CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN

(Central Bank)

Policy Memorandum: Management of Computer Risks

WILLEMSTAD, Updated version April 2011

Policy Memorandum: Management of Computer Risks

I. Introduction

The application of computer and telecommunication technology is currently a wide-spread phenomenon in the financial industry. The trend towards increasing automation is likely to continue for many years. The success of an organization will thus depend to a considerable degree on the quality of its computer and telecommunication systems, and the extent to which it develops these systems to match the evolving needs of its business and its customers. Deficiencies in security and control procedures within those systems can pose a significant threat to the continuity of operations.

The purpose of this memorandum is to provide Senior Management with a firm basis for an evaluation of the risks inherent to the use of computer technology and to increase Senior Management's awareness of the general control elements that may be effective in safeguarding the institution's operations against such risks. The memorandum is also an aid to identify the automation related risks that threaten the effectiveness and continuity of an institution's operations and in understanding their potential consequences, which might be as extreme as prolonged closure.

This memorandum is not aimed at addressing all the detailed questions that are relevant to computer security and control in every installation, and so will not necessarily identify all vulnerabilities which may exist. The subject is technically complex and in each institution there are considerable variations in vulnerabilities and control techniques among different types of systems and equipment. Use of the memorandum cannot replace a detailed review by a computer security audit specialist, whether in house or external. However, by focusing on those controls which can make the greatest contribution to protecting operations, the memorandum provides a firm basis for a global evaluation of the computer security and control procedures in the electronic data processing environment of an institution.

Viewing the contents of this Memorandum one notes that a general introduction to the nature of business risks resulting from the use of computer and telecommunication systems is being presented in a policy framework. It describes the types of control which can be used to minimize potential risks and to ensure that systems are reliable and meet the needs of their business.

Throughout this memorandum, the term "institution" is frequently used as a shorthand for supervised institutions, and the general term "computer" for computer, microcomputer or telecommunication systems, including the applications being used.

II. Managing Computer Risks to Banking Operations

The successful management of computer and telecommunication risks requires effective mechanisms for identifying risks and assessing their consequences. Security and control procedures should then be compared and evaluated in terms of cost and the extent to which they reduce the risks of serious loss arising from inadequacies or failures in the computer systems.

In certain cases it may be possible that certain procedures which are appropriate for a large institution with substantial numbers of data processing staff are inappropriate for a small institution. In general, however, the nature of computer and telecommunication risks is very similar in both large and small organizations and effective security and control procedures are necessary in both cases.

In section III we will address the nature of computer risks and identify five (5) categories of computer risks that may pose significant threats for the institutions if left uncovered.

In order to protect the institution against undue risks, certain controls are described in section IV of this memorandum. These control measures represent a general framework of controls that must be in place to provide protection against computer risks.

III. Nature of Computer Risks

All institutions are exposed to losses resulting from errors and fraud. While it is arguable whether computers have changed the types of risks which exist, it is clear that they have changed the scale of those risks and the ways in which they can arise, as well as the types of security and control procedures necessary to contain those risks to acceptable levels.

This memorandum addresses the following areas which are related to certain types of risks:

1. Development risks;
2. Risk of errors;
3. Risk of business interruption;
4. Risk of unauthorized disclosure of confidential information and
5. Risk of fraud.

III-1 Development risks

Efficiency and quality of services are nowadays so dependent on computer systems that any failure in planning, controlling or developing new systems may have significant commercial consequences.

Major delays in implementing key systems may place an institution at a serious disadvantage in its competitive environment. Failure to anticipate advances made by competitors in their use of technology may lead to inappropriate systems being developed or to operational systems becoming economically obsolete.

The following aspects of computer development require particularly close attention by senior management: long term (strategic) planning of computer systems and equipment, feasibility studies, specification of system requirements, selection of equipment and software suppliers and project control by those in charge with implementation of computer projects (costs, duration and quality). Lack of attention to one or more of these aspects can lead to serious development delays, increased costs, failures of computer projects or inadequate operation of implemented systems.

It is important that all security and control requirements in a new system are immediately taken into consideration when the system is being specified and designed. Otherwise, new systems may be unreliable from the outset. Internal inspection and audit departments can often make a significant contribution in achieving good controls if they are consulted sufficiently early in the systems design process.

Those institutions which do not employ inspection or audit staff with the appropriate skills may find that their external auditors or outside consultants can assist. However, even in these cases proper awareness of the above mentioned aspects of computer development continues to be required for Senior Management.

III-2 Risk of errors

Errors can arise in a variety of ways and can affect customer service, operational efficiency and management and supervisory control. These errors frequently occur during the entry of data by terminal operators and during the development and amendment of computer programs. Significant errors can also occur, however, during the systems design process, during routine system maintenance procedures and when using special programs to correct errors. The cause is usually human failure. It is relatively rare for failure in electronic or mechanical components to be the cause of errors in computer data.

The complexity of computer systems may contribute significantly to the occurrence of errors. Most computer programs contain so many instructions that it is impracticable to test every logical path through them. Even when programs are well tested, errors can remain that may lie dormant for months or years until a particular set of circumstances occurs. When this happens, the results can be unpredictable. Often new errors are introduced during successive system changes.

Errors may also be introduced into standard software packages when these are "customized" i.e. tailored to meet the needs of a particular institution or user. This may pose a significant problem, which may grow as maintenance is carried out. When purchasing standard software packages the aim should therefore be to keep the number of changes to a minimum.

Based on the above, institutions are required to maintain good standards of error control in order to maintain accurate transaction balances and management information. Senior Management must at least be aware of the measures taken by operational management and staff to control the occurrence of errors.

III-3 Risk of business Interruption

Nowadays, once computers have been introduced few institutions can continue to operate for long without their computer systems. Computer systems consist of large numbers of individual equipment and software components, which may bring down the system if they fail. In most organizations, a considerable proportion of these components are centered in one place. Computer systems are therefore particularly vulnerable to breakdown, accidents and malicious damage.

Once the systems are out of function, the damaging effects on services, particularly for those institutions using on-line real-time systems, can increase rapidly. In some banks for instance, customers may be affected immediately as links to automated teller machines (ATM's) or other electronic networks fail. Processing backlogs develop quickly and, after a breakdown lasting several hours, these may take days to clear if there is insufficient processing capacity to cope with the additional load.

If its systems are out of action for several days or more, an institution may have to suspend its business unless adequate contingency plans have been specified and tested beforehand. The

consequential costs of a serious system failure, therefore, can far exceed the costs of replacing damaged equipment, data or software.

The particular importance of protecting an institution's software and data should be kept in mind by Senior Management at all times. Equipment can eventually be replaced, but if, in an accident, all copies of programs and data were to be destroyed, considerable time might elapse before normal operations could be resumed. Total destruction of unique software could require substantial efforts to replace. Similarly, loss of copies of data may cause severe disruption for a considerable period. At worst, a total loss of data or software could cause the prolonged closure of the institution. This event could occur if inadequate steps had been taken to protect the software and data against fire, other calamities or malicious damage.

Institutions must therefore protect their computer resources effectively against physical threats and have adequate backup and recovery procedures or standby arrangements in place and tested, to call on when events occur which cause computer systems to fail. These backup and recovery procedures should be maintained and adapted to changing circumstances as the computer systems evolve.

III-4 Risk of unauthorized Disclosure of Confidential Information

Much of the information stored in an institution's computer systems or transmitted through telecommunication lines is confidential and could damage customer relations and the reputation of the institution, as well as give rise to claims for damages, if it was to fall into the wrong hands. Word processing systems may contain records of customer correspondence and the institution's strategic business plans. Often confidential details of profit forecasts, staff salaries and personnel records are also stored in the computer. In this context, particular attention needs to be paid to private data relating to customers as well as employees.

Confidential information stored in computer systems can be accessed and read in a variety of ways. Potential avenues of unauthorized access include normal terminal inquiry facilities, use of special programs to read data files, physical removal of computer files or printouts from the institution's premises and the tapping of telecommunication lines.

A person may not have to move from his or her normal place of work to access the information and there may be no trace of unauthorized access having occurred. Compared with manual systems, much larger quantities of information can often be removed in a more convenient and processable form (e.g. on tapes or disk).

As with the other categories of risk already described, good security and control procedures are necessary to protect the institution.

These include effective physical security over computer files and good password control systems to allow different levels of access to different users. It may be necessary to encrypt highly confidential information, so that if it is stolen or intercepted, it cannot be deciphered and understood or manipulated.

III-5 Risk of fraud

Losses through fraud in computer systems can be considerable. Many of the computer records contained in these systems represent assets or instructions which ultimately move assets. The wide variety of ways in which computer records can be accessed creates many possibilities for fraud. The increasing dependence of internal control procedures on computer programs and the speed with which assets can be transferred using electronic payment and message switching systems complicates the task of fraud prevention.

There are several ways in which fraudulent transactions in computer systems can be generated. For example:

a) Unauthorized amendments to payment instructions can be made prior to their entry into the computer system;
b) Unauthorized transactions can be entered directly through terminals;
c) Unauthorized changes to programs can be made during routine development or during 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;
d) Special programs can be used to make unauthorized changes to computer records in a way that bypasses the normal control and audit-trail facilities built into the computer systems;
e) Computer files can be removed physically from a computer installation, amended elsewhere by the insertion of fraudulent transactions or balances and returned for processing;
f) Transactions can be introduced or intercepted and amended fraudulently whilst being transmitted through telecommunication networks.

Most computer 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.

Before effective controls to prevent fraud can be implemented, care must be taken to identify all the vulnerable points and areas in each system. Potentially vulnerable records and programs must then be protected against unauthorized changes.

In this respect it should be noted that testing programs and systems, although an effective means of detecting most of them may not detect all unauthorized changes. This is because manipulations to programs can be made in such a way that they do not come into operation until long after testing has been completed, perhaps triggered by a particular date having been passed or by a particular transaction being entered into the system.

Senior Management must be properly aware of the risks of fraudulent transactions through the use of computers and actions should be taken by operational management in the prevention of computer fraud.

IV. Nature of Controls

It is senior management's responsibility to ensure that operations are adequately protected against the risks described under section III above. Management therefore needs to understand not only the nature of computer risks but also the techniques at their disposal to manage these risks. These techniques may be classified broadly as;

- Preventive controls;
- Containment controls;
- Insurance and
- Audit.

IV-1 Preventive Controls

Preventive controls are those designed to ensure that events which threaten operations occur only very infrequently. Examples are the careful design and setting of computer centers, data input controls, security devices to prevent unauthorized access to computer equipment, passwords designed to restrict access to computer programs and data, and authentication of telecommunication messages. Other examples are the procedures used to ensure that systems specifications reflect the institution's needs, projects are properly controlled, systems are well tested before implementation and to ensure that documentation is accurate and physically secured. These types of control are essential to the effectiveness, integrity and reliability of computer systems. Preventive controls, however, are vulnerable to human failure and can never be totally reliable. Therefore, additional measures are required to ensure that potentially damaging events do not cause significant losses or cause operations to fail.

IV-2 Containment Controls

On top of preventive controls, some containment controls must exist. Containment controls are essential to protect institutions from the consequences of events which bypass preventive controls. They are designed to detect and limit the effect on the business of events which occur and threaten operations.

Examples are fire detection and extinguishing equipment, dual capacity in telecommunication and computer networks to limit the consequences of breakdowns of individual components, reconciliation procedures designed to detect errors quickly and contingency plans to aid recovery if the computer center was to be disabled by any calamity (calamity plan).

IV-3 Insurance

Some of the risks referred to in this memorandum can be insured, such as fraud by employees and the costs of replacing data, software and equipment. It may also be possible to insure against the consequential losses for an institution following damage to computer resources and consequent business interruption. Because neither preventive nor containment controls can ever be foolproof, it is usually prudent to obtain insurance coverage appropriate to the particular risks within the institution. Insurance, however, cannot be regarded as a substitute for good preventive and containment controls. To determine the scope of the insurance, particular care should be taken to identify and understand the types of losses which are not recoverable under insurance policies and the limitations imposed by the policies.

IV-4 Inspection and Audit

Even soundly designed security and control systems can fail and leave an institution exposed to losses if the procedures they lay down are not followed in practice. A regular program of independent tests of security and control procedures by inspectors, auditors or consultants should help to identify lapses in control before they put operations at serious risk. Conversely, without regular audit testing, any new or unidentified exposures which exist might not be detected for a considerable period.

Generally the frequency and depth of audit tests conducted in any area should reflect the level of risk to the institution if the security and control procedures in that area fail. With any audit program, either internal or external, it is important to establish the scope of the audit by class of risk and type of control.

Apart from regular audit checks on existing systems, Internal or External Audit involvement at an early stage in the specification and design of new systems can contribute significantly to the quality and effectiveness of security and control procedures to be developed.

V. Conclusion

Supervised institutions can normally achieve effective, secure and reliable computer systems only through an appropriate balance of all the control techniques described in this memorandum. The selected controls will vary from institution to institution, reflecting the particular risks within each institution and the costs of related security and control procedures.

Computer security and control procedures must form an integral part of the system of internal control within an institution. Therefore, it is important for Senior Management to understand the relationship that exist between the computer security and control procedures addressed in this memorandum and the total system of controls within the institution. Discussions with computer security and audit specialists as to the use and interpretation of this memorandum may assist Senior Management to achieve this understanding.