency solutions do not work according to plan. FSAN works out of the hypothesis that contingency solutions do not work, unless proven otherwise by a recent test. It seems that the configurations of the contingency solution on the one hand, and the system which it is supposed to replace on the other, very soon starts to deviate. It seems takes regular testing to unravel the discrepancies and align the systems again.

In these times of financial crisis, several FIs are worried that their ICT-suppliers get into liquidity problems which may impact the delivery. Over time, a trust-relationship may have been built up between the FI and the suppliers. Maybe code, documentation, test libraries and backups all are in the custody of the supplier. The FI now has to approach the supplier and take a firmer grip on these things. The FI also should verify the IPR of the delivery. Owner rights, user rights, reseller rights etc. no longer should be based on informal agreements, but should be firmly agreed contractually.

Risk analysis, controls and compliance

Atle Dingsør, Financial Supervisory Authority of Norway (FSAN), ICT-supervision dept.

Transaction chains are getting longer and more integrated involving many IT-service suppliers. Often it is hard to establish the point where the responsibility of one supplier ends and the next starts. The point where one supplier hands over the transaction to the next supplier in the chain often is a vulnerable point, both technically and with respect to hand-over of responsibility. Hence with respect to supervision and control, there will be shift of focus from the individual financial institutions as such, towards the financial value chains. There is a need for “cross FI-control” and monitoring in many areas. CoMiFin is an example of a EU-funded initiative that is addressing this. FSAN is a partner in the CoMiFin project.

CoMiFin addresses several threats to online banking, among them Denial of Service Attacks (DDoS). CoMiFin will collect data from many FIs, and correlate data in order to assess the real nature of the attack and to inform all partners as soon as possible and possibly to suggest effective countermeasures. For example, CoMiFin will provide Internet Service Providers (ISP) with continuously updated and reliable information on the sources of the attack that is targeting its customer. This information takes into account not only the traffic that is currently part of the attack, but also sources and trends of previous DDoS activities.

CoMiFin also addresses Man in the Middle (MitM) Attacks. By sharing and correlating information related to the source addresses from which financial transactions are initiated, it is possible to detect traffic pattern anomalies much earlier than any local detection algorithm applied by single institutions. Once a MitM server has been detected and communicated to a CoMiFin node, it is possible to immediately spread this information to all the other participants of CoMiFin. Automatic dissemination of MitM addresses can be used to build blacklists of compromised servers.

Some FIs are using data mining to unravel embezzlements performed by its own employees. The mining works out of the assumption that employees that are financially strained are more likely to embezzle money than the ones with a healthy financial situation. Hence the FIs develop for each employee “red flags” that are continuously being monitored. Examples of “red flags” would be

- loan/salary ratio
- overdrafts on the employer’s current account
- amount of debit interest accrued on the current account of the employee (which would be an indication of overdrafts),
- credits posted to the current account that are not salary entries
- funds credited to the employers account that come from accounts that are internal to the bank or is an inactive customer account

Low balance on the current account on the days before salary is paid, combined with a credit that has as its debit an internal account, and a corresponding debit taking place immediately after salary has been paid would arise suspicion.

Several banks also have policies and procedures in place to combat identity fraud. Indications of identity fraud would be:

Risk analysis, controls and compliance

Atle Dingsør, Financial Supervisory Authority of Norway (FSAN), ICT-supervision dept.

- Request for a change of address that is followed closely by a request for an additional or replacement card
- A transaction occurs on customer's credit or deposit account that has been inactive for two years or more
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
- The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry)
- An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - Nonpayment when there is no history of late or missed payments;
 - A material increase in the use of available credit;
 - A material change in purchasing or spending patterns;
 - A material change in electronic fund transfer patterns in connection with a deposit account; or
 - A material change in telephone call patterns in connection with a cellular phone account