Basel Committee's proposal, namely the supervisory review process. This ought perhaps to be complemented by allowing dynamic provisioning, i.e. by consolidating certain income from credit granting during prosperous times to cover credit losses during poorer times. Measures to increase transparency in the banks' exposures should be considered in combination with the dynamic provisioning.

Operational incidents in the banking system – two examples

The Swedish banks, in common with society as a whole, are becoming increasingly dependent on computer and communication systems. This means that software problems can have serious consequences not only for individual banks, but also for the payment system as a whole. Minor interruptions in computer systems occur almost daily at the banks. During the past six months, the Riksbank and Nordbanken have also suffered two serious, prolonged disruptions. Below follows a description of the two incidents, followed by a discussion of the consequences for the payment system and the systemic risks that similar incidents could entail.

THE RIKSBANK

In October 2000, the Riksbank's computer system for settlement of large payments between banks, RIX, suffered a serious disruption. A number of euro payments were sent twice, which led to incorrect bookkeeping. The Swedish banks therefore did not know their actual position in SEK at the end of the day and were unable to effectively balance surpluses and deficits between themselves. The fault was not detected until two days later, and was connected with the communication system linking the banks to the RIX system. It took a further three days to correct the fault and test the new solution.

Thanks to a well-established emergency procedure, the payment flows between the banks could continue without any major problem during this period.

Thanks to a well-established emergency procedure, the payment flows between the banks could continue without any major problem during this period.

NORDBANKEN

At the turn of the year, Nordbanken suffered disruptions to its computer system on several occasions. The problems, which started with the first computer breakdown in the middle of the post-Christmas retail sales period, were not resolved until three days into the new year. The effects of the disruptions were particularly extensive as the number of transactions is always much higher than normal around the New Year holiday. The fact that the bank's computer system could be made operational part of the time prevented what could otherwise have been a serious situation.

The problems could be traced to software that had been changed during the Christmas week. The situation was made worse by faults in the software for restarting the computer system, which had not

been remedied, despite amendments by the supplier several months earlier. The restart therefore took much longer than usual. The bank then tried to make up for lost time by running three days' worth of transactions in two days. The capacity of the system was inadequate for this and a decision was made on prioritising manually in order to steer resources from other parts of the system. Under these stressful conditions a couple of administrative errors were made by the operators, which made the problems even worse.

CONSEQUENCES FOR THE SWEDISH PAYMENT SYSTEM

These incidents are typical examples of what is usually known as operational incidents[41]. It can be observed afterwards that the Riksbank and Nordbanken escaped relatively unharmed in these cases. Incidents of this kind could in the worst possible case have had consequences not only for the bank concerned and its clients, but could also lead to serious disruptions in the payment system.

If a bank is unable (as in the Nordbanken case) to send off payments itself due to a computer error, while all of its counterparties continue to send money to the problem bank, this will result in liquidity becoming locked into this bank. In other words, the problem bank will have a surplus of liquidity, while other financial players will have a deficit. If the problem bank's computer system is not functioning, it might be the case that the bank cannot make use of the surplus liquidity, which would entail a total cost for the system. This could also cause short term disturbances to the liquidity of other banks.

In the Nordbanken case, the emergency routines in RIX were used, which enabled all transactions to be settled. However, in order for the emergency routines to function, it is necessary that RIX can receive the transaction data from the banks' internal computer systems. Fortunately, in this case Nordbanken's system functioned from time to time and could thus communicate transaction data to RIX. The situation could have been very serious if Nordbanken's system had instead been completely down for several days in a row over the New Year holiday period.

To avoid a contagion of this type of liquidity problem, the first thing the Riksbank can do, as soon as the problem is detected, is to inform the other participants and stop further payments to the problem bank. There is then an opportunity to transfer loans manually from the problem bank to other players. As a final resort, other players could borrow money from the Riksbank in its role as "lender of last resort".

The Nordbanken case also had consequences for the consumer end of the payment system. Bank clients now have the opportunity to carry out their business directly at bank offices if there is a problem with ATMs, telephone banking or Internet banking. However, this assumes that there are offices open, available and having sufficient capacity. Moreover, either the office's computer system must function or it must be possible for the business to be administered manually, directly or by storing transactions. As an increasing number

41 The Basel Committee defines operational risk as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events".

of banks are closing down their offices in favour of Internet services, the clients' access to this emergency channel is reduced.

INCREASED DEPENDENCE ON SOFTWARE

Nordbanken's software problem derived from software developed by several different software suppliers, while the Riksbank's software was developed internally. Today's software programs are increasingly complicated and integrated with one another. One problem is that the programs can react differently depending on how they are combined.

Errors in communication and software are often more difficult to detect and remedy than errors in the hardware.

Errors in communication and software are often more difficult to detect and remedy than errors in the hardware. The problem in RIX, for instance, arose only with certain combinations of payments and if there was a queue situation. One potential development is that future software will be able to detect and remedy faults itself. If the trouble-shooting routines in the software are not improved, there is a risk that increasingly complex and integrated computer and communication systems will lead to a greater number of operational incidents.

The incidents at the Riksbank and Nordbanken underline the importance of testing new programs in test environments that are as similar to the normal operating environment as possible and of developing and regularly practising emergency routines.

JOINT SOFTWARE SUPPLIERS

Operational losses differ from market losses and credit losses in that they do not normally affect several banks at the same time. However, apart from virus attacks, joint software errors could achieve this type of contagion among the banks. The Millennium bug, which it was feared would be able to hit several computer systems at the same time, is one example of this, but problems could also arise on a smaller scale. There are not very many international software suppliers, and it is reasonable to assume that the same basic software can be found in more than one bank. Errors can be found even among the products from the most well-reputed software suppliers, which is usually noticed sooner or later and amendments sent out to customers. However, these amendments, combined with all of the updates of the software, comprise a lot of information for the banks. Depending on the strategy of the individual bank and the instructions for program changes, this can lead to prioritising in many cases, which may prove to be a mistake. If several banks' computer systems are affected at the same time, a stability-threatening situation could arise.

If several banks' computer systems are affected at the same time, a stability-threatening situation could arise.

CONCLUSIONS

In order to avoid as far as possible software errors having serious consequences for an individual bank and for the payment system as a whole, it is important that:

- the banks' IT divisions actually follow the internal instructions as to when and how software changes can be implemented;
- the banks maintain good communication with their software suppliers, as well as support agreements that provide rapid support in the event of problems;
- banks developing their own software make sure they test it thoroughly under conditions as close to production conditions as possible;
- the banks have well-defined and rehearsed emergency routines and plans with clear rules for prioritising;
- the banks should warn other banks if they detect a joint software error. It should be noted that a software error that has an effect on one bank need not have the same effect on another bank, due to differences in integration with other computer systems and adjoining software;
- the information flow and co-operation with the authorities involved function in the event of incidents;
- the information flow to the general public functions in the event of incidents.

Increased financial stability through international standards

Financial crises lead to substantial socio-economic costs, as we have been able to observe in recent decades. Standards that provide guidance and specify best practices reduce the risk of financial and macroeconomic crises, provide a frame of reference and methods for evaluating a country, as well as providing guidance for the development of countries that do not yet meet the standards. International organisations push through the development of standards and they also carry out independent assessments of individual countries. The IMF and the World Bank, for instance, have standards that they use as a frame of reference when assessing a country's vulnerability to economic shocks and as conditions when granting credit.

WHICH ARE THE MOST IMPORTANT STANDARDS?

In order to optimise the use of resources, financial organisations representing both industrial nations and developing countries have agreed on a list of twelve prioritised standards. This list contains standards that define the information requirements for monetary policy, financial issues, fiscal policy and statistics, settlement requirements on insolvency and for ownership control, accounting, auditing, payment and settlement systems, as well as market abuse. In addition, there are supervisory requirements for banks, securities companies, securities markets and insurance companies.

The aim has been to select standards that will when combined provide protection against crises. These standards covary to a great