RISKS IN COMPUTER AND TELECOMMUNICATION SYSTEMS (July 1989)

The speed of technological innovation in computers and telecommunications in recent years and the integration of automated operations are increasing the dependence of banks on the reliability and continuity of their EDP systems.

Banks have always been exposed to risks such as error and fraud but the scale of those risks and the speed with which they can arise have changed dramatically. Furthermore, with computerised settlement systems, interbank lending relations now circle the globe in intertwining networks. Once a bank becomes unable to pay because of system problems, default, or any other reason, the banks that have loans outstanding to that bank also incur bad debts and the default is passed along the system in a chain reaction that threatens to envelop and paralyse the entire settlement system.

The types of risk which characterise an EDP environment and the security and control procedures it requires deserve the full attention of supervisors. This note addresses the following types of risks: improper disclosure of information, error, fraud, interruption of business due to hardware or software failure, ineffective planning and risks associated with end-user computing operations.

This paper has been prepared for reference by supervisory authorities in a wide range of jurisdictions. It is not designed as a technical paper for experts in the topic but seeks rather to flag the major problem areas of which supervisors need to be aware.

Improper disclosure of information

Most bank information is created by or directly linked to computer processing. Data and documents are routinely transmitted throughout a bank or between a bank and its correspondents and clients via public telecommunication links, such as telephone lines and satellites. Many users, including employees and bank customers, can directly access this data through computer terminals or telephones. These activities, while improving customer services and internal operations, have also increased the risk of error and abuse of the bank's information.

Much of that information is confidential and could damage customer relations and the reputation of the bank, as well as give rise to claims for damages, if it fell into the wrong hands. Customer balances, overdraft limits and transaction details are examples of such information. Correspondence and bank strategies are also created and stored through text processing. The particular danger of unauthorised disclosure of confidential information in EDP systems, compared with manual systems, lies in the fact that much larger quantities of information can be removed in a more convenient and processable form (e.g. copies on tapes or disks) and there may be no trace of unauthorised access having occurred.

Adequate security and control procedures are therefore necessary to protect the bank. The level of control must be assessed against the degree of exposure and the impact of loss (or disclosure) to the institution.

Technology controls for information security might include: encryption, a process by which plain text is converted into encrypted strings of meaningless symbols; the use of message authentication codes, in which a particular code is designed to protect against unauthorised alteration of electronic data transactions during transmission or storage; and the use of security application software designed to restrict access to computer-based data, files, programs, utilities, and system commands. Such systems can control access by user, by transaction, and by terminal. Security violations, including attempted violations, can be reported.

Errors

Errors typically and frequently occur during the entry of data and during the development and amendment of programs. Significant errors can also arise during the system design process, during routine systems "housekeeping" procedures and when using special programs to correct other errors. The cause is usually human failure, it being relatively rare for errors to be caused by failure of internal electronic or mechanical components. Errors can also be introduced into software packages where these are "customised" and adapted to meet the needs of a particular user. When purchasing standard software packages the aim should be to keep the number of changes to a minimum.

Fraud

Data flows in banking represent assets or instructions which ultimately move assets. The speed with which assets can be transferred using electronic payment and message switching systems complicates the task of internal control. Successful frauds will not only result in a direct financial loss for the institution but, when reported in the media, will detract from confidence in the institution and in the banking system in general. The wide variety of ways that computer records can be accessed creates many possibilities for fraud. For example:

- unauthorised transactions can be entered into the computer system;
- unauthorised changes to programs can be made during routine development or maintenance which may cause the program to generate fraudulent transactions automatically, to ignore control checks on selected accounts or to remove records of specified transactions;
- special programs can be used to make unauthorised changes to computer records in a way that bypasses the normal control and audit trail facilities built into the computer systems;

- computer files can be removed physically from a computer installation, amended elsewhere by the insertion of fraudulent transactions or balances and returned for processing;
- transactions can be introduced or intercepted and amended fraudulently whilst being transmitted through telecommunication networks.

At present, new forms of payment are being introduced permitting payments to be initiated by third parties using electronic equipment. This is likely to increase the probabilities of some of these types of fraud through unauthorised access to telecommunication networks.

Most banking systems contain control facilities and produce reports designed to assist in the prevention or detection of these types of fraud. These too, however, may be vulnerable to manipulation by persons with access to computer terminals or files.

In constructing effective systems of internal control, it is paramount to identify all the vulnerable points in each system. Critical records and programs must be particularly protected against unauthorised changes. Attention must also be given to ensuring that staff in critical areas are properly trained and that duties are appropriately segregated.

Interruption of business due to hardware or software failure

Computer systems consist of large numbers of individual equipment and software components, the failure of any one of which may bring down the system. Often these components are concentrated in one or a few places increasing the vulnerability to accidents.

The classical remedy for system failure was to revert to the manual processes that the computer system superseded. In the majority of cases this procedure is now unrealistic and few banks could operate without computer systems. The processing and delivery of information through improved technology has expanded management dependence on the availability and reliability of automated systems. The continued availability of a bank's information systems is integral to effective management decision-making.

When computer systems are out of action, the damaging effects on the real-time banking services to clients are immediate and increase rapidly. Processing backlogs develop quickly and, after a breakdown lasting several hours, these may take days to clear. Particularly devastating are the effects in the case of EFT and payment systems, in particular those providing a guaranteed same-day settlement service where beneficiaries depend upon receiving funds to offset their commitments. The consequential costs of a serious systems failure can far exceed the costs of replacing damaged equipment, data or software.

The existence of effective contingency plans is one way management can reduce the impact of similar operational problems. Such contingency plans should form an extension of a bank's system of internal control and physical security. It should include provisions for continuing operations and for recovery when the bank's systems become disrupted or inoperative, that is provisions for off-site backup of critical data files, of software and of hardware, as well as alternative means of processing information. The bank's contingency

plans should be tested periodically to demonstrate their continued efficiency. A bank that relies on an outside EDP servicer for its data processing needs should be certain that the servicer's contingency plans complement its own.

Ineffective planning

Sound planning is a crucial factor. Banking efficiency and quality of service are now so dependent on computer systems that any failure in planning or developing new systems may have significant commercial consequences. Failure in implementing new systems and providing new services quickly enough may place a bank at serious disadvantage with respect to its competitors. But, on the other hand, computerisation at all costs, especially where the benefits are marginal, has often proved to be a costly mistake.

Some financial institutions have experienced significant problems in attempting to introduce large-scale integrated financial systems. An integrated software system is a structure in which programs for different applications - loans, deposits, retail and wholesale - that normally are designed and operated as stand-alone programs are built from the start as related parts of a whole. This approach is adopted in an attempt to increase the timeliness of information, foster operational efficiency and ease the introduction of new products. In some cases the cost, time and personnel resources required for the successful installation of integrated systems has been underestimated. Projects developed over many years have been abandoned with enormous costs.

The complexity of EDP systems and their impact on the entire organisation require a commitment from top management for every project to be successful. Management should pay close attention to long-term (strategic) planning of computer systems, equipment and software, feasibility studies, specification of systems requirements, selection of suppliers and project control.

Risks associated with end-user computing operations

Until recently Personal Computers (PCs), microcomputers and end-user computing devices have played a relatively small role in system data-processing activities. Presently, the technological advantages, expediency and cost benefits of end-user computing have greatly increased the use of such devices, taking part of data processing out of the centralised control environment. Computer-related risks are now in new areas of the banks and very often basic controls and supervision of these computer activities have not been introduced. The main worry with end-user computing is that the implementation of these new information delivery and processing networks has outpaced the implementation of controls.

The risks are in general the same as those involved with mainframes but particular attention needs to be paid to the possibility of corruption or loss of data or software and consequent impediment to the efficient functioning of the overall operations network of the institution. Microcomputers are now being used not only as word processors but also as

communications terminals with other computers and stand-alone computer processors. As there is a tendency for these systems to be highly personalised and independent, with one single person often fully responsible for the development, testing, implementation, and operation of a set of programs, the possibility of the use of procedures and treatment of data different from and incompatible with the standards adopted elsewhere in the institution becomes greater.

Management responsibilities

The responsibility for ensuring that the operations are adequately protected against the risks described above rests with the institution's management. The first action required of management is the setting-up of adequate *preventive measures* designed to minimise the probability that the negative events described can occur. Examples of preventive measures are the careful design and siting of computer centres, data input controls, security devices to prevent unauthorised access to computer equipment, and passwords for restricting access to computer programs and data.

As preventive action can never be totally effective, management should also develop adequate systems of *containment measures*. These must be designed to detect and limit the effects on the business of events which bypass preventive controls and threaten banks' operations. Such measures should include dual capacity in telecommunication and computer networks to cover the risk of breakdowns, reconciliation procedures to detect errors and contingency plans for major disasters. A particular containment measure which should complement a carefully-drawn EDP policy is insurance against losses attributable to employees' fraud, costs of replacing data, and destruction of software or equipment.

Internal audit

It is also a responsibility of directors and management to review, monitor and test EDP control systems in order to assure their effectiveness on a day-to-day basis and their continuing relevance to the business. A regular programme of independent tests of security and control procedures by inspectors, auditors or consultants should be implemented. Such a programme should be capable of identifying lapses in control before they put banking operations seriously at risk. The frequency and depth of audit tests conducted in any area should reflect the level of risk to the bank if the security and control procedures in that area should fail.

Supervisory action

From the supervisory standpoint, there is a need both to evaluate the adequacy of an institution's EDP policy and the efficiency of its system of EDP internal control and auditing. One way for supervisors to discharge their responsibilities is to assess the situation by means of *questionnaires* or reports but more often this function falls within the

competence of external auditors or inspectors. A simple questionnaire or report is normally suitable for giving a preliminary indication to supervisors but should not be considered as a substitute for a detailed review by computer security or audit specialists. The subject is technically complex and in each bank there are considerable variations in vulnerabilities and control techniques among different types of system and equipment.

In such a specialised field it would be particularly helpful for the supervisor to take advantage of the expertise of the *external auditors*. They should be stimulated to devote sufficient resources to this part of their responsibilities.

It is recommended that external auditors' attention be drawn to this area by requiring banks to insert in the audit engagement letter a passage to the effect that the external auditor should periodically assess the soundness of the EDP processes which are vital to the institution's operations and the effectiveness of the internal EDP controls. The external auditors should also be asked to refer, in their annual management letter, to any shortcomings and imperfections which have come to their attention, in the course of their examination of this specific field.

Where the supervisors discharge their responsibilities mainly through *on-site inspections*, it is normal procedure for inspectors to include interviews, documentary inspections and sample checks in this area. Nevertheless, limitations of manpower and expertise, in addition to budgetary and other constraints, may make it difficult for inspectors to keep up with the development of new computer systems. Certainly it is now essential that inspectorates include EDP specialists whose training matches the level of EDP sophistication of the banks under inspection.

Both inspectors and auditors normally use, in their work in the EDP area, check-lists or examination guides prepared by supervisory authorities with the assistance of specialised institutions and these represent an extremely useful supervisory tool.